

Large-scale copyright enforcement and human rights safeguards in online markets

A comparative study of 22 sanctioning mechanisms from eight enforcement strategies in six countries between 2004 and 2014

Kreiken, Floris

DOI

[10.4233/uuid:be493008-78cc-46fa-937e-ee7de4559d98](https://doi.org/10.4233/uuid:be493008-78cc-46fa-937e-ee7de4559d98)

Publication date

2017

Document Version

Final published version

Citation (APA)

Kreiken, F. (2017). *Large-scale copyright enforcement and human rights safeguards in online markets: A comparative study of 22 sanctioning mechanisms from eight enforcement strategies in six countries between 2004 and 2014*. [Dissertation (TU Delft), Delft University of Technology]. <https://doi.org/10.4233/uuid:be493008-78cc-46fa-937e-ee7de4559d98>

Important note

To cite this publication, please use the final published version (if applicable). Please check the document version above.

Copyright

Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy

Please contact us and provide details if you believe this document breaches copyrights. We will remove access to the work immediately and investigate your claim.

Large-scale copyright enforcement and human rights safeguards in online markets

A comparative study of 22 sanctioning mechanisms from eight enforcement strategies in six countries between 2004 and 2014

The Internet has facilitated large-scale copyright infringement. Fighting this one case at a time via the standard civil law procedures is costly in terms of time and money. In response, copyright holders have adopted new strategies that they hoped would be more effective at large-scale enforcement. The question is how these large-scale enforcement procedures impact procedural safeguards, most notably due process and fair trial.

Empirical research into large-scale recent enforcement strategies has been limited and tended to focus on individual strategies, rather than on comparative analysis across different strategies and jurisdictions. This dissertation sets out to fill this gap. It presents a comparative empirical study of 22 sanctioning mechanisms from eight enforcement strategies in six countries between 2004 and 2014. It adds to the discussion on the regulation of copyrights and can help policymakers by illustrating the effect of choices made in different countries. For researchers in the field of information policy and law, it provides a detailed description of different enforcement initiatives and adds to the studies on human rights.

This study shows that copyright enforcement procedures are able to scale-up only by offering fewer procedural safeguards to sanctioned parties. Similarly, procedures that impact on a larger scale provide less severe sanctions. The research has also shown that infringement levels are by and large unchanged, and that enforcement procedures create substantial costs, a significant portion of which are externalized to the state and to third parties.

Floris Kreiken works as a policy advisor at the Dutch Ministry of Internal Affairs.

The Next Generation Infrastructures Foundation

represents an international consortium of knowledge institutions, market players and governmental bodies, which joined forces to cope with the challenges faced by today's and tomorrow's infrastructure systems. The consortium cuts across infrastructure sectors, across disciplinary borders and across national borders, as infrastructure systems themselves do. With the strong participation of practitioners in a concerted knowledge effort with social and engineering scientists, the Foundation seeks to ensure the conditions for utilization of the research results by infrastructure policy makers, regulators and the infrastructure industries.

www.nginfra.nl



81

Floris Kreiken

Large-scale copyright enforcement and human rights safeguards in online markets
A comparative study of 22 sanctioning mechanisms from eight enforcement strategies in six countries between 2004 and 2014



Floris Kreiken

Large-scale copyright enforcement and human rights safeguards in online markets

A comparative study of 22 sanctioning mechanisms from eight enforcement strategies in six countries between 2004 and 2014

81



Large-scale copyright enforcement and human rights safeguards in online markets: A comparative study of 22 sanctioning mechanisms from eight enforcement strategies in six countries between 2004 and 2014

Proefschrift

ter verkrijging van de graad van doctor
aan de Technische Universiteit Delft,
op gezag van de Rector Magnificus prof.ir. K.C.A.M. Luyben;
voorzitter van het College voor Promoties,
in het openbaar te verdedigen op
10 April om 10.00 uur

door

Floris Hans KREIKEN
Master of Laws,
Universiteit van Amsterdam, Nederland
geboren te Amsterdam, Nederland

This dissertation has been approved by the
promotor: Prof.dr. M.J.G. van Eeten

Composition of the doctoral committee:

Rector Magnificus Chairman

Independent members:

Prof.dr. J.A. de Bruijn	Delft University of Technology
Prof.dr. M.J. van den Hoven	Delft University of Technology
Prof.dr. M.L. Mueller	Georgia Institute of Technology, USA
Prof.mr. P.B. Hugenholtz	University of Amsterdam
Prof.mr. D.J.G. Visser	Leiden University

This research was funded by the Next Generation Infrastructures Foundation programme and TU Delft. Part of the work was conducted as a Google Policy Fellow at the Electronic Frontier Foundation, which was a position funded by Google.

ISBN/EAN: 978-90-79787-69-2

This thesis is number 81 in the NGInfra PhD Thesis Series on Infrastructures.

An overview of titles in this series is included at the end of this book.

Printed by Gildeprint, Enschede, the Netherlands

Cover illustration: "Grunge textured Jolly Roger pirate flag on vintage paper," by Nicolas Raymond, available under a Creative Commons Attribution 3.0 Unported License at: http://freestock.ca/flags_maps_g80-jolly_roger_pirate_grunge_flag_p1022.html

© 2017 Floris Kreiken. All rights reserved.

Table of contents

1. INTRODUCTION	7
1.1 Introduction	7
1.2 New technologies and large-scale copyright infringement	8
1.3 The challenge for enforcement	13
1.4 The stakes on both sides	16
1.5 Research question	24
PART I: BACKGROUND.....	27
2. LARGE-SCALE INFRINGEMENT.....	29
2.1 Introduction to this chapter.....	29
2.2 Copyright infringement	29
2.3 The Internet facilitates copyright infringement	30
2.4 Different methods of large-scale copyright infringement online	33
2.4.1 P2P Protocols	34
2.4.2 Usenet	36
2.4.3 Cyber lockers	36
2.4.4 Streaming sites	36
2.4.5 New “Darknet” technologies	37
2.5 Players involved in copyright infringement online	38
2.5.1 ‘The scene’	38
2.5.2 Internet intermediaries	39
2.5.3 Peers/users.....	42
2.6 The scale of copyright infringement online.....	43
2.6.1 What constitutes ‘large-scale’ copyright infringement?	43
2.6.2 Estimates on users engaged in copyright infringement	45
2.6.3 Estimates on infringing content and traffic.....	50
2.6.4 Type of infringing content	52
2.7 The business of infringement	53
2.8 Economic impact of infringement	54
3. LARGE-SCALE ENFORCEMENT	63
3.1 Introduction to this chapter.....	63
3.2 New enforcement strategies: scaling-up.....	63
3.3 Different typologies for enforcement strategies	71
3.4 A typology of enforcement strategies.....	72
4. THEORETICAL FRAMEWORK AND RESEARCH DESIGN	81
4.1 Introduction to this chapter.....	81
4.2 The economics of enforcement.....	81
4.3 Procedural safeguards.....	87
4.4 Case study research	91
4.5 Conceptualizing cases.....	93
4.6 Criteria for case selection	94
4.7 Variables and data	97
4.7.1 Scale	98
4.7.2 Severity	99
4.7.3 Safeguards.....	100

4.7.4	Impact on infringement levels.....	104
4.7.5	Costs of the system	104
4.8	Data collection/research tools.....	105
4.9	Interviewees.....	106
4.10	Analysis.....	109
PART II: CASE STUDIES		111
5. TARGETING END USERS DIRECTLY IN THE USA IN 2004-2013		113
5.1	Introduction	113
5.2	Legal background	113
5.3	The procedure in practice	118
5.4	Scale, severity and procedural safeguards	127
5.5	Impact on infringement levels	137
5.6	The costs of the system.....	140
5.7	Conclusion	142
6. TARGETING END USERS DIRECTLY IN THE UK IN 2006-2011		143
6.1	Introduction	143
6.2	Legal background	143
6.3	The procedure in practice	148
6.4	Scale, severity and procedural safeguards	150
6.5	Impact on infringement levels	156
6.6	The costs of the system.....	157
6.7	Conclusion	158
7. THE HADOPI GRADUATED RESPONSE PROCEDURE (FRANCE) IN 2011-2013.....		159
7.1	Introduction	159
7.2	Legal background	159
7.3	The procedure in practice	163
7.4	Scale, severity and procedural safeguards	168
7.5	Impact on infringement levels	176
7.6	The costs of the system.....	187
7.7	Conclusion	189
8. THE EIRCOM GRADUATED RESPONSE PROCEDURE (IRELAND) IN 2010-2013.....		191
8.1	Introduction	191
8.2	Legal background	192
8.3	The procedure in practice	196
8.4	Scale, severity and procedural safeguards	198
8.5	Impact on infringement levels	204
8.6	The costs of the system.....	205
8.7	Conclusion	207
9. NOTICE AND TAKEDOWN AT GOOGLE SEARCH AND YOUTUBE IN 2011-2013.....		209
9.1	Introduction	209
9.2	Legal background	209

9.3	The procedure in practice	214
9.4	Scale, severity and procedural safeguards	221
9.5	Impact on infringement levels	229
9.6	The costs of the system.....	230
9.7	Conclusion	231
10.	NOTICE AND TAKEDOWN IN THE NETHERLANDS IN 2009-2013....	233
10.1	Introduction	233
10.2	Legal background	233
10.3	The procedure in practice	242
10.4	Scale, severity and procedural safeguards.....	247
10.5	Impact on infringement levels.....	255
10.6	The costs of the system	256
10.7	Conclusion.....	256
11.	‘OPERATION IN OUR SITES’ (USA) IN 2010-2013	259
11.1	Introduction	259
11.2	Legal background	259
11.3	The procedure in practice	261
11.4	Scale, severity and procedural safeguards.....	264
11.5	Impact on infringement levels.....	275
11.6	The costs of the system	276
11.7	Conclusion.....	276
12.	LEY SINDE (SPAIN) IN 2012-2013	279
12.1	Introduction	279
12.2	Legal background	280
12.3	The procedure in practice	282
12.4	Scale, severity and procedural safeguards.....	284
12.5	Impact on infringement levels.....	289
12.6	The costs of the system	294
12.7	Conclusion.....	295
	PART III: ANALYSIS AND CONCLUSION	297
13.	FINDINGS AND ANALYSIS	299
13.1	Introduction	299
13.2	Summary of case results.....	301
13.3	Scale comes at the cost of safeguards	312
13.4	Severity and scale do not mix	315
13.5	Economic costs of increased enforcement	317
13.6	Enforcement has had little impact at its current scale	320
13.7	Limitations	323
13.8	Implications for policy	326
	SUMMARY	331
	SUMMARY IN DUTCH.....	339
	BIBLIOGRAPHY	347

Articles, Books, News, Websites	347
Case law used and referenced	385
Interviews and personal communication	388
ACKNOWLEDGEMENTS	391
CURRICULUM VITAE	395
NGINFRA PH.D THESIS SERIES ON INFRASTRUCTURES.....	397

1. INTRODUCTION

1.1 Introduction

The Internet has been a disruptive force in many markets, among them the markets for entertainment and cultural products. The protection of copyright on these products has been undermined by technologies that facilitate large-scale infringement. Copyright is a legal tool which was devised to incentivize cultural production and to facilitate access to culture by the public. How large-scale infringement impacts these values is, so far, unclear. The market is adapting to the changes and seems to be doing well in some areas, and worse in others.

Rights holders, however, view infringement as intrinsically illegal, wrong and harmful. They have sought increased enforcement of copyright via gaining more control over the technologies through which content is distributed. A key problem for any form of control is scale. Since infringement is widespread, enforcement efforts also need to impact at a large scale. Surveys have consistently shown that significant portions of the population in Western countries engage in infringing behavior. Fighting this one case at a time via the standard civil law procedures is costly in terms of time and money. It clearly does not scale well. In response, rights holders have adopted new strategies that they hoped would be more effective at large-scale enforcement. Some of these strategies put intermediaries, like Internet Service Providers (ISPs) and governments in the role of enforcers.

Few people defend infringement, but there are concerns that these new enforcement strategies are disproportionately costly to society. Technologists, academics and civil society organizations, like the Electronic Frontier Foundation, argue that that scaled-up enforcement will be bad for human rights and other public values because it erodes procedural safeguards, most notably due process and fair trial. Fewer safeguards would give too much control over Internet services, and even Internet access, to rights holders. In a nutshell, the argument is that if rights holders can unilaterally decide what is right or wrong because of lacking judicial scrutiny, then this will be bad for free speech, the rule of law, and innovation.

Proponents of intensified enforcement point to the cost of infringement, which they estimate to be in the billions. Rights holders, White House and EU representatives also claim large-scale enforcement can be done in accordance with human rights. According to representatives of the rights holders, such as the Movie Picture Association of America (MPAA) and the US Chamber of Commerce, SOPA and ACTA follow the same rules of civil procedure you would find in an ordinary trial. In their view, copyright enforcement targets illegal sites and people that infringe on copyright only and does nothing to harm legal uses of content and Internet users who are not sharing protected content.

Who is right? A crucial part of the answer depends on identifying the actual impact of the new strategies on procedural safeguards. This is an empirical question. Empirical research into large-scale recent enforcement strategies has been limited and tended to focus on individual strategies, rather than on comparative analysis across different strategies and jurisdictions. This dissertation sets out to fill this gap. It presents a comparative empirical study of 22 sanctioning mechanisms from eight enforcement strategies in six countries between 2004 and 2014.

In the remainder of this chapter, we will first unpack the controversial issues around large-scale infringement and enforcement in a bit more detail. This sets up the main research question to be operationalized, studied, and answered in the subsequent chapters. Part of this introductory chapter was first published as an article in the *Illinois Journal for Law, Technology and Policy*.¹

1.2 New technologies and large-scale copyright infringement

Justin Bieber is one of the biggest and most popular artists of our time. The Canadian star, originally discovered on YouTube in 2007, has won several Grammy awards, attracted over 60 million followers on Twitter, and appeals to audiences worldwide. His success is directly related to his presence on Twitter and, especially, YouTube, where his videos attract millions of views.² YouTube is one of the most popular websites in the world.³ It has become an important cultural medium, reaching well beyond pop stars and their fans. Politicians share their content on the platform, companies build their brands there, and important events are broadcasted live via the site.

Although Justin Bieber has many fans, there are also many people who do not like him. A Google search for the exact phrase “I hate Justin Bieber” brings up hundreds of thousands of results. Among the people who dislike Bieber is a young man with the Internet name ‘iLCreation’. One day, he decided to remove a very large number of Justin Bieber videos from YouTube, including Bieber’s entire official Vevo channel.⁴ This happened relatively easy and quickly. He claimed to own the copyrights on Bieber’s songs and sent notices to YouTube requesting Youtube to take the videos down.⁵ The site complied promptly. Immediately, mobs of teenage girls requested the videos’ reinstatement, with trending topics like “#WEWANTJUSTINBIEBERVEVOBACK”. The videos were back online after some hours.⁶

Notice and takedown, the procedure ‘iLCreation’ used, is a copyright enforcement procedure created to grant rights holders additional tools to protect their content on the Internet. Those tools backfired in this case. It was not the first or last time, either. During U.S. first lady’s Michelle Obama’s speech at the Democratic Convention, her content was flagged as copyright infringement as well,⁷ as was a short NASA video of the Martian Rover landing on Mars.⁸ The list of such examples is seemingly endless, with a long tail that never makes it into the public view.

¹ Floris Kreiken & David Koepsell, “Coase and Copyright,” *University of Illinois Journal of Law, Technology and Policy* 1 (2013): 1-44.

² “Justin Bieber”, www.wikipedia.org.

³ YouTube ranks number 3. See: “Top 500 Global sites,” Alexa, <http://www.alexa.com/topsites>.

⁴ Vevo is the official channel recording studios use to present their work to the public.

⁵ “Cyber-prankster iLCreation gets all of Justin Bieber’s clips yanked from YouTube”, *News.com.au* (August 30, 2011), <http://www.news.com.au/entertainment/music/cyber-prankster-gets-all-of-justin-biebers-clips-yanked-from-youtube/story-e6frfn09-1226125502750>.

⁶ “Cyber-prankster iLCreation gets all of Justin Bieber’s clips yanked from YouTube”, *News.com.au*.

⁷ Will Oremus, “Did YouTube Really Block Michelle Obama’s DNC Speech for Copyright Infringement?”, *Slate* (September 5, 2012), http://www.slate.com/blogs/future_tense/2012/09/05/michelle_obama_dnc_speech_why_did_youtube_flag_it_for_copyright_infringement_.html.

⁸ Alex Pasternack, “NASA’s Mars Rover Crashed Into a DMCA Takedown”, *Motherboard* (August 6, 2012), <http://motherboard.vice.com/blog/nasa-s-mars-rover-crashed-into-a-dmca-takedown>.

New copyright enforcement procedures are meant to better protect content on the Internet, but it would have been much more difficult for the original copyright enforcement procedures to backfire in such a way. 'iLCreation' would have had to go to either YouTube headquarters or to a judge, state his rights and provide evidence.

How did we end up in this situation? First, and most obvious, our society changed. In a short time, we adopted new information and communications technologies (ICT), which affected communication, culture and economics. Sociologists have argued that our society has changed from an industrial society to an information society or network society.⁹ This means we live in a society in which information is an important part of economic, political and cultural life.¹⁰ Historian Adrian Johns claims that information has become one of the most important foundations of the social, economic and cultural order of the 21st century. It has, in fact, become such a key commodity that he claims that the economic power of knowledge and imaginative creativity in the 21st century is on par with the hegemony of manufacturing in the 19th century, and energy in the 20th century.¹¹

At the heart of this shift is the rise of the Internet. One of the Internet's most important characteristics is its openness, according to Jonathan Zittrain. He refers to it as the "generative" character of the Internet. Zittrain defines generativity as the "system's capacity to produce unanticipated change through unfiltered contributions from broad and varied audiences."¹² The infrastructure and technology underlying the Internet and computers remain constantly evolving and thus free for others to build on and improve upon.¹³

Generative systems are powerful and valuable because they allow for the production of useful things like the Web, but also because they allow a huge number of people to express themselves through speech, art, or code and enable them to work with other people in ways previously impossible.¹⁴ The Internet, like the personal computer (PC), was originally designed to have people build on, expand, and 'tinker' with its capabilities. It is exactly this open character that made it initially attractive to large audiences, and made innovations like the World-Wide Web, instant messaging, peer-to-peer networking, Skype, Wikipedia and other innovations possible.¹⁵ There is, of course, a downside to this openness as well. It leaves the Internet vulnerable to problems, like viruses, spam, identity theft and crashes.¹⁶

The Internet's openness has also affected cultural production. One of the most important changes is how cultural artifacts are made.¹⁷ Anyone with a PC and an Internet connection can make a movie or record a song, and can distribute it easily. It has brought about radical changes in the organization of information production, such as the rise of peer-

⁹ See for example: Manuel Castells, *The Rise of the Network Society* (1994) and Yogai Benkler, *The Wealth of Networks* (Yale University Press, 2006).

¹⁰ According to the International Organization for Standardization and the International Electro Technical Commission, information is defined as "knowledge concerning objects, such as facts, events, things, processes, or ideas, including concepts, that within a certain context has a certain meaning." Definition taken from ISO/IEC document 2382-1, from 1993.

¹¹ Adrian Johns, *Piracy: The intellectual property wars from Gutenberg to Gates*, (University of Chicago Press, 2009). P.4.

¹² Zittrain, *The future of the Internet*. P.70.

¹³ Zittrain, *The future of the Internet*. P.27-31.

¹⁴ Zittrain, *The future of the Internet*. P.42.

¹⁵ Zittrain, *The future of the Internet*. Preface.

¹⁶ Zittrain, *The future of the Internet*. P.3.

¹⁷ Lawrence Lessig, *Free culture: How big media uses technology and the law to lock down culture and control creativity*, (Penguin, 2004). P.10-11.

production like Wikipedia and user-generated content via platforms like YouTube.¹⁸ The changing information infrastructure has consequences for the underlying economics and regulation. Information business models no longer require high up-front costs and low marginal costs of distribution to reach a wide population and this challenges the old information business models like the mass media model.¹⁹ Similarly, the openness of the internet has changed the ability to control information flows significantly.

These changes disturb the power balance among actors with competing interests: governments, incumbent companies, new market entrants, intermediaries, users, hackers, et cetera. Different groups try to get control over the new technology. Lessig warned that although cyberspace started out largely free and unregulated, it could potentially be a system of perfect regulation. Governments are intrinsically drawn to this type of control, because it helps to maintain social order. Incumbent companies leverage it to protect profitable business models.²⁰ Lessig warns that governments and commerce could band together to construct an architecture that will allow for perfect control and will make highly efficient regulation possible.²¹ This struggle for control has led to numerous tensions in the online world. In his book 'Code', Lessig predicted that there would be three main areas of controversy: privacy, free speech and intellectual property rights.²²

This dissertation focuses on one arena where this power struggle is taking place: intellectual property, and copyright in particular. Copyright has grown to be one of the main legal tools to regulate information flows. According to the World Intellectual Property Organization, copyrights exist "to encourage a dynamic culture, while returning value to creators so they can lead a dignified economic existence, and to provide widespread, affordable access to content for the public."²³ These laws apply to creations of the human mind and give the creators property rights over their creations.²⁴

There are two types of intellectual property (IP); industrial property, which applies to inventions (broadly speaking), and copyright. The latter applies to artistic creations, like books, music, paintings, sculptures, films and technology-based works such as computer programs and electronic databases. It is said to apply to the form of expression, but not the ideas behind them.²⁵ Although copyright is a property right, it is unlike rights to tangible goods and physical property. Intellectual property concerns goods that can be used by an individual or other entity without affecting the ability of anyone else to use that same object.²⁶ The marginal costs of producing an additional one of the same are essentially zero.²⁷ At the same time, if someone copies a song, it is difficult to prevent further copying. IP is thus said to involve objects that are non-rivalrous (because multiple people can enjoy

¹⁸ Benkler, *The wealth of networks*. P.4.

¹⁹ Benkler, *The wealth of networks*. P.5.

²⁰ Lawrence Lessig, *Code And Other Laws of Cyberspace, Version 2.0*, (Basic Books, 2006). P.Xiii.

²¹ Lessig, *Code, Version 2.0*. P.4.

²² Lessig, *Code, Version 2.0*.

²³ "Copyright and Related Rights," *World Intellectual Property Organisation*, <http://www.wipo.int/copyright/en/> (last visited Jan. 22, 2013).

²⁴ "Enforcement of rights," *World Intellectual Property Organisation*, http://www.wipo.int/freepublications/en/intproperty/909/wipo_pub_909.html#enforcement (last visited Jan. 22, 2013).

²⁵ "Enforcement of rights," *World Intellectual Property Organisation*.

²⁶ David Easley and Jon Kleinberg, *Networks, crowds, and markets: Reasoning about a highly connected world*, (Cambridge University Press, 2010). P.784.

²⁷ Richard Cornes and Todd Sandler, *The theory of externalities, public goods, and club goods*, (Cambridge University Press, 1996). P. 8-10.

the same good) and non-excludable (because it is difficult to prevent others from using the content).²⁸ Excludable goods are things like private goods. You can prevent other people from entering your car, for example. Physical tokens that hold expressions, like CDs, DVDs, and books, are also excludable.

Intellectual property (IP) rights, like copyright, aim to make expressions legally excludable:²⁹ they exclude others from reproducing or making the first sale of any token instantiating a type that has been created by the rights holder.³⁰ This means the author of a book can forbid others from selling a copy of his story without paying him royalties (according to the law, in the case of non-digital books—at least the first sale of the particular token expressing his story—used books and other media may be sold without paying royalties).³¹ Copyright protection is not absolute; it is limited in scope and time, while certain (fair use) exceptions are allowed if they benefit the general good, like exceptions for educational purposes or parody.³²

Today, national copyright laws have been standardized to some extent through international and regional agreements such as the Berne Convention and the European copyright directives. This Berne convention was succeeded in 1967 with the establishment of the World Intellectual Property Organization (WIPO) by treaty as an agency of the United Nations. Copyright is now largely recognized as a fundamental principle in western society. It has been included in the Universal declaration of human rights³³, and has been incorporated in the international Covenant on Economic, Social and Cultural rights.³⁴ It has been standardized more or less through other international treaties, regional agreements and legislation. The WTO agreement on trade related aspects of intellectual property rights (TRIPS) is an international agreement that lays down minimum standards of intellectual property protection. Becoming a member of the WTO requires ratification of this TRIPS agreement. So countries that want to be part of the world economy have to recognize and enforce copyrights.³⁵

New Internet-based technologies have undermined the protection of copyright on cultural products. Digitalization changed the economics and character of reproduction, and dramatically lowered the traditional and economic boundaries to infringe on copyrights. It

²⁸ Lessig, *Code, Version 2.0*. P.182.

²⁹ Bruce A. Lehman, *Intellectual property and the national information infrastructure: The report of the working group on intellectual property rights*, (Diane Publishing, 1995). P.63.

³⁰ Lehman, *Intellectual property and the national information infrastructure*. P.64. P. 90.

³¹ David Koepsell, *Innovation and nanotechnology: Converging technologies and the end of intellectual property*, (Bloomsbury Publishing, 2011). P.176-177.

³² "Enforcement of rights," *World Intellectual Property Organisation*.

³³ Article 27 of the Universal Declaration of Human Rights says that '(1) Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits, and (2) Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.'

³⁴ Article 15 states that: '1. The States Parties to the present Covenant recognize the right of everyone: (a) To take part in cultural life; (b) To enjoy the benefits of scientific progress and its applications; (c) To benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author, 2. The steps to be taken by the States Parties to the present Covenant to achieve the full realization of this right shall include those necessary for the conservation, the development and the diffusion of science and culture, 3. The States Parties to the present Covenant undertake to respect the freedom indispensable for scientific research and creative activity, 4. The States Parties to the present Covenant recognize the benefits to be derived from the encouragement and development of international contacts and co-operation in the scientific and cultural fields.'

³⁵ Lessig, *Free culture*. P.51.

made copying information easy and inexpensive and decoupled information from its medium (the physical entity or token carrying it).³⁶ Networked devices allow for the inexpensive distribution and reproduction of those digitized files.³⁷ At the click of a mouse, perfect copies could be searched for and sent to the other side of the world.

As digitization and the Internet facilitated content reproduction and distribution, it also facilitated infringement on a large scale. Copyright infringement rose rapidly with Napster and the rise of peer-to-peer (P2P) file sharing. P2P file sharing allowed users to swap MP3 files, thereby bypassing traditional music business models, causing massive copyright infringement in the process. One of the groundbreaking features of P2P file sharing is that it, like the Internet, scales well. Instead of relying on one central server to distribute content to users, P2P decentralizes distribution to its users, which prevents the costs of hosting network congestion, and increases the volume of content that can be shared. The only centralized control of Napster was a central index server that allowed users to search for content.³⁸

After Napster was sued, similar programs quickly followed that allowed for the same level of copyright infringement and further decentralized the file sharing architecture, like Grokster, KaZaA, Morpheus, Limewire and eventually BitTorrent, the most sophisticated P2P file sharing protocol.³⁹ After that, BitTorrent followed, the most sophisticated P2P file sharing protocol so far.

According to industry reports, P2P file-sharing platforms were adopted on a massive scale. According to PC Pitstop and BigChampagne, 220 million PC's worldwide had P2P applications installed in 2008.⁴⁰ BitTorrent, specifically, had 100 million regular users worldwide. According to some reports, two thirds of BitTorrent traffic consists of copyright infringing material.⁴¹

File sharing has also grown via other means, mainly through HTTP. This is largely due to the rise of content on demand systems, like YouTube, Megavideo, Dailymotion and Netflix (also called 'Web 2.0' services), the rise of social media like Facebook, LinkedIn and Twitter, and the move towards 'cyber lockers,' like Rapidshare and Megaupload.⁴² Those large cyber lockers and streaming sites like Rapidshare generated 32 million daily visits, whilst megavideo.com and megaupload.com each generated 14 million daily visits.⁴³

According to the research agency Envisional, in 2010, 23,76% of all (non-pornographic)⁴⁴ Internet traffic worldwide was infringing. Other research estimates the percentage of users engaged in copyright infringement online between 15-45%. This means

³⁶ National Research Council (US). Committee on Intellectual Property Rights, et al, *The Digital Dilemma: Intellectual Property in the Information Age*, (National Academy Press, 2000). P.32.

³⁷ National Research Council (US). *Digital Dilemma*. P.38.

³⁸ Annemarie Bridy, "Is Online Copyright Enforcement Scalable?" *Vanderbilt Journal of entertainment and technology law* 13 (2011): 695. P.699.

³⁹ Bridy, "Is Online Copyright Enforcement Scalable?" P.700-703.

⁴⁰ Mary Madden, "The state of music online: Ten years after Napster," *Pew Internet & American Life Project* (2009). P.9.

⁴¹ David Price, *An estimate of infringing use of the Internet*, (Envisional, 2011). See: <http://documents.envisional.com/docs/Envisional-Internet-Usage-Jan2011.pdf>. P.3-4

⁴² Bridy, "Is Online Copyright Enforcement Scalable?" P.704-706.

⁴³ Markmonitor, *Traffic Report: Online Piracy and Counterfeiting* (2011), see: https://www.markmonitor.com/download/report/MarkMonitor_-_Traffic_Report_110111.pdf

⁴⁴ Pornography was left out of the results as it is difficult to establish whether pornography online is copyright protected or not.

millions of users infringe on copyright online. In terms of types of content, users access music, video, games, books, photos, software and other files.

While copyright infringement has happened on such a large scale, it has been difficult to estimate the exact effects on the market for entertainment. There is no scientific consensus about how to synthesize the fragmented empirical evidence of the effects.⁴⁵ There has been an enormous amount of research, which has been interpreted to draw a great number of different, sometimes contradictory, conclusions. Consulting firm Considerati has summarized a wealth of these studies. While some studies find no effect or a net positive effect, the majority of economic studies suggest copyright infringement has a negative influence on legal sales.⁴⁶

In the mean time, the market has been adapting to the changes. It seems to be doing well in some areas, and worse in others. The changes showed that business models in the entertainment industry could no longer rely on the industry's ability to retain exclusive control over distribution through physical channels.⁴⁷ At the same time, Napster and the advent of P2P sharing not only undermined the traditional business model, but also showed the potential benefits of digital distribution. It potentially allows for more direct contact between creators and consumers, and allows for changing the role of 'middlemen.' It reduces some costs, like distribution, but it can also create new costs, like the need for online advertising.⁴⁸

In response, new business models have arisen. For music distribution, this includes a la carte services like iTunes, that sell individual files in digital form, and subscription services like Spotify, which requires users to pay a monthly fee for full access to streaming content (Spotify also offers a free subscription with advertisements and certain access restrictions). The movie industry saw the emergence of similar subscription services, like Netflix, the popular movie streaming service, and services where people can receive a movie file that they can access for only a limited time, like Movielink. Modern technology allows for more personal video recording, like ReplayTV and TiVo, which has been undermining the revenue model for TV, which is mainly based on advertising and subscription. Books switched to eBooks, which mainly follow the same business model, and are strengthened by new distribution tools. Some of these books are protected by DRM. So far, however, we have not seen a massive shift to eBooks, mainly, some authors suggest, because the reading experience is not the same. Other print media rely on advertising, and the switch to the Internet has meant increased competition for advertising revenue. Paper media occasionally switches to an online subscription model, like the New York Times has done.⁴⁹

1.3 The challenge for enforcement

Although the market has shifted and seems to be doing well in some areas, rights holders have understandably focused on the losses to their business models. Rights holders have

⁴⁵ Bart Schermer and Martine Wubben, *Feiten om te delen: digitale contentdistributie in Nederland*, (Considerati, 2011). P.64.

⁴⁶ Schermer and Wubben, *Feiten om te delen*. P.77.

⁴⁷ Urs Gasser, *Copyright and Digital Media in a Post-Napster World: 2005 Update*, (Berkman Publication Series 2005-03 2005). P.9-19.

⁴⁸ National Research Council (US). Committee on Intellectual Property Rights, et al, *The Digital Dilemma: Intellectual Property in the Information Age*, (National Academy Press, 2000). P.41-42.

⁴⁹ Urs Gasser, *Copyright and Digital Media in a Post-Napster World: 2005 Update*, (Berkman Publication Series 2005-03 2005). P.9-19.

sought to increase enforcement of copyright via gaining more control over the technologies through which their content is distributed.

One way to prevent Internet users from downloading copyrighted content without paying is, for example, through technological locks like ‘digital rights management’ (DRM). DRM makes digital works harder to copy, or can make it easier to ensure payment for copying.⁵⁰

Apart from those technological ways, rights holders, sometimes in collaboration with governments, have developed new enforcement strategies through new and existing laws. A key problem that rights holders were trying to solve was scale. This has created a variety of new strategies to scale up enforcement. These can be categorized into four groups – see Table 1.1. We briefly discuss each of the four types of strategies.

Enforcement strategies	Direct	Indirect
Target demand side	Targeting end users through law suits and settlement requests	Graduated response procedure
Target supply side	Criminal cases against large suppliers /(DRM)	Notice and takedown

Table 1.1: four groups of enforcement strategies

(1) Strategies that target the demand for infringing content (end-users) directly on a large scale by aiming for settlements instead of actual lawsuits. Private players, like rights holders or their representatives, sue end users.

In the US, the music industry and lawfirms have targeted thousands of people. Specialized law firms threaten users with lawsuits on the basis of their IP address. The goal of these warning letters is not to actually make it to court, but to generate quick settlements. For example, The US copyright group (DC area firm of Dunlap, Grubb & Weaver) has filed thousands of lawsuits on behalf of independent film makers.⁵¹ In Germany, each year hundreds of thousands of file sharers are sent letters by law firms requesting copyright payments for illegal downloading. According to one lawyer defending recipients of such letters, half a million of those letters were sent in 2011 and about 250,000 were sent in 2012. The letters request payments of between 300 and 1,500 Euros. By fgoing after quick settlements rather than court cases, the costs of sanctioning infringers has gone down.⁵² There is a special term used to describe this strategy in Germany, namely ‘Abmahnwahn’ (warning letter madness). Numerous firms are engaged in this practice.⁵³ A new law has

⁵⁰ I. Trotter Hardy, *Project looking forward*. P.69-70.

⁵¹ Bridy, “Is Online Copyright Enforcement Scalable?” P. 712, and: Nate Anderson, “The RIAA? Amateurs, Here’s how you sue 14,000+ P2P users,” *Ars Technica* (June 2, 2010), <http://arstechnica.com/tech-policy/news/2010/06/the-riaa-amateurs-heres-how-you-sue-p2p-users.ars>.

⁵² Michael Fritz, “File-sharing in Germany: Could the cost of getting caught be about to come down?,” *ZDNet* (August 9, 2013), <http://www.zdnet.com/file-sharing-in-germany-could-the-cost-of-getting-caught-be-about-to-come-down-7000018915/>.

⁵³ Christian Solmecke, “An overview of file sharing in Germany,” *Wilde Beuger Solmecke Rechtsanwälte* (Feburary 28, 2014), <https://www.wbs-law.de/eng/file-sharing-eng/overview-file-sharing-germany-50767/>.

made the requested payment only 150 Euros.⁵⁴ The idea behind that legislative change is to protect consumers.⁵⁵

(2) Strategies that target end-users indirectly through the introduction of graduated response procedures. These procedures use a system of increasingly severe sanctions for each infringement to deter users, often starting with a warning letter and ending with Internet disconnection or fines as the ultimate sanction for repeat infringers. These procedures require intermediaries in the administration of sanctions.

In countries like France,⁵⁶ New Zealand,⁵⁷ Taiwan,⁵⁸ South Korea,⁵⁹ and the UK,⁶⁰ graduated response systems have been introduced.⁶¹ There are some differences between the ways the system is implemented in each country. For example, the French system is legislative in nature, with a public authority administering the system. In Ireland, the whole system is private and implemented by an ISP (Eircom). In the US, rights holders and ISPs agreed to a memorandum of understanding, with provisions that lay down a privately administered graduated response system.⁶²

(3) Strategies that target the supply side directly by taking down or filtering complete websites that offer infringing content. Governmental parties often carry out these procedures, through criminal procedures.

The Court in Sweden sentenced four of The Pirate Bay⁶³ representatives to one in year in jail, and damages of 2.7 million Euros for assistance in making copyright protected content available and providing means.⁶⁴ Meanwhile, a Hong Kong court of appeals sentenced a user to three months in prison for uploading three movies to a P2P site.⁶⁵ The focus now seems to be on fighting infringement on a commercial scale by introducing criminal penalties. The proposed ACTA (article 23(1)) treaty contained provisions on this for example.⁶⁶

Private players sued P2P search engines, cyber lockers, Usenet forums and websites that link to content.⁶⁷ In some cases, lawsuits were unsuccessful, and websites offering content like YouTube were allowed to keep doing business. But in other cases, those

⁵⁴ Michael Fritz, "File-sharing in Germany: Could the cost of getting caught be about to come down?," *ZDNet* (August 9, 2013), <http://www.zdnet.com/file-sharing-in-germany-could-the-cost-of-getting-caught-be-about-to-come-down-7000018915/>.

⁵⁵ Andy, "Germany passes law to mitigate copyright trolling fines," *Torrentfreak* (July 3, 2013), <https://torrentfreak.com/germany-passes-law-to-mitigate-copyright-trolling-fines-130703/>.

⁵⁶ 'Loi favorisant la diffusion et la protection de la création sur Internet,' also referred to as the HADOPI law, 13 May 2009.

⁵⁷ Copyright infringing file sharing amendment act 2011, 18 April 2011.

⁵⁸ Internet Service Provider Liability Limitation Bill 2009, 21 April 2009.

⁵⁹ Copyright Act 1959 Article 133-2 and Article 133-3.

⁶⁰ Digital economy act 2010 C.24.

⁶¹ Christophe Geiger, "Challenges for the Enforcement of Copyright in the Online World: Time for a New Approach" in: *Research Handbook on the Cross-border Enforcement of Intellectual Property*, ed. Paul torremans (Edward Elgar Publishing, 2014). P.5.

⁶² Annemarie Bridy, "Graduated Response American Style: 'Six Strikes' Measured Against Five Norms." *Fordham Intellectual Property, Media & Entertainment Law Journal* 23.1 (2012): 1-66. P. 18-23.

⁶³ A massive torrent indexing website.

⁶⁴ Geiger, "Challenges for the Enforcement of Copyright in the Online World," P.3.

⁶⁵ Geiger, "Challenges for the Enforcement of Copyright in the Online World," P.3.

⁶⁶ Geiger, "Challenges for the Enforcement of Copyright in the Online World," P.12.

⁶⁷ Jessica Litman, "Sharing and stealing." *Hastings communications and entertainment law journal* 27 (2004). P.3 and: See *MGM v. Grokster*, 380 F.3d 1154 (9th Cir. 2004); *A&M v. Napster*, 239 F.3d 1004 (9th Cir. 2001); *In re Aimster*, 334 F.3d 643 (7th Cir. 2003)

websites ceased to exist. The goal of these lawsuits was to put the website out of business, take it down, or change it completely. For example they have tried to sue the Internet service providers that enable consumers to trade files.⁶⁸

Governments have also targeted supply directly, mostly through criminal lawsuits. The US Immigrations and Customs Enforcement (ICE) launched 'Operation in Our Sites' and seized hundreds of domains in the US, often in cooperation with rights holders.⁶⁹ Operators of large websites and cyber lockers are prosecuted for criminal copyright infringement. This is what happened to Megaupload, whose sites were seized.⁷⁰

(4) Strategies that target the supply side indirectly by taking down infringing content through intermediaries. This involves Notice-and-takedown procedures, where under threat of legal action, intermediaries are asked to take down certain content of their platform. This can potentially scale quite well, by automated mechanisms for detecting infringing content and issuing takedown requests. This raises the question, however, of what safeguards are in place for users that upload content from mistaken or disputed takedowns, such as the cases of Justin Bieber and Michelle Obama that were discussed earlier in this chapter. There can be consequences for repeat infringers here too: YouTube blocks users from uploading, if they have received too many warnings. Given that some of these user channels are serious businesses in their own right, generating millions in revenue, mistaken or disputable sanctions are potentially harmful.

Notice and notice also falls under this category. In Canada, this means that ISPs forward notices from rights holders to users when those users host or share infringing content. However, ISPs do not reveal contact details of their subscribers or take action afterwards.⁷¹

1.4 The stakes on both sides

Infringement is illegal and widely disapproved. This does not automatically mean, however, that all forms of enforcement are merited and justified. Some authors are concerned that the new enforcement strategies are disproportionately costly to society. These concerns are articulated in the context of different discussions.

The first discussions focus on the expanded reach of enforcement by the extended application of copyright itself and by technological protection measures. In 1790, only maps, charts and books were covered by copyright, but this has greatly expanded. It only focused on the right to publish, and forbade republishing by others.⁷² It first only regulated publishers, but now also covers users, and authors, because they also make copies and can also distribute.⁷³ This has put pressure on the first sale doctrine. Originally, a user would be free to do anything with a purchased work, but now rights holders would still be able to

⁶⁸ Jessica Litman, "Sharing and stealing." *Hastings communications and entertainment law journal* 27 (2004). P.3 and: See RIAA v. Verizon, 351 F.3d 1229 (D.C. Cir. 2003).

⁶⁹ Joe Karaganis, "Meganomics," *The American Assembly, Columbia University* (January 24, 2012), see: <http://piracy.americanassembly.org/meganomics/>.

⁷⁰ Chloe Albanesius, "Megaupload Shutdown Fails to Slow File Sharing," *PCmag* (February 9, 2012), <http://www.pcmag.com/article2/0,2817,2400052,00.asp>.

⁷¹ Thomas Mennecke, "Canada Plans P2P and file-sharing Crackdown," *Slyck* (March 24, 2005), <http://www.slyck.com/news.php?story=720>.

⁷² Lessig, *Free culture*. P.100.

⁷³ Lessig, *Free culture*. P.102.

control their work, as copies are being made for use.⁷⁴ So the law now controls the creativity of everyone, not just of commercial enterprises.⁷⁵

Other discussions focused on technological regulation like DRM. In his book *Code*, Lessig has brought forward that regulation through technology could pose serious risks, as they disregard fair use. The private parties imposing DRM have not been democratically elected and can now steer our behavior online, as much as the law can do.⁷⁶ Ian Hickson says DRM was intended to provide leverage for content creators against creators of playback devices. It is an extra measure of control.⁷⁷

Increasingly, the discussion has shifted to procedural safeguards. Technologists, academics and civil society organizations, like the Electronic Frontier Foundation, argue that scaled-up enforcement will be bad for human rights and other public values because it erodes procedural safeguards, most notably due process and fair trial. Safeguards prevent mistrial and abuse of the law. These guarantees are laid down in a number of international treaties and national constitutions, and require for example the right to have a fair hearing, certain standards of evidence, the presumption of innocence, some rights to legal assistance, transparency, oversight, accountability and appeals.⁷⁸

Bridy names this as one of the main challenges to copyright: notice and takedown scaled up well to deal with large-scale instances of infringement, but sometimes at the cost of procedural safeguards. She mentions that thus far, copyright holders and governments have looked towards enforcement initiatives that could scale as well for other forms of copyright infringement, like through peer to peer channels. These new enforcement initiatives could be the graduated response procedure, but she warns that in some cases this could put pressure on procedural safeguards like due process and fair trial.⁷⁹

One of the ways this tension arises is because enforcement is delegated to private players, like ISPs, to decrease costs and make it less time consuming. According to Elizabeth Thornburg, this is problematic because they are not legally obligated to guarantee the same procedural safeguards as a judge would. She also writes that they are biased towards corporate repeat players, which in this case refers to the rights holders and their representatives.⁸⁰ Those graduated response procedures also rely on procedures outside of ordinary courts. According to Lilian Edwards, "only this way it can scale to deal with thousands or even millions of file sharers."⁸¹ The special UN rapporteur on free speech has expressed similar concerns.⁸² Similarly, Hugenholtz warns that the gradual displacement of civil law remedies by mechanisms of self-imposed enforcement gives reason for concern, because they potentially affect fundamental freedoms of the citizens subscribing to the

⁷⁴ Lessig, *Free culture*. P.109.

⁷⁵ Lessig, *Free culture*. P.18.

⁷⁶ Lessig, *Code, Version 2.0*.

⁷⁷ Ian Hickson, through *Google +* (March 19, 2013), <https://plus.google.com/+IanHickson/posts/iPmatxBYuj2>

⁷⁸ Edwards, *Role and responsibility of the Internet intermediaries*, P.31.

⁷⁹ Bridy, "Is Online Copyright Enforcement Scalable?"

⁸⁰ Elizabeth Thornburg, "Going private: Technology, due process, and Internet dispute resolution," *University of California at Davis Law Review* (2000).

⁸¹ Edwards, *Role and responsibility of the Internet intermediaries*, P.30.

⁸² Frank La Rue, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression." *U.N. DOC. A/HRC/17/27* (2011). P.10.

Internet – notably, rights of due process, freedom of expression and information and right to privacy.⁸³

Yochai Benkler warns that this is a trend: “copyright maximalists” try to create new pressure points that will allow them to more easily enforce copyright “without having to go to the trouble of identifying specific infringements or proving anything to a court.” Benkler argues that the industry perceives copyright laws as “too balanced” for their taste, and that they wanted to replace traditional copyright law, as balanced by courts, with the unilateral power to shut down whole websites suspected of aiding piracy, he writes.⁸⁴

Free speech, privacy and safeguards

One of the reasons why safeguards could be important is because of their relation with free speech. Free speech is important in democratic society. It serves an instrumental value, that democratic progress and the pursuit of truth and knowledge is based on open discussion,⁸⁵ and protects against tyranny,⁸⁶ and has intrinsic value in itself to enable flourishing.⁸⁷ Free speech is however not absolute, there are restrictions. Some false speech can limit the pursuit of truth and knowledge,⁸⁸ or cause harm. Meanwhile, other values may be more important.⁸⁹

Volokh argues that in the US, copyright is just like any other speech restriction, and should therefore be treated as such: there should be strict judicial review, and authorities should be cautious when restraining speech in advance. He argues that the specific boundaries of whether speech falls in an unprotected category are notoriously hard to define. Merely describing the categories of speech that are unprotected is not sufficient; Courts must independently review judgments to see whether or not certain speech is protected.⁹⁰

Volokh argues that similar scrutiny should apply to copyright as this restricts speech as well. Copyright law restricts you from “writing, singing, painting, or otherwise communicating what you please.”⁹¹ Copyright law regulates expressions. They give the creator or an author of an expression the exclusive right to copy, distribute and adapt certain expressions for a period of time, after which the expression reverts to the public domain. Ideas, the information behind the expression, are free.⁹² It also regulates software. Essentially copyright and freedom of expression regulate the same thing: expressions. Expressions that aren’t covered by copyright, are covered by free speech protection. There is, according to Volokh, no reason to treat copyright different from any other speech restriction.⁹³ Therefore, he argues, safeguards in copyright disputes are important.

⁸³ Bernt Hugenholtz, "Codes of Conduct and Copyright Enforcement in Cyberspace," *Copyright enforcement and the Internet*, Information law series 21 (2012): 303-320. 304.

⁸⁴ Yochai Benkler, "Seven Lessons from SOPA/PIPA/Megaupload and Four Proposals on Where We Go From Here," *Techpresident* (January 25, 2012), <http://techpresident.com/news/21680/seven-lessons-sopapipamegaupload-and-four-proposals-where-we-go-here>

⁸⁵ Frederick Schauer, *Free speech: a philosophical enquiry*, (Cambridge University press, 1982). P.35-39.

⁸⁶ Richard Delgado and Jean Stefancic. *Understanding words that wound*. (Westview Press, 2004).

⁸⁷ Richard Delgado and Jean Stefancic. *Understanding words that wound*. (Westview Press, 2004).

⁸⁸ Schauer, *Free speech*. P.17 and P.33.

⁸⁹ Schauer, *Free speech*.

⁹⁰ Volokh and McDonnell, "Freedom of Speech and Independent Review in Copyright Cases," P.2436

⁹¹ Volokh and McDonnell, "Freedom of Speech and Independent Review in Copyright Cases," P.2433

⁹² Lessig, *Free culture*. P.64

⁹³ Volokh and McDonnell, "Freedom of Speech and Independent Review in Copyright Cases," P.2445.

Connected to that argument is the point made by some critics that it would be bad to give a limited group of players, whether governmental or corporate, a lot of control over what happens in the public sphere without mechanisms for judicial scrutiny. It could hamper people from taking part in the meaning making process and social dialogue that is central to liberal democracy.⁹⁴

Privacy is also important in this context. It can be considered as a legal right connected to due process of law (a safeguard), but also as a value in itself, growing in importance because of technological developments. Because of this, it deserves special attention. Privacy rights protect us from the unlawful interference in our private life by other parties (typically, but not exclusively, the state), unless there are compelling reasons to do so. Privacy rights extend to family, home, possessions, communications, reputation, and honor.⁹⁵ New technologies have made privacy breaches incredibly easy, even where it concerns the most personal human behaviors. Privacy protects us from harm and is an essential aspect of our autonomy.⁹⁶ Moor argues that privacy is also an expression of another core value: security. Societies have become larger, more interactive, and less intimate. We therefore need protection from strangers with potentially bad intentions. Especially in a culture that is highly computerized.⁹⁷

Copyright enforcement potentially impacts privacy in at least two ways; increased surveillance and the loss of anonymity.⁹⁸ Some imply a tradeoff exists between fundamental rights and copyright. In fact, it has brought Pirate party head Christian Engstrom to say that "As long as there are ways for citizens to communicate in private, they will be used to share copyrighted materials."⁹⁹

Opponents of enforcement point to mistakes in large-scale enforcement

NGOs, like the European Digital Rights initiative (EDRI) and the Electronic Frontier Foundation (EFF), have repeatedly pointed towards mistakes made during large-scale enforcement. The EFF has pointed towards problems with the detection of copyright infringement online,¹⁰⁰ which led to the takedown of book reports,¹⁰¹ academic expressions and public domain films.¹⁰² In similar fashion, sites like Torrentfreak highlight other

⁹⁴ Niva Elkin-Koren, "A democratic approach to copyright in cyberspace," *Cardozo arts & entertainment* 14 (1996): 215. P.218.

⁹⁵ John S. Gibson, *Dictionary of International Human Rights Law*, (Lanham, Md.m & London: The Scarecrow Press, Inc. 1996). P.121.

⁹⁶ James H. Moor, "Towards a theory of privacy in the information age," *Computers and society* (1997): 27-32. P.28-29

⁹⁷ Moor, "Towards a theory of privacy in the information age." P.28-29 .

⁹⁸ Bridy, "Graduated Response American Style".

⁹⁹ Christian Engstrom, "Copyright law turns kids into criminals - Reform will enrich artists and the public," *New Europe Online* (October 1, 2011), <http://www.neurope.eu/blog/copyright-law-turns-kids-criminals-reform-will-enrich-artists-and-public>

¹⁰⁰ "EFF Calls Foul on Robo-Takedowns," *Electronic Frontier Foundation* (March 6, 2012), <https://www.eff.org/press/releases/eff-calls-foul-robo-takedowns>.

¹⁰¹ Mike Masnick, "A Glimpse Of The Future Under SOPA: Warner Bros. Admits It Filed Many False Takedown Notices," *Techdirt* (November 10, 2011), <http://www.techdirt.com/articles/20111110/10135116708/glimpse-future-under-sopa-warner-bros-admits-it-filed-many-false-takedown-notices.shtml>.

¹⁰² "Unsafe Harbors: Abusive DMCA Subpoenas and Takedown Demands," *Electronic Frontier Foundation* (September 25, 2003), <https://www.eff.org/wp/unsafe-harbors-abusive-dmca-subpoenas-and-takedown-demands>.

abberations. It reported, for example, that the makers of the movie *Hurt Locker* sued 24,583 people. One of them was a dead man.¹⁰³ Another was a hockey stadium.¹⁰⁴ Other rights holders filed a John Doe lawsuit against a blind man for downloading pornography.¹⁰⁵ And when seven record labels sued Sarah Ward based on just KaZaA screenshots and Comcast's disclosure of her name and address in response to a subpoena, it turned out the accused only had an old Macintosh computer incapable of running KaZaA software.¹⁰⁶ Techdirt repeatedly blogs about these cases, like when a photographer put one of his photos on his own website, and that photo was taken down for copyright infringement.¹⁰⁷ A study by the University of Washington in 2008 revealed that the methods used by anti-piracy companies meant that any user can be framed for copyright infringement today, even if they do not have P2P. The researchers could generate DMCA takedown notices for printers.¹⁰⁸

Critics of the new enforcement strategies also point to rights holders who, in their view, have abused copyright for financial and other reasons.¹⁰⁹ They repeatedly write about abuse by, for example, politicians,¹¹⁰ governments,¹¹¹ companies,¹¹² and the church of Scientology¹¹³. The most extreme example of abuse is that terrorists used a DMCA claim to get the identity of an anti-Islamic YouTuber to threaten him.¹¹⁴

According to these groups, these examples of negative side effects of large-scale enforcement are symptomatic of a larger problem: the lack of safeguards threatens other

¹⁰³ Ernesto, "Anti-piracy lawyers sue dead person," *Torrentfreak* (August 26, 2011), <http://torrentfreak.com/anti-piracy-lawyers-sue-dead-person-110826/>.

¹⁰⁴ Mike Masnick, "Hurt Locker file sharing lawsuit lists hockey stadium IP address," *Techdirt* (September 28, 2011), <http://www.techdirt.com/articles/20110928/02302616122/hurt-locker-file-sharing-lawsuit-lists-hockey-stadium-ip-address.shtml>.

¹⁰⁵ Keegan Hamilton, "Porn, Piracy, & BitTorrent," *Seattle Weekly News* (August 10, 2011), <http://www.seattleweekly.com/2011-08-10/news/porn-piracy-bittorrent/>.

¹⁰⁶ "Unsafe Harbors: Abusive DMCA Subpoenas and Takedown Demands," *Electronic Frontier Foundation* (September 25, 2003), <https://www.eff.org/wp/unsafe-harbors-abusive-dmca-subpoenas-and-takedown-demands>.

¹⁰⁷ Mike Masnick, "GoDaddy Takes Down Entire Site Of Copyright Attorney/Photographer Over Bogus DMCA Claim," *Techdirt* (November 21, 2011), <http://www.techdirt.com/articles/20111119/01060316841/godaddy-takes-down-entire-site-copyright-attorney-photographer-over-bogus-dmca-claim.shtml>.

¹⁰⁸ Michael Piatek, Tadayoshi Kohno, Arvind Krishnamurthy, "Challengers and Directions for Monitoring P2P File Sharing Networks – or – Why my printer received a takedown notice," *HotSec* (2008).

¹⁰⁹ Timothy, "YouTube Identifies Birdsong As Copyrighted Music," *Slashdot* (February 26, 2012), <http://yro.slashdot.org/story/12/02/26/2141246/youtube-identifies-birdsong-as-copyrighted-music>.

¹¹⁰ Ryan Witt, "GOP works to cover up video they previously published on Internet," *Examiner.com* (March 30, 2011), <http://www.examiner.com/political-buzz-in-national/gop-trying-desperately-to-cover-up-video-they-previously-published-on-Internet>.

¹¹¹ Mike Masnick, "UK Trying To Censor Parody Video About The 2012 Olympics," *Techdirt* (February 29, 2012), <http://www.techdirt.com/articles/20120229/04115017911/uk-trying-to-censor-parody-video-about-2012-olympics.shtml>.

¹¹² *OPG v. Diebold*, 337 F. Supp. 2d 1195 (N.D. Cal. 2004),

¹¹³ "Unsafe Harbors: Abusive DMCA Subpoenas and Takedown Demands," *Electronic Frontier Foundation* (September 25, 2003), <https://www.eff.org/wp/unsafe-harbors-abusive-dmca-subpoenas-and-takedown-demands>.

¹¹⁴ Samzenpus, "Terrorists Used False DMCA Claims To Get Personal Data of Anti-Islamic Youtuber," *Slashdot* (November 6, 2014), <http://yro-beta.slashdot.org/story/14/11/06/0435252/terrorists-used-false-dmca-claims-to-get-personal-data-of-anti-islamic-youtuber>.

values. Techdirt has repeatedly¹¹⁵ asserted that some copyright enforcement procedures lack due process.¹¹⁶ That is why they view many of these strategies as disproportional.

NGOs have therefore lobbied for more user rights. Art. 19, a global civil society group for freedom of expression has in the past appealed for a notice and takedown regime involving judicial review.¹¹⁷ In the debates on the e-commerce directive in the EU on the role of intermediaries in copyright enforcement, EDRI warned that an increased role for intermediaries jeopardized due process and other human rights.¹¹⁸ La Quadrature du Net, a French digital rights NGO, calls the French HADOPI law a defeat for the rule of law, in particular because of its erosion of due process rights and the presumption of innocence.¹¹⁹ During EU discussions on the Telecoms package, which included increased pressure by rights holders to include stringent enforcement mechanisms like graduated response, La Quadrature lobbied extensively for the inclusion of procedural safeguards (which would come to be known as 'amendment 138').¹²⁰ The EFF warned against the adoption of graduated response procedures for due process reasons, after the French constitutional court had struck down the first HADOPI law for delegating Internet access control to non-judicial authorities.¹²¹

An additional argument by EDRI is that having little safeguards would be bad for legal certainty, also in the market.¹²² Barriers to entry and transaction costs are higher because of legal uncertainty. It is often unclear which rights have to be cleared, and who the actual rights owners are. For amateurs, failing to do so could result in massive fines.¹²³

Proponents of more enforcement point to societal costs of infringement

The industries in turn argue that they cannot innovate without having adequate protection of their rights. Proponents of intensified enforcement point to the cost of infringement, which they estimate to be in the billions. Bridy for example mentions that the language used by the copyright industries has been effective at framing infringement as a large-scale problem, and this language has seeped through the debates and case law. Copyright infringement happens on a "massive scale," costs "billions of dollars" and "countless

¹¹⁵ Mike Masnick, "ICE Finally Admits It Totally Screwed Up; Next Time, Perhaps It'll Try Due Process," *Techdirt* (February 21, 2011), <https://www.techdirt.com/articles/20110220/17533013176/ice-finally-admits-it-totally-screwed-up-next-time-perhaps-itll-try-due-process.shtml>

¹¹⁶ Mike Masnick, "Homeland Security Won't Even Admit Whether Or Not It Seized Moo.com, Taking Down 84,000 Innocent Sites," *Techdirt* (February 17, 2011), <https://www.techdirt.com/articles/20110217/00082213144/homeland-security-wont-even-admit-whether-not-it-seized-moocom-taking-down-84000-innocent-sites.shtml>

¹¹⁷ "European Commission: Freedom of Expression Needs Better Protection in Digital Communications," *Art 19 Press Release* (9 November 2010), www.article19.org/pdfs/press/european-commission-freedom-of-expression-needs-better-protection-in-digital.pdf

¹¹⁸ Meryem Marzouki, "E-Commerce directive: ensure freedom of expression and due process of law," *EDRI Website* (November 18, 2010), <http://history.edri.org/book/export/html/2445>

¹¹⁹ "Hadopi 2 validated, a defeat for the Rule of Law," *la Quadrature du Net website* (Oct 24, 2009), <https://www.laquadrature.net/en/hadopi-2-validated-a-defeat-for-the-rule-of-law>

¹²⁰ Monica Horten, *The Copyright Enforcement Enigma, Internet Politics and the 'Telecoms Package'*, (palgrave MacMillan, 2012), P.153-164.

¹²¹ Danny O'Brien, "France declares three strikes unconstitutional," *Electronic Frontier Foundation* (June 10, 2009), <https://www.eff.org/deeplinks/2009/06/three-strikes-dead-in-france>

¹²² Meryem Marzouki, "E-Commerce directive: ensure freedom of expression and due process of law," *EDRI website* (November 18, 2010), <http://history.edri.org/book/export/html/2445>

¹²³ Lessig, *Free culture*.

jobs.”¹²⁴ The RIAA (Recording industry association of America) refers to illegal downloading as “stealing.”¹²⁵ The MPAA (Motion Picture Association of America) strongly encourages everyone to protect and enforce intellectual property rights.¹²⁶ Section 1.3 already described the costs associated with infringement and in following chapter we will come back to the academic discussion on this topic.

Michael O'Leary, of the Movie Picture Association of America (MPAA), in a testimony for the House Judiciary Committee on the proposed SOPA law, said that the new law was about saving jobs. He also mentioned the amount of jobs supported by this industry.¹²⁷ The deputy trade representative also said of new initiatives like the ACTA treaty, that “We believe that ACTA will help protect the intellectual property that is essential to American jobs in innovative and creative industries.”¹²⁸

One of the obstacles rights holders face is a lack of public support for regulation and enforcement. Some write that this is because citizens have no direct personal interest in the protection that copyright offers. They will not be entitled to remuneration on the basis of their creative expressions. Citizens do feel an intrusion into their personal freedoms through enforcement. Meanwhile, public support for copyright is further diminished by the image that these norms only serve large companies, like Disney and Universal.¹²⁹

Rights holders have sought to make clear that infringement is intrinsically wrong and harmful. They have tried to shift the norms in this debate. According to Alain d’Astous, associations and recording companies have turned to a number of communication strategies to convince consumers not to engage in piracy behavior.¹³⁰ First of all, they have tried to show that there are negative personal consequences tied to piracy. By suing individual users, they have shown that pirating music on the web can get you into trouble with the law. They view regulation and litigation as part of an ‘education’ campaign. According to RIAA lawyer Cary Sherman, “Enforcement is a tough love form of education.”¹³¹ They also aim to make warning and education part of the graduated response procedure in the US.¹³²

Proponents of enforcement claim it can be done in accordance with human rights

Rights holders, the White House and EU representatives also claim intensified enforcement can be done in accordance with human rights. During the debates on recent proposals like SOPA and ACTA, rights holders like the MPAA and the US Chamber of Commerce claim they follow the same rules of civil procedure you would find in an ordinary trial. In their view,

¹²⁴ Bridy, “Is Online Copyright Enforcement Scalable?” P.704-706.

¹²⁵ “For students writing papers,” *RIAA website*, <http://www.riaa.com/faq.php>, last visited on 20-9-2011

¹²⁶ “Types of content theft,” *MPAA website*, <http://www.mpa.org/contentprotection/types-of-content-theft>, last visited on 20-9-2011.

¹²⁷ Greg Sandoval, “Hollywood's SOPA testimony links job loss to piracy,” *CNET* (November 16, 2011), <http://www.cnet.com/news/hollywoods-sopa-testimony-links-job-loss-to-piracy/>

¹²⁸ Ambassador Miriam Sapiro, “*The Role of the Anti Counterfeiting Trade Agreement (ACTA)*,” *Official office of the U.S. Trade Representative response, We the People*, <https://petitions.whitehouse.gov/response/role-anti-counterfeiting-trade-agreement-acta>

¹²⁹ Dirk Visser, “De interreectuele eigendom van het Grootkapitaal.” *AMI: tijdschrift voor auteurs-, media-en informatierecht* 2011 (2011): 2.

¹³⁰ Alain d’Astous et al., “Music Piracy on the Web – How effective are anti-piracy arguments? Evidence from the theory of planned behavior,” *28 Journal of Consumer Policy* 289 (2005). P. 289-290.

¹³¹ Steve Knopper, “RIAA will keep on suing,” *Rolling Stone* (June 9, 2005).

¹³² Greg Sandoval, “Exclusive: Top ISPs poised to adopt graduated response to piracy,” *CNET* (June 22, 2011), <https://www.cnet.com/news/exclusive-top-isps-poised-to-adopt-graduated-response-to-piracy/>

copyright enforcement targets illegal sites and people that infringe on copyright only and does nothing to harm legal uses of content and Internet users who are not sharing protected content.

Steven Tepp, a lawyer with the U.S. Chamber of Commerce, a U.S. lobby group supporting more copyright enforcement procedures says that opponents of enforcement are constantly misleading and scaring people to make their point.¹³³ He says that opponents engage in scare tactics and that every targeted site under SOPA will be offered due process.¹³⁴

The U.S. Copyright Office supports legislation like SOPA, calling it an essential tool in combating infringement. Maria Pallante, the director of the Office, stated that combating infringement "requires all key members of the online ecosystem, including service providers, search engines, payment processors, and advertising networks, to play a role in protecting copyright interests -- an approach I endorse... In my view, such tools are essential to stopping the economic devastation caused by rogue websites..." And: "there will be times when blocking access to websites may be the only quick and effective course of action and that providing this tool to the Attorney General is therefore a critical part of the equation. Likewise, I believe that search engines should be fully within the reach of the Attorney General and should be ordered in appropriate circumstances to dismantle direct hyperlinks that send unwitting consumers to rogue websites."¹³⁵

It is "beyond troubling to hear hyperbolic charges that this bill will open the floodgates to government censorship," said Rep. Mel Watt, a North Carolina Democrat, during a House Judiciary committee hearing.¹³⁶

On SOPA, the MPA has said in a testimony before congress, that it is narrowly defined to target only rogue websites, not the legitimate ones. They also explicitly mention that sufficient rules of due process would apply. They say "in fact, it provides foreign-based sites with exactly the same procedural protections afforded U.S. citizens under the Federal Rules of Civil Procedure. This includes requiring prosecutors to notify the site and its registrants or owners of their intent to act under the bill, and to notify any intermediary that may be ordered by the court to discontinue providing services to that site. As such, domain name owners or site operators would have every right to defend themselves in court should they choose to."

They also mention that: "equally strict standards would apply in cases where a content owner seeks to act to prevent online theft by a rogue site. Contrary to wild assertions bandied about by those who oppose this legislation, H.R. 3261 does not give content owners the power to shut down websites. The bill sets out a new voluntary notification process that encourages private, out-of-court solutions as the preferred means to efficiently and effectively protect against the enormous losses that result from content theft. Indeed, the bill contains provisions that will provide immunity for voluntary action against sites dedicated to the theft of U.S. property or sites that endanger public health. At the same time, the bill preserves the ability of rights holders to seek limited injunctive relief

¹³³ Declan McCullagh, "SOPA's most aggressive defender: U.S. Chamber of Commerce," *CNET* (November 30, 2011), <http://www.cnet.com/news/sopas-most-aggressive-defender-u-s-chamber-of-commerce/>

¹³⁴ Declan McCullagh, "Copyright bill controversy grows as rhetoric sharpens," *CNET* (October 31, 2011), <http://www.cnet.com/news/copyright-bill-controversy-grows-as-rhetoric-sharpens/>

¹³⁵ Declan McCullagh, "Copyright Office will endorse SOPA anti-piracy bill," *CNET* (November 15, 2011), <http://www.cnet.com/news/copyright-office-will-endorse-sopa-anti-piracy-bill/>

¹³⁶ Declan McCullagh, "SOPA bill won't make U.S. a 'repressive regime,' Democrat says," *CNET* (November 16, 2011), <http://www.cnet.com/news/sopa-bill-wont-make-u-s-a-repressive-regime-democrat-says/>

in the courts against a rogue website if intermediaries choose not to take action against a website. Rights holders must clearly show, as they would under Federal Rule of Civil Procedure 65, that immediate and irreparable injury, loss, or damage will result in the absence of timely action. Content owners that file frivolous or unsupported claims could face damages, including costs and attorneys fees.”¹³⁷

This reasoning also surfaces for other new enforcement procedures. On graduated response, rights holders assert that the real mitigation measures have judicial scrutiny, and that the other measures do not have the same amount of scrutiny but that this is reasonable because they are about education first.¹³⁸

On ACTA, the deputy trade representative of the White House says: “ACTA recognizes the importance of online privacy, freedom of expression and due process, and calls on signatories to protect these values in the course of complying with the Agreement.”¹³⁹ In Europe, some blame the media for simplifying the copyright enforcement provisions in the ACTA Treaty. They claim that the treaty would not rewrite the rules of liability.¹⁴⁰ European Commissioner Karel de Gucht has said: “ACTA is not an attack on our liberties, it is a defense of our livelihoods. This is because we do not have to modify any part of our internal legislation, the so-called *acquis communautaire*. What is legal today in the European Union will remain legal once ACTA is ratified. And what is illegal today will still remain illegal with ACTA,” (..) “Nothing changes in the eyes of the law. And since our freedoms are not threatened by our current laws, our freedoms will not be threatened by ACTA.”¹⁴¹

1.5 Research question

Who is right? To offer policymakers guidance on this question, this dissertation aims to make an empirical contribution to the academic and policy literature through a comparative empirical study of the effects of large-scale enforcement on procedural safeguards. The need for a more empirical basis for the debate is widely recognized. In 2013, the US National Research Council released a report on the status quo of research on copyright policy at the time. In it, they identified new avenues for research. Among other things, they called for more empirical data and research on the enforcement of copyrights.¹⁴²

Previous research that explored this avenue has focused on a specific copyright enforcement procedure. For example, there has been research on the practice of notice and

¹³⁷ Greg Sandoval, “Hollywood's SOPA testimony links job loss to piracy,” *CNET* (November 16, 2011), <http://www.cnet.com/news/hollywoods-sopa-testimony-links-job-loss-to-piracy/>

¹³⁸ Nate Anderson, “Major ISPs agree to “six strikes” copyright enforcement plan,” *ArsTechnica* (July 7, 2011), <http://arstechnica.com/tech-policy/2011/07/major-isps-agree-to-six-strikes-copyright-enforcement-plan/>

¹³⁹ Ambassador Miriam Sapiro, “The Role of the Anti Counterfeiting Trade Agreement (ACTA),” *Official office of the U.S. Trade Representative response, We the People*, <https://petitions.whitehouse.gov/response/role-anti-counterfeiting-trade-agreement-acta>

¹⁴⁰ “Brussels denies rumours of secret anti-piracy treaty,” *Euractiv* (February 4, 2010), <http://www.euractiv.com/infosociety/brussels-denies-rumours-secret-anti-piracy-treaty>

¹⁴¹ Karel de Gucht, “ACTA: Making the right choice,” *speech for the European Commission* (June 20, 2012), http://europa.eu/rapid/press-release_SPEECH-12-477_en.htm

¹⁴² Stephen A. Merrill and William J. Raduchel, eds. *Copyright in the Digital Era: Building Evidence for Policy* (National Academies Press, 2013).

takedown in the U.S.¹⁴³ These studies have been incorporated in the chapters dealing with specific enforcement procedures.

The contribution of this dissertation is empirical, rather than performing legal analysis. The case studies refer to legal analyses to provide the legal background of enforcement procedures, but the research does not intend to propose new legal interpretations.

All empirical research is bounded in time. The empirical part of this research has been conducted between 2004 and 2014. This unfortunately, but inevitably, means that some of the very recent empirical work is not included in the case studies, such as those on the practical application of enforcement procedures¹⁴⁴ and a comparative study of several enforcement mechanisms.¹⁴⁵

With its focus, this research adds to existing studies by providing empirical evidence of the practical effects on procedural safeguards of eight enforcement strategies in six countries, providing a uniquely broad comparative perspective and shedding light on the empirical reality of copyright enforcement and the relationship between scale, severity and safeguards. This brings us to the following overall research question :

“How does large-scale copyright enforcement on the Internet influence procedural safeguards like due process and fair trial, what are its costs and its effectiveness, and what do these findings imply for public policy?”

To answer these questions, the study has been divided in two parts. The first part provides the background against which this research has been done and operationalizes the question into an empirical research design. The second part offers the empirical work through case studies and synthesizes the main findings into an answer to the research question.

Part I will first describe infringement (chapter 2). The main problem copyright enforcement strategies try to solve is that of rampant copyright infringement. How big is this problem? Rights holders have proceeded to frame the problem as large-scale, but what exactly constitutes large-scale? If enforcement strategies target specific behavior, how is copyright infringement currently taking place? What does research say about the damages of copyright infringement? It will then describe enforcement procedures (chapter 3). Copyright enforcement strategies might influence different variables, but how do copyright enforcement strategies differ? Afterwards it will describe the theoretical framework and research design (chapter 4). Although the discussion on deterrence, costs and safeguards is done in the political and public debate, what theoretical predictions can be made on these relations? How can we best evaluate these claims?

Part II will describe the empirical research. Two cases deal with the direct pursuit of file sharers in the US and the UK (chapters 5 and 6). Two cases deal with graduated response procedures in France and Ireland (chapter 7 and 8). Two cases deal with notice and takedown procedures as applied by Google and in the Netherlands (chapter 9 and 10). Two

¹⁴³ Jennifer Urban and Laura Quilter, "Efficient Process or 'Chilling Effects'? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act," *Santa Clara Computer and High Technology Law Journal* 22 (2006): 621.

¹⁴⁴ Jennifer M. Urban, Joe Karaganis and Brianna L. Schofield, "Notice and Takedown in Everyday Practice," UC Berkeley Public Law Research Paper No. 2755628 (March 29, 2016), Available at SSRN: <http://ssrn.com/abstract=2755628>

¹⁴⁵ T. McGonagle, "Study of Fundamental Rights Limitations for Online Enforcement through Self-Regulation." Institute for Information Law (IViR), University of Amsterdam, forthcoming.

cases will describe procedures aimed directly at the supply of infringing content in the US and in Spain (chapter 11 and 12). Chapter 13 will provide the analysis and discussion, followed by limitations to this research, a summary and bibliography.

PART I: BACKGROUND

2. LARGE-SCALE INFRINGEMENT

2.1 Introduction to this chapter

This chapter shows how new Internet-based technologies have undermined the protection of copyright on entertainment products and how these technologies have facilitated large-scale copyright infringement. It will show that there are multiple ways through which users can infringe on copyrights online. After that, the chapter will show that there are different actors involved.

The chapter will then go into the scale of infringement. What constitutes large-scale? The chapter will show how infringement currently happens on a large scale. It will show the different incentives for infringement. Although infringement has happened on a large scale, the exact effect on the entertainment market is unclear. In a segment on the economic impact of infringement, the chapter will show that the market has adapted to some changes and seems to be doing well in some areas.

2.2 Copyright infringement

Copyright is infringed when the exclusive rights copyrights grant are exercised without permission of the copyright holder while the limitations included in copyright law don't apply. Copyrights give the creator or author of an expression a set of exclusive rights, which can be categorized in two dimensions: Moral rights give the author the right to take actions to maintain the personal link between himself and the work. Economic rights allow the author or rights owner the rights to reap financial benefits from his creations.¹⁴⁶

Copyright protection is however not absolute; it is subject to numerous limitations to benefit the general public. First of all, the protection is not extended to certain categories of work. For example, in most countries no copyright protection is granted to laws and court decisions. Another limitation is that certain free uses are allowed, like quoting from copyright protected works, use of protected works in education, or use for news reporting. In some countries there are laws that allow for free reproduction, if the work is only for personal, private and non-commercial use. In the US, copyrights are regulated in such a way that they balance individual rights (the right of the author) with societal rights or the 'general good', such as the value of free information. That is why fair use and fair dealing are permitted as they benefit the public, without sacrificing the creators' rights. This also allows the use of works without the authorization of the rights holder, limited to some requirements. In Europe there is no broad exception like fair use, but a category of exceptions that sums up uses that are allowed. Although the roots of the exceptions differ, they are broadly similar in practice.¹⁴⁷

A somewhat different limitation is the use of non-voluntary licensing. This means that in some cases third parties can use the work of creators without their authorization, but only if those third parties pay compensation.¹⁴⁸

¹⁴⁶ "Enforcement of rights," *World Intellectual Property Organisation*, http://www.wipo.int/freepublications/en/intproperty/909/wipo_pub_909.html#enforcement (last visited Jan. 22, 2013).

¹⁴⁷ "Enforcement of rights," *World Intellectual Property Organisation*.

¹⁴⁸ "Enforcement of rights," *World Intellectual Property Organisation*.

Copyrights exist from the moment of expression. Originally, registration was required, but legislators reversed this provision in 1978. Copyrights last for a long time. The duration is provided for in national law, but it is generally 50 years after the death of an author. Some countries, like the US, have extended the term to 70 years after the death of an author.¹⁴⁹

Another limitation is what is referred to as the ‘first sale doctrine,’ this means that a copyright owner never has complete control over all possible uses of his work.¹⁵⁰ If you buy a book, it is not up to the author to decide how many times you read it, and whether you choose to read the last chapter first. The rights cover only the first sales of the tokens containing the expression, and protect against appropriation of the types for all but a limited number of uses.

Moral rights always belong to the original author of the work, but economic rights can be transferred. This happens through assignment, which means the ownership of the rights is transferred, or through licensing, which means the rights owner transfer the performance of acts for a specific period of time and for a specific purpose. After transfer, the original owner of the right can collect royalties, a payment based on the use by the third party. Licensing can take the form of the collective administration of rights, which means a single entity gains the exclusive licenses from authors and other rights holders, so it can act on their behalf in for example collecting remuneration, or in preventing or detecting infringement.¹⁵¹

Related rights are copyright-like rights, and are the rights granted to protect the legal interests of certain persons and legal entities that contribute to the creation of works or making the work available to the public. This means they protect performers, broadcasting organizations, or producers of phonograms. Related rights are similar to copyright, and for example allow related rights holders the right to prevent communication to the public without consent, usually last for a shorter period of time (20 years after the recording is made or the performance took place for example), and are also subject to limitations.¹⁵²

In summary, copyright infringement means that the copyright protected work is used without authorization or license by the rights holder, which means reproducing the work (copying), performing, distributing it, public performance, broadcasting or communication to the public, translation into other languages or making derivative works without consent, or without falling under one of the exceptions or fair use provisions specified in national copyright law.¹⁵³

2.3 The Internet facilitates copyright infringement

Internet-based technologies have undermined the protection of copyright on cultural products. Copyright infringement through new technologies is off course nothing new. People were copying music illegally since the 1960s using cassette tapes and in the 1980’s by videotaping to copy broadcasts and movies. Yet Internet piracy is by far the biggest challenge to existing industries. It grew massively in the mid 1990's because of affordable CD burners and the Internet in conjunction with digitalization (in particular the mp3 file format

¹⁴⁹ “Enforcement of rights,” *World Intellectual Property Organisation*.

¹⁵⁰ Lessig, *Free culture*. P.62.

¹⁵¹ “Enforcement of rights,” *World Intellectual Property Organisation*.

¹⁵² “Enforcement of rights,” *World Intellectual Property Organisation*.

¹⁵³ “Enforcement of rights,” *World Intellectual Property Organisation*.

for compressing digital music).¹⁵⁴ Piracy started in the Internet Relay Chat (IRC) groups, where users could communicate in private.¹⁵⁵

According to the 'digital dilemma', a report prepared by the Computer Science and Telecommunications Board and the USA National Research Council, new technologies put pressure on copyright in a number of ways. In particular, three technological innovations altered the way we access and use information: digitalization, the incredible growth of computer networks, and the creation of the World Wide Web.

Analog technology records sound waves or video waves in their original form, and translates them into electronic pulses. Digital technology samples the analog wave, and turns that wave into numbers that are stored in a digital device. This video or audio data are translated in a series of "1"s and "0"s. This provides many benefits: it is easier to store and compress information. An analog CD allows for around 74-80 minutes of music, whereas a CD that contains MP3 files¹⁵⁶ that can be played on a computer allows for around 480 minutes of mp3 music.¹⁵⁷ Copying digital information is easy and inexpensive. A digital copy can be as good as its original, so having access to digital information can assure perfect reproduction of an infinite number of copies.¹⁵⁸

This development liberated information from its physical carrier or medium. It means that information can flow through networks without the need for a physical entity or token to carry that information.¹⁵⁹ This put pressure on business models that depended on the sale of those tokens, which were an important source of income in the music (CDs) and movie business (DVDs).

Networks connect our computers, and allow for rapid and inexpensive distribution and reproduction of information. This also lowers the barriers for piracy. Getting access to information means that it can be freely distributed to an unlimited amount of people connected to the network.¹⁶⁰ Distribution happens through the click of a mouse and can reach the outskirts of the world within seconds.¹⁶¹

Consequently, the web provides the infrastructure on which computers can exchange, organize and publish information. This information can in turn be scanned for information of interest, and more information can be put on the web.¹⁶² The web also makes the tools for replication and distribution available to all users.¹⁶³ This has consequences for traditional modes of business, as it allows for more direct contact between creators and consumers, and allows for the cutting out of 'middlemen'. It strips some costs, like distribution costs, but it can also create new costs, like online advertising.¹⁶⁴

¹⁵⁴ Adrian Adermon & Che-Yuan Liang, "Piracy, Music, and Movies: A Natural Experiment," *Working Paper Series 13, Center for Fiscal Studies, Uppsala University* (2010). P.5.

¹⁵⁵ Alexander Peukert, "Why Do 'Good People' Disregard Copyright on the Internet?" in: *Criminal Enforcement: A Blessing or a Curse for Intellectual Property?* Ed: Cristophe Geiger (Edward Elgar Publishing, 2012). P.2.

¹⁵⁶ MP3's are digital representations of music that have comparable quality to music on a CD.

¹⁵⁷ "How much MP3 music fits on a CD?," *Answers.com*, http://wiki.answers.com/Q/How_much_mp3_music_fits_on_a_CD, last visited on 25-5-2011.

¹⁵⁸ National Research Council (US). Committee on Intellectual Property Rights, et al, *The Digital Dilemma: Intellectual Property in the Information Age*, (National Academy Press, 2000). P.32.

¹⁵⁹ National Research Council (US). *The Digital Dilemma*. P.32.

¹⁶⁰ National Research Council (US). *The Digital Dilemma*. P.38.

¹⁶¹ National Research Council (US). *The Digital Dilemma*. P.39.

¹⁶² National Research Council (US). *The Digital Dilemma*. P.39.

¹⁶³ National Research Council (US). *The Digital Dilemma*. P.40.

¹⁶⁴ National Research Council (US). *The Digital Dilemma*. P.41-42.

According to Lessig, it was originally also difficult to regulate the Internet, because to regulate constituents, “you need to know (1) who someone is, (2) where they are, and (3) what they’re doing. But because of the way the Internet was originally designed (..), there was no simple way to know (1) who someone is, (2) where they are, and (3) what they’re doing. Thus, as life moved onto (this version of) the Internet, the regulability of that life decreased. The architecture of the space—at least as it was—rendered life in this space less regulable.”¹⁶⁵ This applies directly to copyright: If a user infringes on copyrights, enforcing them requires that rights holders can identify the infringing user that is infringing,¹⁶⁶ and that they can take the social context of content access or use into account. It is almost impossible to identify whether use falls under ‘plain use’, copyright exceptions or the fair use clause.¹⁶⁷ The first sale doctrine can also not apply, as selling a digital good once, makes it available for everyone else, because of its digital nature.¹⁶⁸

The worldwide web adds additional problems by *being worldwide*. Copyright infringement can transcend national boundaries, so it is sometimes unclear which jurisdiction applies to a case.¹⁶⁹ Furthermore, all countries have different perceptions of laws, views and culture with regards to information and copyright.¹⁷⁰

Apart from those technological innovations, the widespread adaptation of those new technologies as a part of everyday life added to the increasing pressure on copyright.¹⁷¹ The Internet has grown at an incredible rate. It has doubled in size every fourteen months, since its conception approximately forty years ago.¹⁷² A growth rate like that can lead to scaling problems, but the founders of the Internet solved this by decentralizing the transmission and distribution of data as packets through the entire network. This makes data transmission more efficient, carried out by each machine in the network, instead of flowing through one central hub, like in the case of the original telephone.¹⁷³

Digitalization changed the economics and character of reproduction, and dramatically lowered the traditional and economic boundaries to infringe on copyrights, and the worldwide Internet and its rapid adoption made spreading this information easy. This changed the economics of piracy: as a cost structure, copyright works have high sunk development costs and low costs of reproduction and dissemination. ICT lowers costs of reproduction and dissemination. The costs of creating new works also fall, but not as much.¹⁷⁴

Although initially mainly music was pirated, a general increase in Internet speed during the 2000s together with the development of better video encoding techniques made it possible to share movies and TV shows.¹⁷⁵ This speeding up of network connections

¹⁶⁵ Lessig, *Code, Version 2.0*. P.23.

¹⁶⁶ National Research Council (US). *The Digital Dilemma*. P.49.

¹⁶⁷ National Research Council (US). *The Digital Dilemma*. P.49.

¹⁶⁸ National Research Council (US). *The Digital Dilemma*. P.51.

¹⁶⁹ National Research Council (US). *The Digital Dilemma*. P.49.

¹⁷⁰ National Research Council (US). *The Digital Dilemma*. P.54.

¹⁷¹ National Research Council (US). *The Digital Dilemma*. P.28.

¹⁷² Bridy, “Is Online Copyright Enforcement Scalable?” P.697.

¹⁷³ Bridy, “Is Online Copyright Enforcement Scalable?” P.697.

¹⁷⁴ Christian Handke, Bodo Balazs, Joan-Josep Vallbé, “The value of online licenses for recorded music,” *Paper presented at Annual Congress of the Society for Economic Research on Copyright Issues*, (2014). P.2

¹⁷⁵ Adrian Adermon and Che-Yuan Liang, “Piracy, Music, and Movies: A Natural Experiment,” *Working Paper Series 13, Center for Fiscal Studies, Uppsala University* (2010). P.5.

happened quickly. Broadband reached 100 million users in June 2004,¹⁷⁶ and went up to 221 million in June 2007, and was at 357.6 million fixed broadband subscribers in 2014.¹⁷⁷ The next generation of broadband is so fast, that it allows users to send or receive 200 mp3 music files in five minutes, an entire Star Wars DVD in 3 minutes and all the works by Charles Dickens in less than 10 minutes.¹⁷⁸

2.4 Different methods of large-scale copyright infringement online

As infringement was made easy, large-scale infringement took off. The Internet has been remarkable at scaling up its network. The creators of the Internet decentralized data transmission by distributing data in tiny packets through the network. This makes transmission less susceptible to interruption, as data does not travel through one single hub. Through nodes, the Internet can expand from any point in the network, which in turn increases its ability to grow. “The bigger it gets, the bigger it can keep getting.”¹⁷⁹ But this ability to scale up the network has also allowed the network to scale up copyright infringement.

There are many different ways to infringe on copyrights online. Harris interactive conducted a survey in 2009 that “showed a net increase in the use of web-based or “non-P2P” methods during the last six months, with the biggest increases in use coming from overseas unlicensed MP3 pay sites (47%) and newsgroups (42%). Other significant rises included MP3 search engines (28%) and forum, blog and board links to cyber lockers¹⁸⁰(18%).”¹⁸¹

Especially the use of cyber lockers rose. In 2010, when Harris Interactive researched the knowledge of 5000 respondents of where they could download infringing content, 74% said P2P, but 66% said cyber lockers. When asked what the most popular way was to access infringing content, 80% said they used P2P, and almost 50% said they used cyber lockers.¹⁸² The IFPI had the same conclusion in its 2010 report (on 2009), which said that P2P file sharing was not diminishing, but access to infringing music through other platforms was “growing considerably.”¹⁸³

Cisco systems predicted that although P2P traffic would keep growing through 2014, it would drop to 17% of total Internet traffic. File hosting traffic would grow much faster.¹⁸⁴ A study by Netnames, commissioned by NBCUniversal, shows that compared to 2011, in

¹⁷⁶ “OECD Broadband Statistics,” *OECD Website* (January 2005), see: <http://www.oecd.org/sti/broadband/oecdbroadbandstatisticsjune2005.htm>

¹⁷⁷ “OECD Broadband Statistics update,” *OECD Website* (July 2015), see: <http://www.oecd.org/sti/broadband/broadband-statistics-update.htm>

¹⁷⁸ Robin Hunt et al., *Copycats? Digital consumers in the online age, a CIBER report for the strategic advisory board for intellectual property policy* (University College London, May 2009), <http://ciber-research.eu/download/20090601-SABIP-main-1.pdf>

¹⁷⁹ Bridy, “Is Online Copyright Enforcement Scalable?” P.697.

¹⁸⁰ A cyber locker is a third party website that allows for the storage of files.

¹⁸¹ Harris Interactive, *Growing threat from illegal web downloads* (2009), <http://www.wipo.int/ip-outreach/en/tools/research/details.jsp?id=2479>.

¹⁸² BPI, The British Recorded Music Industry, *Digital Music Nation 2010* (BPI Limited 2010). P. 25: quoting a report called “Digital Music Survey 2010” by Harris Interactive.

¹⁸³ International Federation of the Phonographic Industry, *Digital Music Report 2010* (IFPI 2010).

¹⁸⁴ Cisco, “Cisco visual networking index: Forecast and methodology, 2009–2014,” *CISCO White paper* (2010).

2013 the traffic to cyber lockers fell by 8%, while the traffic to P2P sites grew by 31% and the traffic to streaming sites grew by 34%.¹⁸⁵

2.4.1 P2P Protocols

Like the Internet, P2P decentralizes by distributing workload. This makes it scale up infringement well. Instead of having one central server that serves individual clients which is susceptible to crashing by too much demand, the P2P system operates at the edges of the network, and scales up distribution by having every peer offer downloads. This means that an increase in peers increases the overall network capacity.¹⁸⁶

Different P2P protocols exist. Napster was the first one, and introduced peer-to-peer file sharing in 1999. It still had a central index server, which enabled users to search for files and connected peers for transfers, but this central server was not used to store or transfer data. It was so popular, that a year after its launch, almost one in four adult American Internet users said they downloaded music files, and more than half had used Napster to do so.¹⁸⁷ Worldwide, Napster had 64 million Napster users in 2001.¹⁸⁸ According to Mediametrix, Napster was the fastest software adoption in history.¹⁸⁹

After Napster was forced to shut down, different P2P protocols followed that enjoyed similar success. KaZaA, Napster's first successor, was downloaded by more than 230 million users worldwide.¹⁹⁰ Limewire is another P2P follow up that was forbidden by an American judge at the end of 2010, but a number of unofficial versions are still used.¹⁹¹ Other follow ups are eMule, a P2P client that works on the eDonkey network,¹⁹² Grokster, Morpheus and several regional protocols.

In terms of technology, later file sharing protocols, like FastTrack (which is used by Grokster and KaZaA) and Gnutella (used by Morpheus and Limewire) removed the central indexing server and further decentralized.¹⁹³ FastTrack used super nodes, mini-indexing servers that indexed content of nodes connected to them. Gnutella was completely distributed, so searches were routed through the network to all the different nodes until the file was located. This made Gnutella somewhat inefficient en meant longer search times.¹⁹⁴ But because these P2P follow-ups further decentralized by making every individual

¹⁸⁵ David Price, "Sizing the piracy universe", *Netnames* (September 2013), available at:

<https://copyrightalliance.org/sites/default/files/2013-netnames-piracy.pdf>

¹⁸⁶ Bridy, "Is Online Copyright Enforcement Scalable?" P.698-699.

¹⁸⁷ Amanda Lenhart and Susannah Fox, "Downloading free music: Internet music lovers don't think it is stealing," *Pew Internet & American Life Project* (2000), available at:

<http://www.pewInternet.org/reports/2000/downloading-free-music.aspx>

¹⁸⁸ Lynette White and Sean Elliot, "Large-scale Copyright Infringement: the Inevitable Consequence of the Digital Age," *Melbourne School of Engineering, Department of Computer Science and Software Engineering* (2001). P.8.

¹⁸⁹ "Napster usage quadruples," *CNN.com*, September 11, 2000, through: Alejandro Zentner, "Measuring the effect of file sharing on music purchases." *Journal of Law and Economics* 49.1 (2006): 63-90.

¹⁹⁰ Alejandro Zentner, "Measuring the effect of file sharing on music purchases." *Journal of Law and Economics* 49.1 (2006): 63-90.

¹⁹¹ Schermer and Wubben, *Feiten om te delen*. P.42.

¹⁹² Schermer and Wubben, *Feiten om te delen*. P.42.

¹⁹³ Bridy, "Is Online Copyright Enforcement Scalable?" P.699.

¹⁹⁴ Bridy, "Is Online Copyright Enforcement Scalable?" P.699.

computer acting as a search engine and an indexer, it was easier for the technology to respond to legal challenges.¹⁹⁵

The only problem with these P2P protocols was that they enabled free riding. Nodes could download content without uploading. This decreases content availability and puts pressure on the limited nodes that are uploading.¹⁹⁶

This problem was solved by the BitTorrent file-sharing protocol in 2001. The protocol made it impossible to download without uploading. Like FastTrack, BitTorrent is a hybrid P2P model. It is currently the most popular P2P protocol and a relatively quick way to exchange large files. File exchange happens through Torrents, small files that refer to other files. These .torrent files contain the information that is needed to start a download through BitTorrent. Users use indexing sites or torrent portals (websites) to find torrents quickly. Popular sites were Piratebay.org, Mininova and Isohunt.com at the time of this research. This is where users can also upload torrents, which can be searched on the site. Trackers facilitate traffic between different peers in the network. They make sure that users are referred to other users that share content through the .torrent file. Trackers are not necessarily operated by the same party as the indexing site. Peers in turn are the different participants in the network. The files are shared by peers partly or completely (called seeders), and downloaded by other peers (called leechers). Downloaders automatically are available for uploads, which make BitTorrents quick.¹⁹⁷ The collective of peers sharing a file is called a swarm. When leechers request files, they are immediately send a list of other peers (about twenty) currently transferring the same file. These neighbors are forced to share the file whilst downloading. The leecher then downloads the file from the seed and the other peers currently transferring the file. This means a leecher serves other peers whilst downloading. This makes data transfer fast and efficient. The only inefficiency that remains is that neighbors are named randomly, not based on the actual location. This over consumes bandwidth and can prolong download times. This has caused concerns for ISPs.¹⁹⁸

According to the PEW Internet tracking survey, in 2008, 15 percent of online American adults admitted to using BitTorrent.¹⁹⁹ Big champagne, a media measurement company, estimated in 2009 that around 200 million computers worldwide had P2P Applications installed, and the popular pirate bay torrent index site had more than 25 million unique peers that used their site to exchange files.²⁰⁰

In a study by the Internet Commerce Security Laboratory, the researchers found that in 2010 43,3% of all BitTorrent torrents were movies, 29,1% of them were TV shows, and 16,5% of them were music.²⁰¹ An IPOQUE study from 2009 painted a similar picture, saying that video was the most popular content in terms of volume and by number of files. Second

¹⁹⁵ Chukwuyere Ebere Izuogu, "The Interim Digital Britain Report, File Sharing and the Emerging Role of Internet Service Providers" (May 30, 2009). Available at SSRN: <http://ssrn.com/abstract=1601787>. P.4.

¹⁹⁶ Bridy, "Is Online Copyright Enforcement Scalable?" P.700.

¹⁹⁷ Schermer and Wubben, *Feiten om te delen*. P.41-42.

¹⁹⁸ Bridy, "Is Online Copyright Enforcement Scalable?" P.703-704.

¹⁹⁹ Princeton Survey Research Associates Int., "Spring Tracking Survey," *Pew Internet & American Life Project* (2008). Available at: http://www.pewInternet.org/files/old-media/Files/Questionnaire/Old/PIP_Broadband.2008.Topline.pdf.

²⁰⁰ Mary Madden, "The state of music online: Ten years after Napster," *Pew Internet & American Life Project* (2009). P.9.

²⁰¹ Robert Layton and Paul Watters, "Investigation into the extent of infringing content on BitTorrent networks," *Internet Commerce Security Laboratory* (April 2010), http://www.screenassociation.com.au/uploads/reports/bt_report_final.pdf

on BitTorrent is software (one third of the files), whereas on eDonkey this was audio. Software was on the rise compared to 2007.²⁰²

2.4.2 Usenet

Usenet is a synchronized global network meant for the exchange of text files and binary files (like music, movies and images). It is divided into a broad range of discussion groups that are referred to as 'newsgroups,' intended for public viewing. They are arranged around different subjects, which vary from technical issues to hobbies. Users can reach these newsgroups and interact with them by making contact with the newsgroup server. This is done through a newsreader, or specific applications. Most ISPs offer Usenet, but there are also commercial Usenet servers, like Giganews. They are popular, because they allow for newsgroups in which binary files are offered, and allow these binary messages to be on their servers for long periods of time. They usually also offer software and index, which make searching the network easier. An example of such index sites are Fill Threads Database (FTD) and NZB.²⁰³ At the time of this research, popular community-based websites that allowed members to link to content were warez-bb.org and Risloh.net. A popular newsgroup that allowed users to post something that others could download was Newzbin.com.

2.4.3 Cyber lockers

Cyber lockers are sites where consumers can temporarily store content. Through a download link (that sometimes requires a password) those files can be shared with other parties.²⁰⁴ Technologically speaking, one could argue that this is a step backwards from P2P networks, as cyber lockers have a centralized architecture, which makes them inefficient and an easy target for copyright holders.

Some of those cyber lockers require payment, which makes them seem like legal retailers, and some claim to sell licensed files only. However, this is often not the case. Examples of these sites are Mp3fiesta.com and legalsounds.com. Popular hosting sites at the time of this research were Rapidshare.com and Megaupload, which were taken down. Both were in the top 50 of the most visited websites in the world.²⁰⁵ Aggregators give users a convenient single location to search for content. They are cyber locker search machines or cyber locker index/link sites. At the time of this research, popular examples of this were filestube.com and neemp3.com.²⁰⁶

2.4.4 Streaming sites

A distribution model that at the time of this research was on the rise both legally and illegally was the streaming model. This means that infringing content can be made public through streaming sites. Most of these sites are indexed through linking sites, like Surfthechannel.com.²⁰⁷ Popular unauthorized streaming sites were Skreemr.com and Megavideo. Users can in turn use other programs to convert those streaming files into

²⁰² Hendrik Schulze and Klaus Mochalski, "Internet Study 2008/2009," *Ipoque Report* 37 (2009): 351-362. P.7.

²⁰³ Schermer and Wubben, *Feiten om te delen*. P.42.

²⁰⁴ Schermer and Wubben, *Feiten om te delen*. P.42.

²⁰⁵ "The top 500 sites on the web", <http://www.alexa.com/topsites>

²⁰⁶ Schermer and Wubben, *Feiten om te delen*. P.43.

²⁰⁷ Schermer and Wubben, *Feiten om te delen*. P.43.

content. Fetschmp3 for example allowed users to convert streaming files into mp3's. The most popular authorized streaming site is YouTube, although some of its content is unlicensed.

According to an IPOQUE study in 2010, streaming took over P2P users for video content and would grow more in the future.²⁰⁸ YouTube was at the time of this research the third most popular Web site.²⁰⁹

2.4.5 New "Darknet" technologies

The darknet is the collective noun for "a collection of networks and technologies used to share digital content (...)" which is "not a separate physical network but an application and protocol layer riding on existing networks."²¹⁰ Darknets stand for the diverse ways end users share music, like new P2P, but also CD and DVD copying, or key and password sharing on email and newsgroups. There are numerous new ways to share content on the rise. Because of new enforcement measures, users flock to more private P2P networks that protect their anonymity and stand less of a chance to be prosecuted than in the larger more public P2P networks. Examples are DirectConnect, WASTE, ALLPeers, Wuala, MUTE, Freenet, the U2P Network and JAP.²¹¹ These new networks also allow for more encryption, making it more difficult to identify its source. Other surveys reveal that users might use emails to start file sharing.²¹²

Apart from this Internet sharing, users may step towards hand to hand physical sharing. Users have incredible libraries of content on their computers (In Britain for example, the average teenager had 800 songs illegally copied from friends on his or her computer²¹³), and burning and exchanging content between friends is common. As the cost of digital storage media decreases, and its storage capacity increases, this form of file sharing could grow exponentially.²¹⁴ Apart from Moore's law, that processing power doubles every two years, there's such a thing called Kryder's law (same for storage capacity) and Nielsen's law (connectivity speed). In fact some said that 60 TB disk drives would be a reality in 2016. That is 10 million mp3 files.²¹⁵

Other examples that were on the rise: Tribler, a decentralized BitTorrent client, supposedly downloaded by the thousands.²¹⁶ RetroShare allows users to create a private and encrypted file-sharing network, where you can add friends by exchanging PGP certificates, and communication is encrypted by OpenSSL, so files that are downloaded always go through a friend.²¹⁷

²⁰⁸ Hendrik Schulze and Klaus Mochalski, "Internet Study 2008/2009," *Ipoque Report 37* (2009): 351-362. P.11.

²⁰⁹ "The top 500 sites on the web", <http://www.alexa.com/topsites>

²¹⁰ Peter Biddle et al., "The Darknet and the Future of Content Distribution," in: *Proceedings of the 2002 ACM Workshop on Digital Rights Management* (2002), <http://crypto.stanford.edu/DRM2002/darknet5.doc>.

²¹¹ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). Footnote 128.

²¹² Mary Madden and Lee Rainie, "Pew Internet Project Data Memo, Re: Music and Video Downloading beyond P2P," *Pew Internet & American Life Project* (2005).

²¹³ Dan Sabbagh, "Average Teenager's iPod Has 800 Illegal Music Tracks," *The Times* (June 16, 2008).

²¹⁴ Electronic Frontier Foundation, *RIAA vs. The People: Five Years Later* (2008).

²¹⁵ Lucas Mearian, "60TB disk drives could be reality in 2016," *Computerworld* (May 22, 2012), http://www.computerworld.com/s/article/9227382/60TB_disk_drives_could_be_a_reality_in_2016

²¹⁶ "Tribler Usage Statistics based on Dispersy (ALPHA)", *Tribler website* (November 23, 2014), available at: <http://statistics.tribler.org/>

²¹⁷ "Download Retroshare," *Retroshare website*, <https://retroshare.github.io/index.html>.

2.5 Players involved in copyright infringement online

According to consulting firm Considerati, there are a number of players involved with copyright infringement online. I have taken their overview as the standard, and have supplemented it with other information.

2.5.1 'The scene'

'The scene' or 'Warez scene' is a set of groups that have as their main goal the spread of content. They are underground communities that specialize in distribution of copyrighted material, in cracking software, and in creating circumvention tools. They view cracking software as a challenge.²¹⁸

They have no central leadership, central location or organizational features, but consist of groups with their own rules and procedures that are especially geared towards content categories. There is hardly a financial incentive, groups are in competition to get content released as quickly as possible.²¹⁹

The scene originally took form at The Massachusetts Institute of Technology (MIT) during the end of the nineteen-seventies. They were a so called virtual society, aimed mostly at games at first. Software companies started calling this underground hacker movement 'pirates', and the most notorious hang out was called 'pirate's harbor.'²²⁰ In the current day and age, they have become more known, and there is even a TV show that focuses on their activities in a dramatized way, called 'the scene.'²²¹

Although the scene has been big, normal downloaders hardly get into contact with them. Someone affiliated with the scene will get his or her content from a source, which can be something straight out of a production studio, release that to a release group, which in turn is delivered to a top site. Topsites are large websites where all files are spread. After the upload, they announce it in the topsite IRC, and on other websites. In 2010 there were about 100 different active groups and 100 topsites worldwide, which accounted for 500 new releases each day.²²² Couriers eventually take the content from the top site to FTP sites, Usenet, or P2P.²²³

According to Cuevas and others, in 2010 67% of all content spread on Bit torrent derives from these only 100 sources, and these sources enable 75% of all downloads.²²⁴

²¹⁸ David McCandless, "Warez Wars," *Wired* (April 1997), http://www.wired.com/wired/archive/5.04/ff_warez.html

²¹⁹ "The scene", www.wikipedia.org

²²⁰ Linus Wallei, *Copyright does not exist (chapter 'subculture of subcultures')*, found through Way back machine (July 25, 2011):

<http://web.archive.org/web/20110725143825/http://home.c2i.net/nirgendwo/cdne/ch5web.htm>

²²¹ www.wikipedia.org

²²² Wouter Schilpzand, "Large scale European police action against piracy networks," *Future of Copyright* (September 14, 2010), <http://www.futureofcopyright.com/home/blog-post/2010/09/14/large-scale-european-police-action-against-piracy-networks.html>

²²³ Schermer and Wubben, *Feiten om te delen*. P.44-46.

²²⁴ Ruben Cuevas and others, "Is Content Publishing in BitTorrent Altruistic or Profit-Driven?" *Proceedings of ACM CoNext* (2010).

2.5.2 Internet intermediaries

Other players that willingly or unwillingly facilitate copyright infringement are Internet intermediaries. According to the OECD, 'Internet intermediaries' "bring together or facilitate transactions between third parties on the Internet (see figure 2.1). They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties."²²⁵

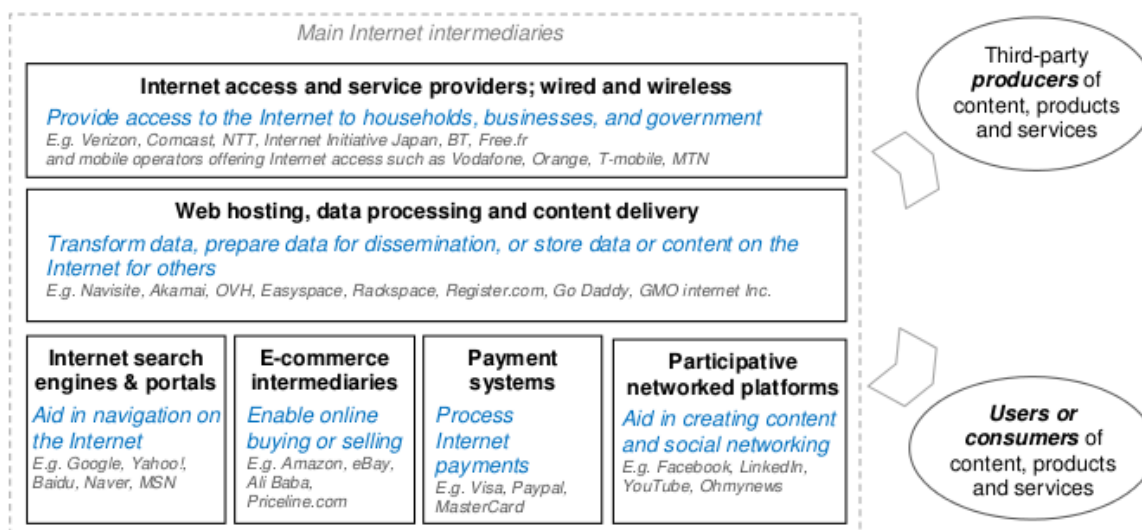


Figure 2.1: Internet intermediaries.²²⁶

Internet intermediaries form the middle ground between end users or consumers, and producers. The roles in this graph are presented in a way that separates them by clear lines. However, often, Internet intermediaries fulfill more than one role.²²⁷

Internet intermediaries add economic and social value to the Internet by using their position of middleman. An interesting economic aspect of this position is that Internet intermediaries are severely dependent on having a great number of users, because Internet services create network effects. This means that if more users are connected to a network, that network becomes more valuable. However, intermediaries often operate two sided business models. This means that they have two distinct groups of users, and the value that one type of user gets increases if the quality of the other kind of users increases. The intermediary needs to bring the two groups together. Search engines service users and advertisers and e-commerce services service buyers and sellers. Intermediaries have many tasks and different groups to cater to and this can create tension.²²⁸ For example, it is in the interest of the search engine to appeal to users, and clearing its search results of any copyright infringing files might not supply those users with what they want.

Internet intermediaries have different revenue models. These can be advertisement models, fee models (users pay to subscribe to a service), brokerage models (like

²²⁵ Karine Perset, "The economic and social role of Internet intermediaries," *OECD* (2010). P. 9.

²²⁶ Image source: Karine Perset, "The economic and social role of Internet intermediaries," *OECD* (2010). P.9.

²²⁷ Perset, "The economic and social role of Internet intermediaries," P.10-11.

²²⁸ Perset, "The economic and social role of Internet intermediaries," P.15-18.

commissions on transactions in e-commerce platforms) or models based on voluntary donations.²²⁹

They provide more and more social and economic benefits, and play a key role in the Internet ecosystem. As they operate, create and maintain most of the Internet infrastructure, they control most of what is happening online. This makes them interesting for rights holders that look for efficient ways of copyright enforcement.²³⁰ As mentioned there are many different forms of Internet intermediaries.

Access providers/ISPs

The first group consists of access and service providers. Although many use the terms interchangeably with the acronym ISP, there is a difference: access providers provide subscribers with access to the Internet. 'Service provider' on the other hand is a confusing term as it fails to differentiate between the different roles of providing access, hosting, etc. This is because access providers many times also provide web hosting, web page design and other smaller services. For the purpose of this research, ISP will refer to access provider.²³¹ Access providers thus provide the access to the Internet that their subscribers can use to up- or download copyright infringing material.

Hosting providers

Hosting providers offer the technical infrastructure where distributors can store or upload content.²³²

They have huge data centers that allow space usually for web hosting. This means that these intermediaries allow users to create their own website and make this website accessible through the World Wide Web. Sometimes they also allow server hosting or data processing services. This also involves cloud computing, which is currently on the rise.²³³ These services are usually provided by ISPs, and are mostly small scale for personal web pages. Hosting providers can allow users to host infringing content.

Search engines

Other parties involved are for example search engines. Internet search engines and portals are websites like Google or Baidu in China that use a search engine to generate and maintain databases of Internet addresses and content that is easily searchable.²³⁴ Search engines are important, because they can allow users to find infringing content. BPI performed an experiment where they searched Google for the UK's top 20 singles, followed by 'mp3.' On average 17 of the 20 first results linked to infringing material.²³⁵

Web e-commerce intermediaries

Web e-commerce intermediaries connect buyers and suppliers and enable Internet transactions between them. They consist of Internet retailers and auction platforms, or business-to-business electronic markets using the Internet.²³⁶ Internet retailers might allow

²²⁹ Perset, "The economic and social role of Internet intermediaries," P.18-20.

²³⁰ Perset, "The economic and social role of Internet intermediaries," P.8.

²³¹ Perset, "The economic and social role of Internet intermediaries," P.11.

²³² Schermer and Wubben, *Feiten om te delen*. P.44-46.

²³³ Perset, "The economic and social role of Internet intermediaries," P.11-12.

²³⁴ Perset, "The economic and social role of Internet intermediaries," P.12.

²³⁵ BPI, The British Recorded Music Industry, *Digital Music Nation 2010* (BPI Limited 2010). P.20-21.

²³⁶ Perset, "The economic and social role of Internet intermediaries," P.12-13.

for the selling or buying of infringing goods.

Payment service providers

E-commerce payment systems consist of payment systems that use a credit or bank account to enable e-commerce transactions and payment systems for paid services, provided by non-bank institutions operating on the Internet.²³⁷ They offer online services to merchants, and accept payments through for example credit card, online banking or money transfer. They usually are able to connect to multiple banks. This is good for the merchant, because it saves the merchant the trouble of connecting to different banks. This especially comes in handy when a company operates internationally. They sometimes also offer risk management services. They make money by taking a small percentage of each transaction or a low fixed cost per transaction.²³⁸ Examples of payment service providers are ideal, PayPal, and Paymate. Interestingly enough they often don't know who is using their services,²³⁹ which means they also handle payment for websites that offer services that might be based on infringing content, generating income for those websites.

Participative-networked platforms

Participative-networked platforms facilitate social communication and information exchange. They range from blogs, to wikis, instant messaging services, mobile applications, social networking sites, virtual worlds, online computer games, video content and file sharing sites, sites allowing feedback on written works, photo sharing sites, podcasting and group based aggregation.²⁴⁰ Participative-networked platforms can enable users to contribute their own information, which can consist of copyright infringing material.

P2P Operators

P2P operators offer networks or platforms that allow users to up- or download content, or that provide guidance to places where this can be done.²⁴¹ Often a peer to peer network uses an overlay network (built as an application layer) on top of native or physical network topology. This overlay is used for indexing and peer discovery and make P2P systems independent from the network. Content is subsequently exchanged directly over these IP networks. The exceptions to this rule are anonymous P2P systems, which use extra routing layers to obscure the identity of the source or of the destination node/user.²⁴²

Advertisers

Advertisers sell advertising space at popular websites, which generates income for those sites as well. This is done through banner ads, for example, and websites and advertisers make money per visitor, view, or click. As some infringing sites are dependent on sources of income, advertisers play a role in the distribution of infringing content. However, advertisers buy their advertising space at blind networks, so they often don't know where their money goes.²⁴³

²³⁷ Perset, "The economic and social role of Internet intermediaries," P.13.

²³⁸ "Payment service providers", www.wikipedia.org

²³⁹ Schermer and Wubben, *Feiten om te delen*. P.44-46.

²⁴⁰ Perset, "The economic and social role of Internet intermediaries," P.14.

²⁴¹ Schermer and Wubben, *Feiten om te delen*. P.44-46.

²⁴² "P2P," www.wikipedia.org

²⁴³ Schermer and Wubben, *Feiten om te delen*. P.44-46.

This part shows that different internet intermediaries are willingly or unwillingly involved in copyright infringement.

2.5.3 Peers/users

The third big group is users or peers. Users up- and download potentially infringing content through the different distribution networks. Legally there are a couple of important distinctions to be made.

Users are mostly identified by their IP address. This is the numerical label assigned to a device (for example a computer or a printer) that is connected to a computer network and uses the Internet Protocol.²⁴⁴ In this sense it can identify a host or network interface, and serves as location addressing.²⁴⁵ However, as a result of a shortage in IP addresses, the Network Address Translation (NAT) was created, which allows for communication through the router. Computers inside of the private network of that Internet connection communicate with the router, which in turn communicates with the other IP addresses in the public network. This means that the router is identified as the Internet connection of the subscriber that communicates with the outside world.²⁴⁶

This is relevant because this can lead to erroneous identification of copyright infringement. Subscribers that pay for the Internet connection might not be the actual users of that Internet connection, and the ones engaged in copyright infringement. Many more people can use that Internet connection than the subscriber. For example, a bar may allow for open Wi-Fi, enabling many users to use the same Internet connection. Another problem could be that a connection might be infected with malware, which means that some of its actions will be outside of the owners' control. As one American judge put it: "Where an IP address might actually identify an individual subscriber and address the correlation is still far from perfect, (...) the infringer might be the subscriber, someone in the subscriber's household, a visitor with her laptop, a neighbor, or someone parked on the street at any given moment."²⁴⁷ As a response, rights holders have sued subscribers on the basis of the idea of 'negligence', for leaving their Wi-Fi open to infringement by others.²⁴⁸

Because IP addresses identify users, this information is privacy sensitive. Only ISPs can identify users on the basis of their IP address. But a problem is that there are dynamic IP addresses as well, which change every period of time. This could make identification problematic.²⁴⁹

²⁴⁴ Jon Postel, "DOD Standard for the Internet Protocol," *Prepared for DARPA* (January 1980)

<http://tools.ietf.org/html/rfc760>.

²⁴⁵ Jon Postel, "Internet Protocol, DARPA Internet Program, Protocol Specification," *Prepared for DARPA* (September 1981) <http://tools.ietf.org/html/rfc791>.

²⁴⁶ "The IP network address translator (NAT)," *Network working group*, (May 1994), <http://tools.ietf.org/html/rfc1631>

²⁴⁷ VPR Internationnale v. Does 1-1017, U.S. District Court, ILCD, April 29, 2011.

²⁴⁸ "Ruggiero argues negligence," *Copyright Clerk website* (27 September, 2012),

<http://copyrightclerk.com/2012/09/27/ruggiero-argues-negligence/>

²⁴⁹ "IP," www.wikipedia.org

2.6 The scale of copyright infringement online

It is difficult to make an exact, objective statement about the scale on which copyright infringement happens online. Throughout the years a lot of research has been done, some aimed specifically at the scale of different methods of copyright infringement or at the scale of infringement regionally. Researchers have employed different methods when estimating the amount of infringement, and have focused on different indicators to establish the scale of infringement. Some research and estimates have been brought forward by the industry itself and may therefore not be independent. Other research may not take into account all the relevant factors in determining scale and the development of scale throughout the years. Therefore this chapter aims to provide an overview of research done in this field to get a broad image of scale, rather than look for one specific number. Note that none of these reports take into account basic forms of what could theoretically be copyright infringement, like sending files to friends or family. They focus on larger scale infringement, while actual infringement might be much higher.

2.6.1 What constitutes 'large-scale' copyright infringement?

It is difficult to establish what constitutes the large scale in 'large-scale infringement.' Bridy points out that this is to an extent a rhetorical construct. Rights holders have succeeded in constantly referring to copyright infringement as 'massive' and 'large-scale,' which has been an effective strategy, as this rhetoric has been followed into court decisions and legal documents.²⁵⁰

There are a number of facts that seem to suggest that copyright infringement happens on a much larger scale than before. Because the economics of reproduction and distribution changed, every user is potentially a large-scale reproducer and distributor. Originally copyright infringement generally required high upfront costs, which means it was reserved for larger scale organizations. As James Boyle puts it: "The technologies of reproduction or the activities necessary to infringe were largely, though not entirely, industrial. Imagine someone walking up to you in 1950, handing you a book or a record or a movie reel, and saying "Quick! Do something the law of Intellectual property might forbid." (...) triggering the law of intellectual property would be genuinely difficult. Like an antitank mine, it would not be triggered by the footsteps of individuals. It was reserved for bigger game."²⁵¹

There are many ways to evaluate large-scale infringement. One can look at the amount of users connected to P2P protocols, the amount of Internet traffic used by P2P protocols and then look at the amount of illegality on those networks. Or one can look at the amount of infringing content accessed through the HTTP protocol. Afterwards, one can compare those numbers to copyright infringement numbers before digitization and the Internet.

The majority of studies suggest that most of the files on P2P networks are infringing. However, it is difficult to find research that is truly independent or uncontested.²⁵² A study by the Internet Commerce Security Laboratory in 2011 deducted from a sample of trackers

²⁵⁰ Bridy, "Is Online Copyright Enforcement Scalable?" P.706-708.

²⁵¹ James Boyle, *The public domain: Enclosing the commons of the mind*, (New Haven: Yale University Press, 2008). P.50.

²⁵² Bridy, "Is Online Copyright Enforcement Scalable?" P.708-710.

that 117 million seeds were available across more than one million torrents. They said that around 0,3% of all content offered on BitTorrent was legal.²⁵³ However, this study was heavily criticized because it only included popular torrents.²⁵⁴ Another organization, Envisional, also researched the amount of infringing content in 2011 in the most popular downloaded torrents. They concluded that of the 10,000 most popular torrents, 99,2% were infringing. In total they argued that 63,7% of all content offered through BitTorrent was infringing.²⁵⁵ Scientists from the University of Amsterdam and TNO estimated that 95% of all content exchanged through file sharing sites and networks was infringing in 2008.²⁵⁶

Envisional specifically researched BitTorrent index site Mininova. At the time of that research Mininova was removing all infringing content from its network (on 29 November 2009). According to Envisional, after the removal, the amount of torrents dropped from 1,3 million to 10,000 (which equals a drop in 99%). The amount of downloads dropped from 10 million to 500,000 a day. Other BitTorrent sites reported an increase in visitors immediately.²⁵⁷

With regard to the HTTP protocols, Envisional researched the amount of infringing cyber locker traffic, and said that 73,2% of all cyber locker content was infringing in 2010.²⁵⁸ They claimed that video streaming was mostly legitimate, but that 5,3% was copyright protected content.²⁵⁹

A logical next step would be to look at the amount of users connected to those protocols and the amount of Internet traffic used up by those protocols to see at what scale copyright infringement takes place. As the next couple of pages will show, those numbers range in the millions of users.

Then there can be a comparison with copyright infringement before digitalization and the Internet. These numbers are difficult to come by, but in the mid 90's, RIAA released a report that CD piracy started to slowly overtake music cassette piracy. Mainly street vendors were arrested, with the number of arrests ranging in the hundreds. The number of seized CD's was over 1 million, and the same for infringing cassettes.²⁶⁰ Taken together, for example for the US, this means that the majority of P2P traffic is infringing, we know that millions of US households have P2P applications installed, we know that music piracy is a common form of piracy, and we know that the number of arrests by the RIAA mid 90's for music piracy was in the hundreds. We also know that the number of infringing files floating around the Internet is in the billions, and the number of confiscated CD's and cassette tapes

²⁵³ Robert Layton and Paul Watters, "Investigation into the extent of infringing content on BitTorrent networks," *Technical report* (Internet Commerce Security Laboratory, University of Ballarat, Australia, 2010).

²⁵⁴ Ernesto, "Tech News Sites Tout Misleading BitTorrent Piracy Study," *Torrentfreak* (July 24, 2010), <http://torrentfreak.com/tech-news-sites-tout-misleadingbittorrent-piracy-study-100724/>

²⁵⁵ David Price, *An estimate of infringing use of the Internet*, (Envisional, 2011). See: <http://documents.envisional.com/docs/Envisional-Internet-Usage-Jan2011.pdf>. P.1.

²⁵⁶ Annelies Huygen et al, "Ups and downs; economic and cultural effects of file sharing on music, film and games." *TNO Information and Communication Technology Series* (2009). P.95.

²⁵⁷ Envisional, *Mininova: Assessment of Copyrighted Torrent Link Removal* (2010).

²⁵⁸ David Price, *An estimate of infringing use of the Internet*, (Envisional, 2011). See: <http://documents.envisional.com/docs/Envisional-Internet-Usage-Jan2011.pdf>. P.1.

²⁵⁹ Price, *An estimate of infringing use of the Internet*, P.1.

²⁶⁰ "RIAA releases yearend anti-piracy statistics," *Negativland & The RIAA*, http://www.negativland.com/archives/014riaa/piracy_stats.html (the original link was on the RIAA website, but it has disappeared: http://www.riaa.com/newsitem.php?news_year_filter=&resultpage=140&id=876C1BEF-6ACE-E99D-2755-71A875EF2A66)

by the RIAA mid 90's was in taken together 2 million. Taken together, and also considering that CD burners were already around mid-90's, it is fair to say that we are dealing with large-scale copyright infringement.

2.6.2 Estimates on users engaged in copyright infringement

As copyright infringement took off at the turn of the millennium, mostly through sharing music on P2P protocols, early research focuses mainly on P2P platforms and music files to estimate the amount of copyright infringement online. The International Federation of the Phonographic Industry (IFPI), representing the recording industry worldwide, released numerous 'Digital Music Reports' between 2004 and 2011,²⁶¹ on the state of the music industry online. In these reports, the IFPI reserved considerable attention to the threat of online piracy. Its first reports highlighted a large scale by focusing on the amount of *simultaneous* users on p2p networks, and by estimating the number of infringing websites. As different forms of copyright infringement became more dominant later on, the IFPI stopped using these data as an indicator for the scale of copyright infringement after 2006. Around the same time, the OECD released its Broadband report, in which it also estimated the amount of simultaneous users on P2P networks.²⁶² Both reports have been included in Table 2.1.

According to Big Champagne, the number of simultaneous users on P2P networks was higher.²⁶³ They released a report with data on P2P in the USA alone, with levels that already surpassed the worldwide numbers as provided by the IFPI. Table 2.2 shows the amount of infringing websites and FTP (File transfer protocol) sites, as stated by the IFPI.

Organization	Year	Studied region	Amount of users
IFPI	2002	Worldwide	3 million
IFPI	2003	Worldwide	5 million
IFPI	2004	Worldwide	6,2 million
OECD	2004	Worldwide	10 million
Big Champagne	2004	USA	7,4 million
IFPI	2005	Worldwide	8,6 million
Big Champagne	2005	USA	8,9 million
Big Champagne	2006	USA	10 million
Big Champagne	2007	USA	9,35 million

Table 2.1: studies on simultaneous users on P2P networks.

Organization	Year	Studied region	Websites and FTP sites
IFPI	2002	Worldwide	430,000
IFPI	2003	Worldwide	250,000
IFPI	2004	Worldwide	350,000
IFPI	2005	Worldwide	450,000

Table 2.2: studies on infringing websites and FTP sites.

²⁶¹ The reports can be found on their website: <http://www.ifpi.org/>
²⁶² OECD, *Digital Broadband Content: Music* (2005), DSTI/ICCP/IE(2004)12/FINAL
²⁶³ Thomas Mennecke, "P2P Population Remains Steady," *Slyck* (October 20, 2006), http://www.slyck.com/story1314_P2P_Population_Remains_Steady

These reports focused on the amount of simultaneous users. This means that the actual amount of people engaged in copyright infringement may have been many times higher. There have been few estimates on the amount of users worldwide, for most research has been country specific (table 2.3).

Organization	Year	Studied region	Total users engaged in copyright infringement
PEW	2000	USA	13 million downloading unlicensed content
PEW	2002	USA	35 million downloading unlicensed content
PEW	2003	USA	18 million downloading unlicensed content
PEW	2004	USA	23 million downloading unlicensed content
EFF	2004	USA	60 million used P2P networks ²⁶⁴
The NPD group	2006	USA	15 million households downloading from P2P networks
PC Pitstop and BigChampagne media measurement	2006	Worldwide	184 million PC's with P2P installed ²⁶⁵
PC Pitstop and BigChampagne media measurement	2007	Worldwide	190 million PC's with P2P installed ²⁶⁶
PC Pitstop and BigChampagne media measurement	2008	Worldwide	220 million PC's with P2P installed ²⁶⁷
TNO/IVIR	2008	The Netherlands	4,7 million people download from an illegal source ²⁶⁸
Forrester research	2009	The Netherlands	5,4 million people download from an illegal source ²⁶⁹
Netnames	2013	N-America, Europe,	327 million unique

²⁶⁴ Stan Liebowitz, "File Sharing: Creative Destruction or Just Plain Destruction?" *Journal of Law and Economics* 49.1 (2006): 1-28. P.7.

²⁶⁵ Mary Madden, "The state of music online: Ten years after Napster," *Pew Internet & American Life Project* (2009). P.9.

²⁶⁶ Mary Madden, "The state of music online: Ten years after Napster," *Pew Internet & American Life Project* (2009). P.9.

²⁶⁷ Mary Madden, "The state of music online: Ten years after Napster," *Pew Internet & American Life Project* (2009). P.9.

²⁶⁸ Annelies Huygen et al, "Ups and downs; economic and cultural effects of file sharing on music, film and games." *TNO Information and Communication Technology Series* (2009).p. 72.

²⁶⁹ Schermer and Wubben, *Feiten om te delen*.

		Asia/Pacific	Internet users ²⁷⁰
TruOptik	2014	Worldwide	970 million unique IP addresses used P2P (estimated +500 million actual users) ²⁷¹

Table 2.3: studies on total users engaged in copyright infringement.

These numbers were mostly based on P2P traffic, but the HTTP protocol accounted for a large number of infringing traffic as well. According to the Mark Monitor Traffic report for 2011, Rapidshare generated 32 million daily visits, whilst megavideo.com and megaupload.com each generated 14 million daily visits in 2011.²⁷²

Another, comparable way to estimate the amount of copyright infringement online, is by looking at the percentage of Internet users that access or share unlicensed content (table 2.4).

Organization	Year	Studied region	Percentage of users
PEW	2000	USA	25% accessed unlicensed music
OECD	2002	Japan	17,9% of broadband users downloads unlicensed music ²⁷³
Jupiter research	2002	UK, France, Germany, Italy, Spain, Sweden	18% regularly swaps music on P2P networks
Jupiter research	2003	UK, France, Germany, Italy, Spain, Sweden	18% regularly swaps music on P2P networks
PEW	2003	USA	29% accessed unlicensed music
Jupiter research	2004	UK, France, Germany, Italy, Spain, Sweden	15% regularly swaps music on P2P networks
Jupiter research	2005	UK, France, Germany, Italy, Spain, Sweden	15% regularly swaps music on P2P networks
Jupiter research	2006	UK, France, Germany, Italy, Spain, Sweden	14% regularly swaps music on P2P networks
Ipoque	2007	Worldwide	20% connected to P2P
Jupiter research	2007	UK, France, Germany, Italy, Spain, Sweden	17,6% regularly swaps music on P2P networks
Jupiter research	2008	Europe	16% regularly swaps music on P2P networks
TNO/IVIR	2008	The Netherlands	38% overall illegal file sharing ²⁷⁴

²⁷⁰ David Price, "Sizing the piracy universe", *Netnames* (September 2013) available at: <https://copyrightalliance.org/sites/default/files/2013-netnames-piracy.pdf>.

²⁷¹ TruOptik, *Digital media unmonetized demand and peer-to-peer file sharing report* (2015). see: <http://truoptik.com/digital-media-unmonetized-demand-and-peer-to-peer-file-sharing-report-2014>

²⁷² Markmonitor, *Traffic Report: Online Piracy and Counterfeiting* (2011), see: [https://www.markmonitor.com/download/report/MarkMonitor - Traffic Report 110111.pdf](https://www.markmonitor.com/download/report/MarkMonitor%20-%20Traffic%20Report%20110111.pdf)

²⁷³ OECD, *Digital Broadband Content: Music* (2005), DSTI/ICCP/IE(2004)12/FINAL P.74.

²⁷⁴ Annelies Huygen et al, "Ups and downs; economic and cultural effects of file sharing on music, film and games." *TNO Information and Communication Technology Series* (2009).p. 72.

Forrester research	2009	Holland	40% downloading without license
Jupiter research	2009	Europe's top markets	21% engaged in unauthorized music sharing
Harris interactive	2010	UK	29% downloads music without license ²⁷⁵
IFPI	2010	Spain	45% downloads music without license
Nielsen company	2010	EU top 5 markets	23% of users visiting unlicensed services ²⁷⁶
Nielsen company	2010	Brazil	44% of users visiting unlicensed music services ²⁷⁷
Nielsen company	2010	Spain	45% of users visiting unlicensed music services ²⁷⁸
Canadian Intellectual Property Council	2011	Canada	29% acquires music through illegal means ²⁷⁹
Wiggin Entertainment Media Research	2011	UK	32% infringes copyrights online ²⁸⁰
The American Assembly	2011	USA	46% of adults have accessed unauthorized content ²⁸¹
NPD Group	2011	USA	65% of all music acquired through illegal means (of which 19% online)
IVIR/CentERdata	2012	The Netherlands	27% of the population share files illegally ²⁸²
Netnames	2013	N-America, Europe, Asia/Pacific	25,9% of all Internet users infringe copyrights ²⁸³
IVIR/CentERdata	2013	The Netherlands	25,8% of people between 12 and 65

²⁷⁵ BPI, The British Recorded Music Industry, *Digital Music Nation 2010* (BPI Limited 2010). P.24.

²⁷⁶ International Federation of the Phonographic Industry, *Digital Music Report 2011* (IFPI 2011).

²⁷⁷ IFPI, *Digital Music Report 2011*.

²⁷⁸ IFPI, *Digital Music Report 2011*.

²⁷⁹ Canadian Intellectual Property Council, *The True Price of Peer to Peer File-Sharing* (2010). Available at: <http://musiccanada.com/wp-content/uploads/2015/06/The-True-Price-of-Peer-to-Peer-File-Sharing.pdf>.

²⁸⁰ Wiggin Entertainment Media Research, *Digital Entertainment Survey* (2011). Available at: <http://www.slideshare.net/WigginLLP/digital-entertainment-survey-2011>.

²⁸¹ Joe Karaganis and Lennart Renkema, "Copy Culture in the US and Germany," *Columbia University: The American Assembly* (2012).

²⁸² Joost Poort and Jorna Leenheer, "File sharing 2@12: Downloading from illegal sources in the Netherlands," *Institute for Information Law & CentERdata*, Amsterdam/Tilburg (2012). Retrieved from http://www.ivir.nl/publications/poort/Filessharing_2012

²⁸³ David Price, "Sizing the piracy universe", *Netnames* (September 2013) available at: <https://copyrightalliance.org/sites/default/files/2013-netnames-piracy.pdf>

			shares movies illegally ²⁸⁴
--	--	--	--

Table 2.4: studies on percentage of infringing internet users.

There are a couple of points to take away from this research. First of all, most of this research or these estimations were either financed or commissioned by important stakeholders like the music industry, which makes their independence questionable. This is the case with many of the estimations made by the IFPI for example.

Also, there are some methodological difficulties. They focused on what happened online. A report by the NPD group revealed that the majority of all music in the US was acquired through illegal means (65%). Most of that happened offline, through hard drive trading or through burning from others.²⁸⁵ It also did not take into account what happened to files after downloading. The files could be spread amongst friends and family members for example. Another important point is that most of this research was based on surveys. Surveys suffer from the problem that some people might not confess to downloading or uploading illegal content online. Another problem in general was that some parts of the population or some regions in the world might have slower Internet connections, no connections at all, or might be technologically less savvy. Another problem is that some of the surveys or estimates included older parts of the population as well, who tend to be technologically less savvy. For example, in the research done by the American Assembly, it was revealed that although 46% of adults in the USA had accessed unauthorized content, that number rose to 70% among young adults (18-29).²⁸⁶

One thing is clear from these numbers: copyright infringement online has happened on a large scale throughout the years consistently, with percentages of the population infringing on copyrights estimated between 14% and 50% in different reports. In fact, when the digital music index was released in 2012, which shows how many people pirate and what they pirate, those numbers were so all-encompassing, the Guardian proceeded to refer to file sharing as “mainstream.”²⁸⁷

On the other hand, some studies suggest that overall file sharing is declining. However, this differs per type of content. Sharing music illegally has declined and sharing games illegally decreased slightly, while sharing audiovisual content has increased massively. They hypothesise that the steep drop in the illegal sharing of music is due to the rise of viable legal alternatives.²⁸⁸ Follow up research suggested that sharing movies illegally kept increasing the following year, but only slightly, while the use of legal services online for audiovisual content increased steeply to the same level as sharing movies illegally.²⁸⁹

²⁸⁴ Jorna Leenheer and Joost Poort, "Alleen maar nette mensen." Consumentenonderzoek Downloadgedrag Films." *IViR/CentERdata* 14 (2014), http://www.ivir.nl/publicaties/download/alleen_maar_nette_mensen.pdf

²⁸⁵ The NPD Group, "After Years of Defection, The Number of U.S. Music Buyers is On The Upswing," *The NPD Group* (March 6, 2012), https://www.npd.com/wps/portal/npd/us/news/press-releases/pr_120306/.

²⁸⁶ Joe Karaganis and Lennart Renkema, "Copy Culture in the US and Germany," *Columbia University: The American Assembly* (2012).

²⁸⁷ Lanre Bakare, "Illegal music filesharing is now mainstream," *the Guardian* (September 18, 2012), <http://www.theguardian.com/commentisfree/2012/sep/18/illegal-music-filesharing-mainstream-ed-sheeran>

²⁸⁸ Joost Poort and Jorna Leenheer, "File sharing 2@12: Downloading from illegal sources in the Netherlands," *Institute for Information Law & CentERdata*, Amsterdam/Tilburg (2012). Retrieved from http://www.ivir.nl/publicaties/poort/Filesharing_2012

²⁸⁹ Jorna Leenheer and Joost Poort, "Alleen maar nette mensen." Consumentenonderzoek Downloadgedrag Films." *IViR/CentERdata* 14 (2014), http://www.ivir.nl/publicaties/download/alleen_maar_nette_mensen.pdf

2.6.3 Estimates on infringing content and traffic

Another indication of scale is the amount of infringing content and traffic on the Internet. One of the ways to measure this is by looking at the percentage of Internet traffic that is infringing. Researchers have mostly looked at P2P traffic for this (table 2.5).

Organization	Year	Studied region	Percentage of Internet traffic
EFF	2004	USA	60% File sharing ²⁹⁰
Ipoque	2007	Worldwide	80% infringing traffic ²⁹¹
Ipoque	2007	Eastern Europe	83% P2P Traffic ²⁹²
Ipoque	2007	Germany	69% P2P Traffic ²⁹³
Ipoque	2007	Middle East	49% P2P Traffic ²⁹⁴
Ipoque	2007	South Western Europe	64% P2P Traffic ²⁹⁵
IFPI	2008	Europe	80% Illegal file sharing
Ipoque	2008	Southern Africa	66% P2P Traffic ²⁹⁶
Ipoque	2008	South America	65% P2P Traffic ²⁹⁷
Ipoque	2008	Eastern Europe	70% P2P Traffic ²⁹⁸
Ipoque	2008	Northern Africa	42% P2P Traffic ²⁹⁹
Ipoque	2008	Germany	52% P2P Traffic ³⁰⁰
Ipoque	2008	Southern Europe	55% P2P Traffic ³⁰¹
Ipoque	2008	Middle East	45% P2P Traffic ³⁰²
Ipoque	2008	South Western Europe	54% P2P Traffic ³⁰³
Sandvine	2008	Worldwide	45% P2P Traffic
Sandvine	2009	North America	15,1% P2P Traffic
Sandvine	2009	Europe	22% P2P Traffic
Sandvine	2009	Latin America	31,9% P2P Traffic
Sandvine	2009	Asia/Pacific	8,4% P2P Traffic
Envisional	2010	Worldwide	23,76% Infringing traffic ³⁰⁴
Sandvine	2010	North America	19,2% P2P Traffic
Sandvine	2010	Europe	11% P2P Traffic
Sandvine	2010	Latin America	36,7% P2P Traffic

²⁹⁰ Stan Liebowitz, "File Sharing: Creative Destruction or Just Plain Destruction?" *Journal of Law and Economics* 49.1 (2006): 1-28. P. 7.

²⁹¹ Hendrik Schulze and Klaus Mochalski, "Internet study 2007," *Ipoque GmbH White Paper* (2007).

²⁹² Schulze, "Internet study 2007."

²⁹³ Schulze, "Internet study 2007."

²⁹⁴ Schulze, "Internet study 2007."

²⁹⁵ Schulze, "Internet study 2007."

²⁹⁶ Hendrik Schulze and Klaus Mochalski, "Internet Study 2008/2009," *Ipoque Report 37* (2009): 351-362. P.2.

²⁹⁷ Schulze, "Internet Study 2008/2009." P.2.

²⁹⁸ Schulze, "Internet Study 2008/2009." P.2.

²⁹⁹ Schulze, "Internet Study 2008/2009." P.2.

³⁰⁰ Schulze, "Internet Study 2008/2009." P.2.

³⁰¹ Schulze, "Internet Study 2008/2009." P.2.

³⁰² Schulze, "Internet Study 2008/2009." P.2.

³⁰³ Schulze, "Internet Study 2008/2009." P.2.

³⁰⁴ David Price, *An estimate of infringing use of the Internet*, (Envisional, 2011). See: <http://documents.envisional.com/docs/Envisional-Internet-Usage-Jan2011.pdf>. They did not take pornographic works into account because it is often uncertain how they are copyright protected.

Sandvine	2010	Asia/Pacific	25,7% P2P Traffic
Deepfields	2012	North America	15-20% File sharing ³⁰⁵
Netnames	2013	N-America, Europe, Asia/Pacific	23,8% Infringing traffic ³⁰⁶

Table 2.5: studies on percentage of infringing internet traffic.

Early research also included the number of infringing files circulating the web. Although this is not directly relevant to this research, it shows that the number is high. Off course, these numbers do not take streaming into account (table 2.6).

Organization	Year	Studied region	Infringing files
IFPI	2001	Worldwide	0,6 billion music files
Webnoize	2001	Worldwide	2,79 billion music files ³⁰⁷
IFPI	2002	Worldwide	0,6 billion music files
Webnoize	2002	Worldwide	3,05 billion music files ³⁰⁸
NetPD	2002	Worldwide	3,6 billion files ³⁰⁹
IFPI	2003	Worldwide	1,1 billion music files
IFPI	2004	Worldwide	0,9 billion music files
IFPI	2005	Worldwide	8,7 billion music files
IFPI	2006	Worldwide	8,85 billion music files
IFPI	2009	Worldwide	40 billion music files

Table 2.6: studies on number of infringing files.

Markmonitor research further determined that sites that offered pirated digital content had 53 billion visits in 2011,³¹⁰ and the digital music index showed that the amount of BitTorrent downloads was incredibly high in 2012. In the US it was at around 96 million torrents, whilst in the UK it was 43 million.³¹¹

Again, it shows that copyright infringement has happened on a large scale, as a huge amount of infringing content is spread around the Internet, and accounts for a large

³⁰⁵ "The rise and fall of P2P," *DeepField blog* (April 10, 2012), <http://blog.deepfield.net/2012/04/10/the-rise-and-fall-and-rise-of-p2p/>, last viewed February 1, 2012.

³⁰⁶ David Price, "Sizing the piracy universe", *Netnames* (September 2013) available at: <https://copyrightalliance.org/sites/default/files/2013-netnames-piracy.pdf>

³⁰⁷ Stan Liebowitz, "File Sharing: Creative Destruction or Just Plain Destruction?" *Journal of Law and Economics* 49.1 (2006): 1-28. P.6

³⁰⁸ Stan Liebowitz, "File Sharing: Creative Destruction or Just Plain Destruction?" *Journal of Law and Economics* 49.1 (2006): 1-28. P.6.

³⁰⁹ David Rowan, "Inside the web of thieves," *the Guardian* (April 21, 2002), <http://www.theguardian.com/technology/2002/apr/21/observersciencepages.theobserver>, and: Alejandro Zentner, "Measuring the effect of file sharing on music purchases." *Journal of Law and Economics* 49.1 (2006): 63-90.

³¹⁰ "Report Sheds Light on Scale and Complexity of Online Piracy and Counterfeiting Problem," *Realwire* (Jan 12, 2011), <http://www.realwire.com/releases/Report-Sheds-Light-on-Scale-and-Complexity-of-Online-Piracy-and-Counterfeiting-Problem>

³¹¹ Dave Lee, "A Glimpse at Piracy in the UK and Beyond," *BBC.com* (Sept 16, 2012), <http://www.bbc.com/news/technology-19599527>

percentage of Internet traffic. Research done by Netnames suggests that the amount of infringing traffic was still growing steadily in 2013.³¹²

2.6.4 Type of infringing content

Although early research in particular focused more on the sharing of music files, users switched to other types of content, like videos, games, books, software, photos and other files.³¹³ Music started off as the most popular content to share illegally. NetPD said that 3.6 billion files were downloaded monthly in 2002, of which 60-70% were music files.³¹⁴ Gradually, as bandwidth increased, movies and TV shows became more popular too. In fact, 35% of all torrents consisted of video material towards the end of 2010.³¹⁵ Other research suggested that sharing music illegally declined and sharing games illegally decreased slightly, while sharing audiovisual content has increased massively. These studies suggested that this difference could be attributed to the rise of viable legal alternatives in music at the time.³¹⁶ Research done the next year suggested a continuation of this trend: the illegal sharing of audiovisual content increased slightly, while the use of legal services online for audiovisual content increased steeply to the same level as sharing movies illegally.³¹⁷

But other types of content have grown popular as well, such as software. In 2008 the Entertainment Software Alliance detected more than 700,000 copyright infringements a month, spread over 100 countries.³¹⁸ According to the Business Software Alliance, 57% of all the worlds' computer users admitted they pirate software in 2011. In Western Europe this figure was 32%, in North America it was 19%.³¹⁹ The numbers by the BSA have been criticized for its assumptions, because it assumed that customers would otherwise buy software at market price.³²⁰

For videogames, the International Intellectual Property Alliance said that in December 2008 13 video game titles were downloaded 6.4 million times without consent.³²¹ Ubisoft even claimed that they suffered a 93-95% piracy rate for PC games, by which they

³¹² David Price, "Sizing the piracy universe", *Netnames* (September 2013) available at: <https://copyrightalliance.org/sites/default/files/2013-netnames-piracy.pdf>

³¹³ OECD, *Digital Broadband Content: Music* (2005), DSTI/ICCP/IE(2004)12/FINAL

³¹⁴ David Rowan, "Inside the web of thieves," *the Guardian* (April 21, 2002), <http://www.theguardian.com/technology/2002/apr/21/observersciencepages.theobserver>, and: Alejandro Zentner, "Measuring the effect of file sharing on music purchases." *Journal of Law and Economics* 49.1 (2006): 63-90.

³¹⁵ David Price, *An estimate of infringing use of the Internet*, (Envisional, 2011). See: <http://documents.envisional.com/docs/Envisional-Internet-Usage-Jan2011.pdf>.

³¹⁶ Joost Poort and Jorna Leenheer, "File sharing 2@12: Downloading from illegal sources in the Netherlands," *Institute for Information Law & CentERdata*, Amsterdam/Tilburg (2012). Retrieved from http://www.ivir.nl/publications/poort/Filesharing_2012

³¹⁷ Jorna Leenheer and Joost Poort, "Alleen maar nette mensen." Consumentenonderzoek Downloadgedrag Films." *IViR/CentERdata* 14 (2014), http://www.ivir.nl/publicaties/download/alleen_maar_nette_mensen.pdf

³¹⁸ Daniel Castro, Richard Bennett, and Scott Andes, "Steal these policies: strategies for reducing digital piracy," Information Technology and Innovation Foundation (Washington, DC: 2009), <http://www.itif.org/files/2009-digital-piracy.pdf>. P.4.

³¹⁹ BSA, the Software Alliance, "2011 Piracy Study," <http://globalstudy.bsa.org/2011/>

³²⁰ Mike Palmedo, "BSA Report on Global Software Piracy," *Infojustice.org* (May 17. 2012). <http://infojustice.org/archives/23902>

³²¹ International Intellectual Property Alliance, *Special Report 301*, (February, 2009).

meant only 7% of users actually paid for the product.³²² On the other hand, console based video game piracy seemed to be low, limited to only 1-2% of the population in the USA for example.³²³

With regards to books, some have claimed that book piracy is a non-issue.³²⁴ However, FairShare Guardian, the anti-piracy service of copyright protection company Attributor, estimated that of every book published, 10,000 copies were downloaded for free. The most popular books that were stolen were investing and business books, according to the study. However, it should be noted that Attributor sells copyright solutions for authors and publishers, and thus has a stake in these numbers.³²⁵

2.7 The business of infringement

Apart from ideological and social motives for file sharing, some distributors have financial incentives for facilitating copyright infringement as well. They make money through payment sites or advertisement.³²⁶ As distributors don't pay for the spread of content, most costs are limited to the cost of spreading content or hosting content.

Payment sites are sites that attract consumers with infringing content that can be downloaded, bought or streamed at a low price. At times these forms of payment involve a subscription. In the case of cyber lockers, payment is usually generated by offering 'premium' services instead of the free light version that has all kinds of downsides.³²⁷

Another way to make money from distributing infringing content is by allowing for advertisement at places where users can download or access infringing content. These amounts are supposedly big, as those sites generate many visitors a year. In 2010, Markmonitor calculated that Megavideo, Megaupload and Rapidshare combined a total of 21 billion visitors a year.³²⁸ Mininova supposedly had a turnover of 1 million Euros, of which the majority was based on advertisement sales.³²⁹

Distributors also make money by selling products and services that stimulate the spread of infringing content. The problem is that usually those products or services have substantial non-infringing uses, and do not qualify as infringement tools per se.³³⁰

Although there are many claims that piracy is profitable, Joe Karaganis disputes these claims. He provides a list with some famous platforms for infringing content and their revenues.

³²² Dan Pearson, "Guillemot: as Many PC players pay for F2P as boxed product," *Gamesindustry.biz* (Aug 22, 2012), <http://www.gamesindustry.biz/articles/2012-08-22-guillemot-as-many-pc-players-pay-for-f2p-as-boxed-product>

³²³ Joe Karaganis and Lennart Renkema, "Copy Culture in the US and Germany," *Columbia University: The American Assembly* (2012).

³²⁴ Paul Carr, "Book Piracy: A Non-Issue," *TechCrunch* (Aug 23, 2011), <http://techcrunch.com/2011/08/23/book-piracy-a-non-issue/>

³²⁵ Paul Boutin, "E-book piracy costs U.S. publishers \$3 billion, says study," *Venturebeat.com* (March 2, 2010), <http://venturebeat.com/2010/03/02/book-piracy-costs-u-s-publishers-3b-says-study/>

³²⁶ Schermer and Wubben, *Feiten om te delen*. P.43.

³²⁷ Schermer and Wubben, *Feiten om te delen*. P.43.

³²⁸ Markmonitor, *Traffic Report: Online Piracy and Counterfeiting* (2011), see: <https://www.markmonitor.com/download/report/MarkMonitor-Traffic-Report-110111.pdf>.

³²⁹ Hamel, E. (2009), "Jaaromzet Mininova 1 miljoen euro," *Webwereld.nl* (March 13, 2009), <http://webwereld.nl/nieuws/56410/jaaromzet-mininova-1-miljoen-euro.html>

³³⁰ Schermer and Wubben, *Feiten om te delen*. P.44.

For example, when The Pirate Bay was taken to trial in 2009 in Sweden, many groups made statements on its revenues. The IFPI claimed that the site made around 3 million dollars a year. The MPAA claimed it was even more, around 5 million. However, prosecutors calculated its revenues as much lower: 170,000 dollars from advertising. The website itself claimed to pay 112,000 dollars a year for server and bandwidth costs, whilst making 100,000 dollars a year in revenue. One has to take into consideration that this was one of the most visited websites in the world (top 100).

When the site owners of NinjaVideo, a movie indexing site based in Brooklyn, were arrested in 2011, prosecutors alleged they had made 500,000 in two and a half years. Brian McCarthy, the owner of Channelsurfing.net, a sports streaming site, was alleged to have made 90,000 dollars in five years. Both the primary owner of NinjaVideo and the owner of Channelsurfing faced jail time under the US No Electronic Theft Act.

During their domain name seizure program in 2010 (called 'Operation in Our Sites'), the US Immigrations and Customs Enforcement (ICE) made some revenue estimates, based on information from advertising network Valueclick. According to ICE, Torrentfinder, a BitTorrent site, made about \$15,000 in ad revenue from Valueclick over a year in 2008-2009. Onsmash, a music link site, made around \$2,500 in 2009-2010.³³¹

2.8 Economic impact of infringement

The copyright industries have thus far dominated the debate on the economic impact of copyright infringement online. They claim that they suffer huge losses as a result of large-scale copyright infringement, but these claims are often contested.

For example, in the debates surrounding the extremely controversial SOPA law in the US, the US Chamber of Commerce, a lobby organization that advocates for more IP protection and enforcement, claimed that piracy threatens "19 million American jobs"³³² This number was debunked for including the entire tech sector, which was actually against more IP enforcement.³³³ An earlier BASCAP (Business Action to Stop Counterfeiting and Piracy, set up by the US Chamber of Commerce) study claimed that in 2.5 million jobs were destroyed by counterfeiting and piracy across G20 economies in 2008.³³⁴ However, according to the US congressional research service, the US movie industry had only 374,000 people working in it in 2010, which is not much less than the 392,000 in 1998.³³⁵ Another well cited report by the industry was by frontier economics that reported 1.2 trillion in losses. However, this report was also commissioned by BASCAP.³³⁶ This report has also been criticized on methodological grounds.³³⁷ The US government accountability office concludes

³³¹ Joe Karaganis, "Meganomics," *The American Assembly, Columbia University* (January 24, 2012), see: <http://piracy.americanassembly.org/meganomics/>

³³² "19 Million American Jobs at Risk," *U.S. Chamber of Commerce* (May 12, 2011), <https://www.uschamber.com/ad/19-million-american-jobs-risk>

³³³ Mike Masnick, "Ridiculous: Lamar Smith Basing His Plan To Massively Regulate The Internet On False Or Misleading Research," *Techdirt* (Dec 15, 2011), <https://www.techdirt.com/articles/20111214/23451317095/ridiculous-lamar-smith-basing-his-plan-to-massively-regulate-Internet-false-misleading-research.shtml>

³³⁴ Masnick, "Ridiculous."

³³⁵ Full report at: Mike Masnick, "Ridiculous."

³³⁶ Mike Masnick, "Ridiculous."

³³⁷ Mike Masnick, "Ridiculous."

that it is difficult, even maybe impossible to quantify the economy-wide impacts of piracy.³³⁸ They say that for example a 200 billion dollar in losses figure surfaced in an FBI press release, but the FBI itself has no record of the source or methodology. BSA numbers, who claimed to have lost 9 billion to piracy in 2008, were also considered false because they assumed a one-to-one rate of substitution, and also extrapolated data of surveyed countries to non-surveyed countries. A well cited OECD report claimed that 200 billion dollars per year could be lost to counterfeiting.³³⁹ However, that report intended to indicate an upper bound, which meant to illustrate that the number could be that high, but is in reality probably much lower.³⁴⁰

Other reports suggest that having less strict IP rules and less enforcement would actually benefit the economy. A study by Australian Digital Alliance claimed that expanding copyright exceptions like fair use could potentially add 600 million to the local economy.³⁴¹ Another study by the Computer and Communications Industry Association claimed that fair use accounts for 5,4 trillion in revenue for the USA.³⁴²

The same uncertainty arises in the academic world, where different studies reveal contradicting outcomes. Well cited research by Harvard says that people that download would not necessarily have bought those files, and this leads them to conclude that file sharing is harmless.³⁴³ Some say that file sharing has only a modest impact on box office revenue.³⁴⁴ Others study says that BitTorrent does not hurt sales.³⁴⁵ Stan Liebowitz has repeatedly argued against this and says that file sharing is harmful.³⁴⁶ Other research claims that file sharing leads to more societal welfare and is therefore overall beneficial.³⁴⁷ According to consulting firm Considerati, although some studies suggest there are no effects and some suggest positive effects, the majority of the different economic studies suggest copyright infringement has a negative influence on legal sales.³⁴⁸

What we do know is that global record music sales dropped from 26 billion (2000) to under 16 billion (2010). However, there could be other reasons for this, like tougher

³³⁸ Nate Anderson, "US government finally admits most piracy estimates are bogus," *ArsTechnica* (April 13, 2010), <http://arstechnica.com/tech-policy/2010/04/us-government-finally-admits-most-piracy-estimates-are-bogus/>

³³⁹ "OECD project on counterfeiting and piracy," *OECD Website*, <http://www.oecd.org/sti/ind/oecdprojectoncounterfeitingandpiracy.htm>

³⁴⁰ Felix Salmon, "Counterfeiting: Much Less Prevalent Than You Think," *Upstart Business Journal* (Oct 26, 2007), <http://upstart.bizjournals.com/views/blogs/market-movers/2007/10/26/counterfeiting-much-less-prevalent-than-you-think.html?page=all>

³⁴¹ Lateral Economics, "Copyright reports," *report for the Australian Digital alliance* (september 2012), <http://digital.org.au/content/LateralEconomicsReports>

³⁴² Thomas Claburn, "Fair Use Worth More to Economy Than Copyright, CCA Says," *InformationWeek* (Sept 12, 2007), <http://www.informationweek.com/fair-use-worth-more-to-economy-than-copyright-ccia-says/d/d-id/1059122?>

³⁴³ Felix Oberholzer-Gee and Koleman Strumpf, "The Effect of File Sharing on Record Sales: An Empirical Analysis," *Journal of Political Economy* 115 (February 2007): 1-42.

³⁴⁴ Koleman Strumpf, "Using Markets to Measure the Impact of File sharing on Movie Revenues," *Conference paper* (July 11, 2014), <http://conference.nber.org/confer/2014/SI2014/PRIT/Strumpf.pdf>

³⁴⁵ Chris Taylor, "Hey hollywood, Online Piracy Doesn't Hurt Your U.S. Box Office Returns [STUDY]," *Mashable* (Feb 13, 2012), <http://mashable.com/2012/02/13/online-piracy-box-office/#mTHsb11Q9skl>

³⁴⁶ Stan Liebowitz, "File Sharing: Creative Destruction or Just Plain Destruction?" *Journal of Law and Economics* 49.1 (2006): 1-28.

³⁴⁷ Annelies Huygen et al, "Ups and downs; economic and cultural effects of file sharing on music, film and games." *TNO Information and Communication Technology Series* (2009).

³⁴⁸ Schermer and Wubben, *Feiten om te delen*. P.77.

economic times. A U.S. consumer expenditure survey revealed that 40 % of people who have no computer also bought less music in these years. Also, the decline in sales has not stopped creation. In fact more music albums were released: 75,300 in 2010, which is 25% more than in 2005.³⁴⁹ There is also an increase in concert visits, which could mean that money originally spent on records is now spent elsewhere, but still benefitting the artists.³⁵⁰ Meanwhile the Congressional research service showed that box office revenues for movies have been steadily rising.³⁵¹

All in all it remains a controversial topic for methodological reasons. Research and studies seem to suggest that piracy has affected sales, but these studies suffer from a number of problems. First of all, there appears to be no consensus on how these losses should be measured. Some research focuses on a comparison between regions, some include consumer surveys in which consumers are asked about their downloading and buying coupled with monitoring P2P networks and sales. The biggest problem facing these studies is the problem that it is difficult to predict the exact relation between downloads and sales. According to Considerati, this relation is 'endogenous,' which means factors unknown to researchers exert their influence on sales and downloads. The best way to describe this is that there is no easy measurable causal link between the two.³⁵² Downloading the song does not imply same user would have bought the CD otherwise.³⁵³ The Considerati report says that downloading unlicensed content has a number of negative effects: First of all substitution. This means that the price consumers are willing to pay for a product is the same or higher as the product market price, but turn to downloading instead because it is free. This means a loss in sales. If the price they are willing to pay is lower than the market price, there is no substitution. In other words, substitution happens when consumers will not buy a product they otherwise would have bought, because they can download it for free. Another negative effect could be loss of demand by sampling. Consumers can now try content, and if they do not like the product may decide to stop themselves from buying. Consumers can also trying new content now, which can lead to postponement of buying the actual content. Because prices get lower over time, this is a negative effect for the rights holders. Positive effects of downloading unlicensed content include sampling, and 'Indirect appropriability,' which means that a consumer is willing to pay more for the original if he can copy it and because it can allow for network effects, which means that when more people have a certain type of content, the better or more profitable it is for rights holders.³⁵⁴

Another difficulty is that consumption patterns differ between types of content. Users might prefer actual paper books over eBooks, the experience of going to a concert might benefit from music downloads, and cinema sales are soaring, even though DVD rental stores are shutting down. This is why some studies look at societal welfare. Although copyright infringement undermines certain business models, societal welfare increases by allowing more users to access content.

³⁴⁹ Eduardo Porter, "The Perpetual War: Pirates and Creators," *The New York Times* (Feb 4, 2012), http://www.nytimes.com/2012/02/05/opinion/sunday/perpetual-war-digital-pirates-and-creators.html?_r=3&

³⁵⁰ Julian Sanchez, "Internet Regulation & the Economics of Piracy," *CATO Institute* (Jan 17, 2012), <http://www.cato.org/blog/Internet-regulation-economics-piracy>

³⁵¹ Mike Masnick, "Congressional Research Service Shows Hollywood is Thriving," *TechDirt* (Dec 12, 2011), <https://www.techdirt.com/articles/20111212/02244817037/congressional-research-service-shows-hollywood-is-thriving.shtml>, the link contains full report.

³⁵² Schermer and Wubben, *Feiten om te delen*. P.64-65.

³⁵³ Lessig, *Free culture*. P.56.

³⁵⁴ Schermer and Wubben, *Feiten om te delen*. P.63-64.

A number of studies argue that pirates are the best customers. HADOPI, the French anti-piracy authority paradoxically released this in research, later analyzed and made public by Techdirt.³⁵⁵ A survey from the American Assembly, a think tank, confirms this.³⁵⁶ The European Commission has also done research that says that file sharers buy more music.³⁵⁷ A UK government report also said that the top downloaders are the top spenders.³⁵⁸ Research by the University of Amsterdam says that pirates spend more on legal sales.³⁵⁹ In other words, numerous sources show that pirates tend to spend money on content. Meanwhile, many studies claim that the entertainment market is doing well, but that only specific sections of the industry have been suffering.

Jonathan Band researched the performance of the five leading firms in three copyright intensive industries: motion pictures, publishing, and software. He compared this with the performance of five leading firms in three other industries: construction, transportation, and mining. They also compared the profitability of the firms in those industries. They found that copyright intensive industries were more profitable and performed better than the other industries in the past ten years.³⁶⁰

In 2014 Jonathan Band and Jonathan Gerafi looked at reports “prepared by investment advisors concerning publicly traded companies. These equity research reports make investment recommendations (e.g., buy, hold, or sell) based on the companies’ performance and the risks they face.” They found that “overwhelming majority of the equity research reports did not mention copyright infringement as a possible risk factor.”³⁶¹ This would suggest that even to the entertainment industries themselves, infringement is less of a big deal.

In 2013 Jonathan Band and Jonathan Gerafi also looked at CEO compensation in copyright intensive industries. In their report, they make clear that CEOs of those industries receive “significantly higher compensation” than the CEOs of firms in other industries, like construction, transportation, and mining.³⁶²

Numbers on revenues in the major rights holders industries seem to confirm that those industries are performing quite well under infringement pressure. A report by the Movie industry in 2014 said that the revenue for movie studios went up four percent globally to 34,9 billion dollars, displayed in figure 2.2.³⁶³

³⁵⁵ Mike Masnick, "Another Day, Another Study That Says 'Pirates' Are The Best Customers.. This Time From HADOPI," *TechDirt* (Jul 28, 2011), <https://www.techdirt.com/articles/20110727/16233815292/another-day-another-study-that-says-pirates-are-best-customers-this-time-hadopi.shtml>

³⁵⁶ Joe Karaganis and Lennart Renkema, “Copy culture in the US & Germany,” *the American Assembly* (2013)

³⁵⁷ Luis Aguiar and Bertin Martins, "Digital Music Consumption on the Internet: Evidence from Clickstream Data," European Commission, Joint Research Centre, *Institute for Prospective Technological Studies* (March, 2013), <http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=6084>

³⁵⁸ Kantar Media, "OCI Tracker Benchmark Study, 'Deep Dive' Analysis Report," Prepared for Ofcom (2013), <http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/online-copyright/deep-dive.pdf>

³⁵⁹ Joost Poort and Jorna Leenheer, "File sharing 2@12: Downloading from illegal sources in the Netherlands," *Institute for Information Law & CentERdata*, Amsterdam/Tilburg (2012). Retrieved from http://www.ivir.nl/publications/poort/Filessharing_2012

³⁶⁰ Jonathan Band, "New Study: The Profitability of Copyright-Intensive Industries," *Infojustice.org* (June 17, 2013), <http://infojustice.org/archives/29916>

³⁶¹ Jonathan Band and Jonathan Gerafi, "Infringement Risk in Copyright-Intensive Industries," *Infojustice.org* (Jan 6, 2014), <http://infojustice.org/archives/31827>

³⁶² Jonathan Band and Jonathan Gerafi, "CEO Compensation in the COpyright-Intensive Industries," *Infojustice.org* (Aug 14, 2013), <http://infojustice.org/archives/30466#more-30466>

³⁶³ “Theatrical Market Statistics 2013”, *Motion Picture Association of America*, http://www.mpa.org/wp-content/uploads/2014/03/MPA-Theatrical-Market-Statistics-2013_032514-v2.pdf

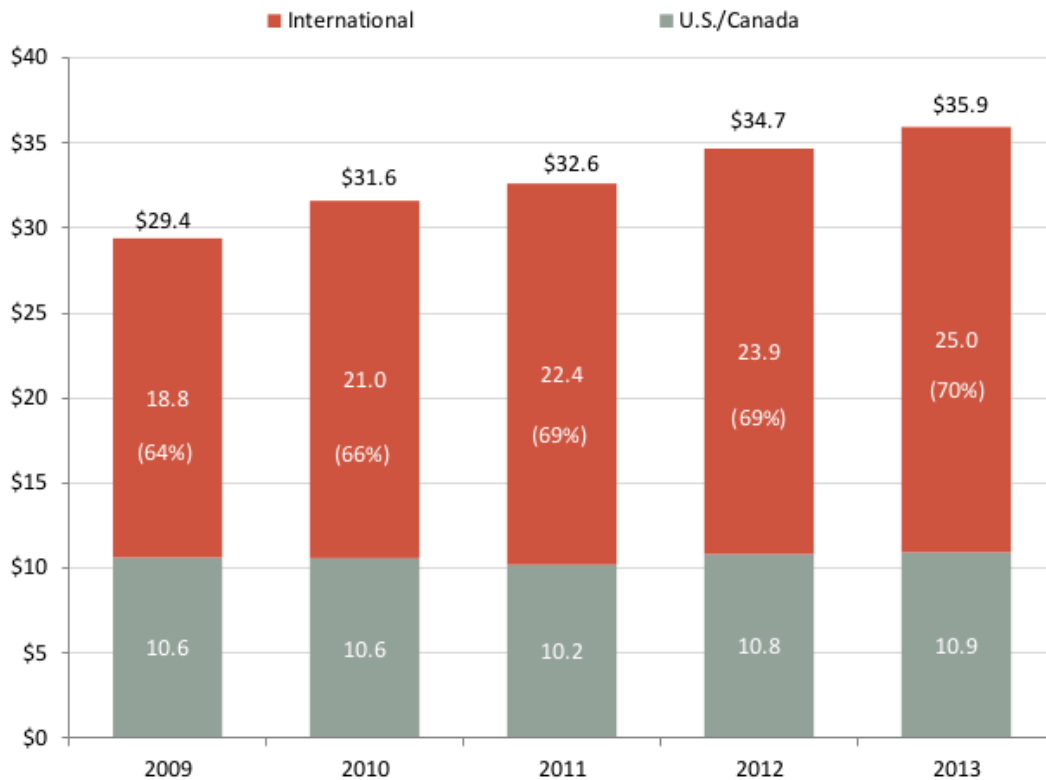


Figure 2.2: Global box office of films (in US\$ Billions).³⁶⁴

In 2013, the number of people employed by the movie industry hit an all time high.³⁶⁵ PRS for Music and others said that the music industry was actually still growing (in spite of analog record sales falling).³⁶⁶ In February 2013, it was revealed that the music industry grew as well. This growth was mainly attributed to digital sales.³⁶⁷ The London School of Economics released a policy brief in which they revealed the music industry was thriving and that policy should be based on that (figure 2.3).³⁶⁸

³⁶⁴ Image source: "Theatrical Market Statistics 2013", *Motion Picture Association of America*, http://www.mpa.org/wp-content/uploads/2014/03/MPAA-Theatrical-Market-Statistics-2013_032514-v2.pdf

³⁶⁵ "All employees: Information: Motion Picture and Sound Recording Industries," *Bureau of Labor Statistics website*, <https://fred.stlouisfed.org/series/CES5051200001>

³⁶⁶ Will Page and Chris Carey, "Adding Up the Music Industry for 2008", *PRS for Music* (2009), [http://www.prsformusic.com/creators/news/research/Documents/Will%20Page%20and%20Chris%20Carey%20\(2009\)%20Adding%20Up%20The%20Music%20Industry%20for%202008.pdf](http://www.prsformusic.com/creators/news/research/Documents/Will%20Page%20and%20Chris%20Carey%20(2009)%20Adding%20Up%20The%20Music%20Industry%20for%202008.pdf)

³⁶⁷ Eric Pfanne, "Music Industry Sales Rise, and Digital Revenue Gets the Credit," *The New York Times* (Feb 26, 2013), http://www.nytimes.com/2013/02/27/technology/music-industry-records-first-revenue-increase-since-1999.html?_r=0

³⁶⁸ Bart Cammaerts et al, "Copyright & Creation", *Media Policy Brief*, *London School of Economics* (Sept 2013), <http://blogs.lse.ac.uk/mediapolicyproject/>

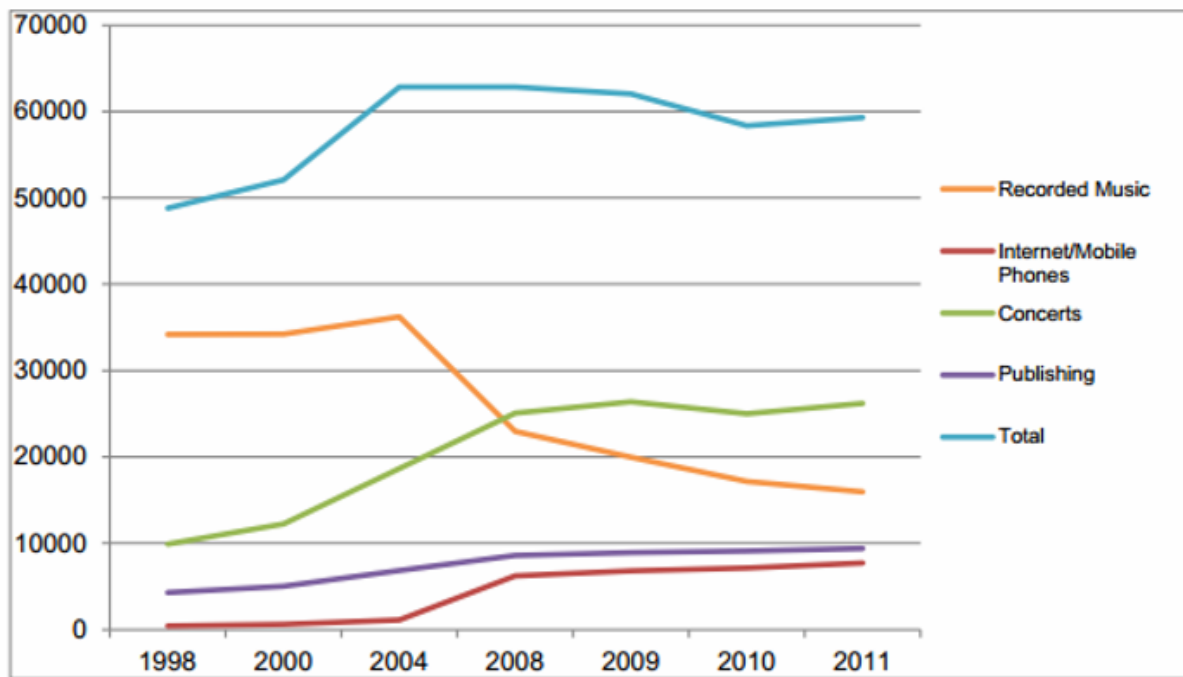


Figure 2.3: Trends in total revenue of the music industry, USD Million.³⁶⁹

Country specific reports on for example Canada³⁷⁰, Sweden,³⁷¹ And Norway³⁷² paint a similar picture. Techdirt has released ‘The sky is rising’ report, in which they cite other research. They claim that more books are published each year, that the eBook market is growing, video game revenues are up, and that video and music are up as well.³⁷³

Lunney and Glynn revealed that the rise of file sharing did limit revenue in the music market, but that it also meant that more new music was created.³⁷⁴ The bureau of labor statistics also showed massive growth in independent artists in 2013.³⁷⁵

However, other researchers say that file sharing limits diversity: Hervas-Drane and Noam analyzed the cross border implications of the Internet on the cultural sector and found that consumer online sharing has short term effects: producers cut prices, consumers download more foreign content (due to less import barriers). This is desirable: less import costs is less wasteful. However, it homogenizes consumption patterns across countries and

³⁶⁹ Image source: Bart Cammaerts et al, "Copyright & Creation", *Media Policy Brief*, London School of Economics (Sept 2013), <http://blogs.lse.ac.uk/mediapolicyproject/>

³⁷⁰ Dwayne Winseck, "Restrictive copyright plays into music industry myths," *The Globe and Mail* (May 17, 2011), <http://www.theglobeandmail.com/technology/digital-culture/restrictive-copyright-plays-into-music-industry-myths/article624736/#articlecontent>

³⁷¹ Mike Masnick, "More Charts The Record Labels Don't Want You To See: Swedish Musicians Making More Money," *TechDirt* (Dec 14, 2009), <https://www.techdirt.com/articles/20091213/1648377324.shtml>

³⁷² Image source: Richard Bjerko and Anders Sorbo, "The Norwegian Music Industry in the Age of Digitalization," *BI Norwegian School of Management - Thesis* (September 2010), <http://www.scribd.com/doc/37406039/Thesis-Bjerko-Sorbo>

³⁷³ Michael Masnick and Michael Ho, *The Sky is Rising, a detailed look at the state of the entertainment industry*, (Jan 2012), <https://www.techdirt.com/skyisrising/>

³⁷⁴ Glynn Lunney, Jr., "Empirical Copyright: A Case Study of File Sharing and Music Output," *Tulane Public Law Research Paper No. 14-2* (January 2014), Available at <http://dx.doi.org/10.2139/ssrn.2372630>

³⁷⁵ Mike Masnick, "Massive Growth In Independent Musicians & Singers Over The Past Decade," *TechDirt* (May 30, 2013), <https://www.techdirt.com/blog/casestudies/articles/20130529/15560423243/massive-growth-independent-musicians-singers-over-past-decade.shtml>

reduces volume of production. Also drives consumers to consume the same content, it reduces cultural diversity in the world economy.³⁷⁶

Some of the reports show that business is not necessarily declining, but that business models are shifting. Peter di Cola did a large analysis of artist interviews and revealed that as many musicians as file sharing hurts them as say that it helps them, and that musicians were only dependent on music sales for 50% of their income (figure 2.4).³⁷⁷ The Future of Music Coalition recently concluded a survey of musicians, which found that only six percent of artist revenue comes from sound recordings; two-thirds of respondents received zero income from recordings.³⁷⁸

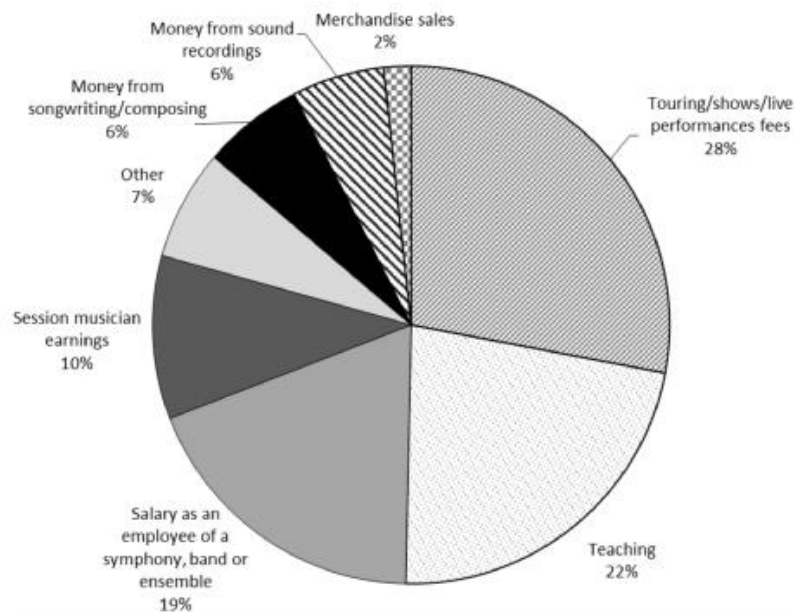


Figure 2.4: average share of music income from major revenue streams, all respondents.³⁷⁹

This means that missed income through declining record sales could be compensated elsewhere. Dutch website Sargasso revealed that the price of concert tickets in the Netherlands went up (figure 2.5).³⁸⁰ This could be an example for those compensating revenue streams.

³⁷⁶ Andres Hervas-Drane and Eli M. Noam, "Peer-to-Peer File Sharing and Cultural Trade Protectionism," (September 2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1793131

³⁷⁷ Peter DiCola, "Money from Music: Survey Evidence on Musicians' Revenue and Lessons About Copyright Incentives," *Arizona Law Review, Forthcoming; Northwestern Law & Econ Research Paper No. 13-01* (January 9, 2013), Available at SSRN: <http://ssrn.com/abstract=2199058>

³⁷⁸ "Mythbusting: Data Driven Answers to Four Common Assumptions About How Musicians Make Money," *Future of Music Coalition* (Dec. 13, 2012), <http://money.futureofmusic.org/mythbusting/4/>

³⁷⁹ Image source: Peter DiCola, "Money from Music: Survey Evidence on Musicians' Revenue and Lessons About Copyright Incentives," *Arizona Law Review, Forthcoming; Northwestern Law & Econ Research Paper No. 13-01* (January 9, 2013), Available at SSRN: <http://ssrn.com/abstract=2199058>

³⁸⁰ Stephan Ockhuijsen, "Stijgende prijs pop- en rockconcertkaartjes bevestigd," *Sargasso.nl* (March 28, 2013), <http://sargasso.nl/stijgende-prijs-pop-en-rockconcertkaartjes-bevestigd/>

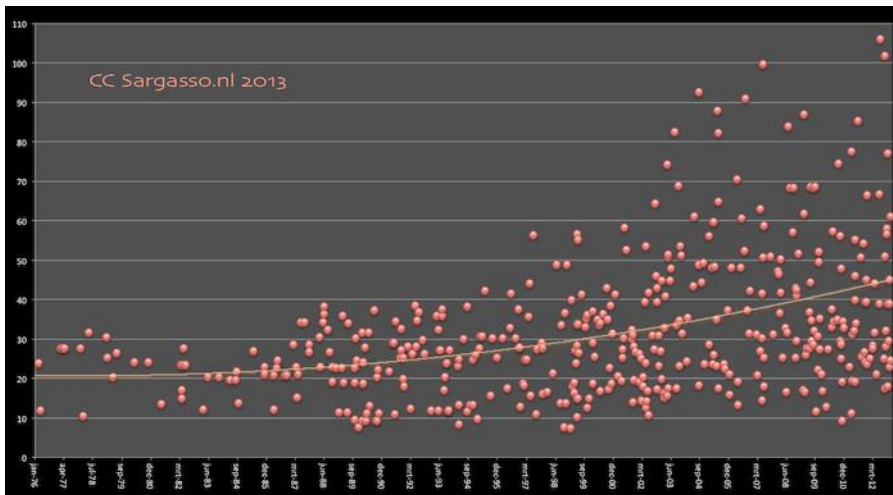


Figure 2.5: price concert tickets in the Netherlands between 1976 – 2012 in Euros, corrected for inflation.³⁸¹

Another big business change has come from new Internet distribution. YouTube for example paid out 1 billion in music payouts alone, it was revealed in 2014.³⁸²

These new platforms are growing. Netflix and YouTube recently surpassed 50% of all Internet traffic, much higher than BitTorrent.³⁸³ A report by Generator research predicts that online movie streaming can be as profitable as TV or disc sales.³⁸⁴ Price Waterhouse Coopers predicts that online sales of music will displace CD sales in 2015.³⁸⁵

Some argue that subscription services like Spotify are unprofitable.³⁸⁶ But Spotify has helped the Swedish music market get back to levels of 2004. The market has gone up by 30%, a report says.³⁸⁷ Payouts are increasing, the company itself says.³⁸⁸ In 2011, Spotify had paid over \$100 million to rights holders since its launch, a large portion of which went to the independent (“indie”) music community.³⁸⁹

Wired magazine called it the “neo-Napster transformation,” “in which music is

³⁸¹ Image source: Stephan Ockhuijsen, "Stijgende prijs pop- en rockconcertkaartjes bevestigd."

³⁸² Stuart Dregde, "YouTube reveals \$1bn music payouts, but some labels still unhappy," *The Guardian* (Feb 3, 2014), <http://www.theguardian.com/technology/2014/feb/03/youtube-reveals-1bn-music-payouts-but-some-labels-still-unhappy>

³⁸³ Joshua Brustein, "Netflix and YouTube Dominate Online Video. Can Amazon Catch Up?," *Bloomberg Business* (Nov 11, 2013), <http://www.businessweek.com/articles/2013-11-11/netflix-and-youtube-dominate-online-video-dot-can-amazon-catch-up>

³⁸⁴ Lucas Mearian, "Online movie streaming can be profitable as TV, disc sales," *Computerworld* (Jan 23, 2014), http://www.computerworld.com/s/article/9245666/Online_movie_streaming_can_be_profitable_as_TV_disc_sales

³⁸⁵ "Muziek via Internet verslaat cd in 2015," *Nu.nl* (Aug 27, 2013), <http://www.nu.nl/tech/3560636/muziek-via-Internet-verslaat-cd-in-2015.html>

³⁸⁶ Lucas Mearian, "Music industry sucks life from subscription services," *Computerworld* (Feb 14, 2014), http://www.computerworld.com/s/article/9246365/Music_industry_sucks_life_from_subscription_services?taxonomyId=71&pageNumber=1

³⁸⁷ "Spotify helps Swedish music sales rise 30.1% in first half of 2012," Music Ally site (July 13, 2012), <http://musically.com/2012/07/13/spotify-sweden-ifpi-figures/>

³⁸⁸ Elliot Van Buskirk, "Report Shows Big Increase in Spotify's Payouts to Indie Labels (Updated)," *Evolver.fm* (May 8, 2012) <http://evolver.fm/2012/05/08/confidential-report-shows-big-increase-in-spotifys-payouts-to-indie-labels/>

³⁸⁹ Bruce Houghton, "Spotify Offers Additional Response to Independent Label Defections," *Hypebot.com* (Sept. 20, 2011), <http://www.hypebot.com/hypebot/2011/09/spotify-offers-additonal-response-to-independent-label-defections.html>

streamed from a collection of servers, rather than stored on local hard drives.”³⁹⁰ Major Internet companies, including Apple, Amazon, and Google, have launched services similar to the Facebook and Spotify connection.³⁹¹ All these cloud services might “clear . . . the psychological attachment that people have to owning their music. Once songs live in the cloud—hand customers pay rent to store them (which Apple intends to launch)—it is a small step to do away with the concept of ownership all together.”³⁹²

Apple’s iTunes sold its 100 millionth song in 2011 and was negotiating with Hollywood to stream movies through iTunes.³⁹³ Kindle books (e-books) were already outselling ordinary books in the Amazon store at the time of this research,³⁹⁴ and new platforms similar to iTunes were being launched for eBooks, like CalibrE and Apple’s own iBooks 2.³⁹⁵

The access to free content has apparently in some cases increased sales or aided remuneration of artists through parallel sales. Spotify has apparently increased iTunes sales.³⁹⁶ YouTube has actually devised new ways to allow artists to make money, including through partner programs for visible channels and sharing advertising revenues.³⁹⁷ It has also created a “Merch” store that will allow fans to buy merchandise directly on their channels, as well as digital downloads, concert tickets, or possibly meetups.³⁹⁸

Some say that a proper evaluation of industry, should also take into account how funds are being spread within rights holders’ studios. Some say movie studios keep too much for themselves without actually rewarding creativity.³⁹⁹ Although rights holders and especially collective rights organizations have come under increased scrutiny, there is still criticism on how they divide funds. Collective rights organization BUMA in the Netherlands for example, has been criticized for not evenly paying artists for music distributed through Internet channels, like Spotify.⁴⁰⁰

³⁹⁰*The Second Coming*, Wired Magazine (Nov. 7, 2011), <http://castroller.com/Podcasts/WiredFeatures/2678827>

³⁹¹ *The Second Coming*, Wired Magazine (Nov. 7, 2011), <http://castroller.com/Podcasts/WiredFeatures/2678827>

³⁹²*The Second Coming*, Wired Magazine (Nov. 7, 2011), <http://castroller.com/Podcasts/WiredFeatures/2678827>

³⁹³Ben Fritz, “Apple prepping movie cloud service,” *LA Times* (Oct. 12, 2011), <http://latimesblogs.latimes.com/entertainmentnewsbuzz/2011/10/apple-prepping-movie-cloud-service-devices-may-work-with-ultraviolet.html>

³⁹⁴ Brandon Griggs, “Amazon e-Books Now Outselling Print Books,” *CNN* (May 19, 2011), <http://edition.cnn.com/2011/TECH/gaming.gadgets/05/19/kindle.outsells.books/index.html?hpt=T2>

³⁹⁵ “Calibre Ebook management,” <http://calibre-ebook.com/>

³⁹⁶ Zach Shaw, “Earache Records Responds to Spotify Press Release,” *Metal Insider* (Aug. 10, 2011, 12:47 PM), <http://www.metalinsider.net/digital-media/exclusive-earache-records-responds-to-spotify-press-release>

³⁹⁷ Christian Weitenberner, “New YouTube Features for Music Artists,” *The Official YouTube Blog* (Oct. 16, 2011), <http://youtube-global.blogspot.com/2011/10/new-youtube-features-for-music-artists.html/>

³⁹⁸ Christian Weitenberner, “New YouTube Features for Music Artists,” *The Official YouTube Blog* (Oct. 16, 2011), <http://youtube-global.blogspot.com/2011/10/new-youtube-features-for-music-artists.html/>

³⁹⁹ Derek Thompson, “How Hollywood accounting can make a \$450 million dollar movie unprofitable”, *The Atlantic* (September 14, 2011), see: <http://www.theatlantic.com/business/archive/2011/09/how-hollywood-accounting-can-make-a-450-million-movie-unprofitable/245134/>

⁴⁰⁰ Joris Zwetsloot, “Buma Stemra betaalt te weinig voor online muziek,” *de Volkskrant* (June 1, 2015)

3. LARGE-SCALE ENFORCEMENT

3.1 Introduction to this chapter

The previous chapter has shown that copyright infringement happens on a large scale and in a number of ways. The scale on which infringement takes place has remained relatively stable. Depending on the region, 15% to 70% of the population has infringed on copyright. While it is unclear what the exact effect of this on the entertainment economy is, most research suggests the losses are concentrated in a certain sector of that economy. The overall welfare effects are not clear and might even be positive.

This chapter shows one of the ways in which rights holders have tried to respond to this infringement: by seeking increased enforcement of copyright via gaining more control over the technologies through which their content is distributed. The previous chapter showed that a key problem that rights holders are trying to solve is scale. Since infringement is widespread, enforcement efforts also need to impact at a large scale. Dealing with infringement on a case-by-case basis is too costly in terms of time and money, especially when judicial procedures have to be followed.

In response, rights holders have adopted new strategies to scale up enforcement, which can be categorized into four groups: (1) they target the demand for infringing content (end-users) directly on a large scale by aiming for settlements instead of actual lawsuits. (2) They target end-users indirectly through the introduction of graduated response procedures. These procedures use a system of increasingly severe sanctions for each infringement to deter users, often starting with a warning letter and ending with Internet disconnection or fines as the ultimate sanction if infringement keeps happening. These procedures require intermediaries in the administration of sanctions. (3) They target the supply side directly by taking down or filtering complete websites that offer infringing content. Governmental parties often carry out these procedures. (4) They target the supply side indirectly by taking down infringing content on other websites. Notice and takedown procedures allow rights holders to notify websites of infringement and require them to take this content down.

3.2 New enforcement strategies: scaling-up

Today national copyright laws have been standardized to some extent through international and regional agreements such as the Berne Convention and the European copyright directives. This Berne convention was succeeded in 1967 with the establishment of the World Intellectual Property Organization (WIPO) by treaty as an agency of the United Nations. Copyright is now largely recognized as a fundamental principle in western society. It has been included in the Universal declaration of human rights,⁴⁰¹ and has been incorporated in the international Covenant on Economic, Social and Cultural rights.⁴⁰² It has

⁴⁰¹ Article 27 of the Universal Declaration of Human Rights says that '(1) Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits, and (2) Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.'

⁴⁰² Article 15 states that: '1. The States Parties to the present Covenant recognize the right of everyone: (a) To take part in cultural life; (b) To enjoy the benefits of scientific progress and its applications; (c) To benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production of

been standardized more or less through other international treaties, regional agreements and legislation. The WTO agreement on trade related aspects of intellectual property rights (TRIPS) is an international agreement that laid down minimum standards of intellectual property protection. Becoming a member of the WTO requires ratification of this TRIPS agreement.⁴⁰³ The latter requires each WTO member to implement appropriate measures to prevent the abuse of intellectual property rights, like efficient enforcement procedures, measures to prevent infringement, and criminal procedures to fight copyright piracy on a commercial scale. After TRIPS, countries have sought to further develop copyright laws through bilateral free trade agreements and economic partnership agreements.

Multilaterally, the WIPO copyright treaty (WCT) and WIPO performance and phonogram treaty (WPPT) were the first change to specifically combat copyright infringement online. Rights holders have attempted to further combat infringement multilaterally through for example the Anti-Counterfeiting Trade Agreement, negotiated from 2008 between several countries, which aimed to increase international standards for IP enforcement. Although the treaty was signed by the participating countries, it was not ratified after the European Parliament rejected it after much protest.

Within the Council of Europe the convention on cybercrime was adopted (Budapest convention) and entered into force in July 2004.⁴⁰⁴ Non-Council of Europe countries like for example Australia, Japan, US and Canada ratified as well. It deals with crimes committed via the internet, particularly linked to copyright. Article 10 of that convention established that each party had to establish criminal offenses under its law for the infringement of copyrights.

Within the EU framework, numerous laws have aimed to increase copyright enforcement and to transpose the WCT and WPPT in EU law. The InfoSoc Directive⁴⁰⁵ harmonised several essential rights (reproduction right, distribution right, right of communication to the public of works and right of making available to the public) of authors and rightsholders (performers, phonogram producers, film producers and broadcasting organisations), as well as the limitations and exceptions to these rights. It also granted rights holders protection against circumvention of technological protection measures. The Enforcement Directive⁴⁰⁶ of 2004 aimed to create a level playing field for enforcement of IPR in different EU countries, by harmonising enforcement measures across the EU. It contained provisions on civil law measures, damages, corrective measures and evidence, while also containing provisions on injunctions or seizures of suspected goods,⁴⁰⁷ and permanent

which he is the author, 2. The steps to be taken by the States Parties to the present Covenant to achieve the full realization of this right shall include those necessary for the conservation, the development and the diffusion of science and culture, 3. The States Parties to the present Covenant undertake to respect the freedom indispensable for scientific research and creative activity, 4. The States Parties to the present Covenant recognize the benefits to be derived from the encouragement and development of international contacts and co-operation in the scientific and cultural fields.'

⁴⁰³ Lessig, *Free culture*. P.51.

⁴⁰⁴ Convention on Cybercrime, Budapest, 23.11.2001, <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

⁴⁰⁵ Information society directive Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32001L0029>

⁴⁰⁶ Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004L0048R%2801%29>

⁴⁰⁷ Article 9.

injunctions.⁴⁰⁸ It also stimulated the development of self-regulation.⁴⁰⁹ The E-Commerce Directive harmonized a special liability regime for certain types of online intermediaries.⁴¹⁰ It for example created liability exemptions for intermediaries⁴¹¹ and included a provision that member states would not impose a general obligation on intermediaries to monitor their networks.⁴¹² It also encouraged the creation of 'Codes of Conduct' for self-regulation to combat infringement.⁴¹³

Through these regulatory initiatives, rights holders have looked to combat copyright infringement on the internet, and to scale up enforcement. Consumers take the risk of getting caught into account when infringing on copyrights, which would imply that large-scale infringement requires large-scale enforcement.⁴¹⁴ The two most important ways to enforce copyrights are through civil remedies and through criminal sanctions (the latter for large/commercial scale infringement). For civil remedies enforcement is intended to compensate economic injury suffered as a result of infringement and as a deterrent to further infringement. Criminal sanctions are intended to punish and deter further infringement.⁴¹⁵ Enforcement online is difficult. P2P networks operate anonymously, so in to discover users for enforcement purposes, enforcers are dependent on IP addresses identified by ISPs. This requires help by ISPs. Also, as mentioned before, getting an IP address does not mean it identifies the actual user infringing.

To discover infringing content, enforcers usually depend on surveillance programs. They use particular types of monitoring, performed by private, non-governmental entities, that maintain extra-judicial determinations of copyright infringement, and are extra-legal in nature (outside of litigation).⁴¹⁶ This has led to the creation of industries of anti-piracy enforcement technologies. Companies like Audible Magic scan online for copyright material, and check it with a huge database of content. Other companies are Gracenote, Advestigo, Auditude, Vobile, and Attributor.⁴¹⁷

Enforcement is also complicated. It contains a wide range of subject matter (ranging from literary works to performances), a wide range of infringers (ranging from kids downloading music to international cartels), and a wide range of enforcers (ranging from different civil entities like the copyright holders to enforcers in the form of the state).⁴¹⁸

The WIPO copyright treaties of 1996 formed the first significant change to facilitate copyright protection in the online environment. These treaties have been implemented in the USA through the Digital Millennium Copyright Act (DMCA) and in the EU through the copyright directives, and extended copyright protection to computer programs. According to

⁴⁰⁸ Article 11.

⁴⁰⁹ Article 17.

⁴¹⁰ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), <http://eur-lex.europa.eu/legalcontent/en/ALL/?uri=CELEX:32000L0031>

⁴¹¹ Article 12-14.

⁴¹² Article 15.

⁴¹³ Article 16.

⁴¹⁴ Chris Dent, "Copyright as (Decentered) Regulation: Digital Piracy as a Case Study." *Monash UL Rev.* 35 (2009): 348. P.361-362.

⁴¹⁵ "Enforcement of rights," *World Intellectual Property Organisation*.

⁴¹⁶ Sonia Katyal, "Filtering, Piracy Surveillance, and Disobedience." *Columbia Journal of Law & the Arts* 32.4 (2009). P.405.

⁴¹⁷ Katyal, "Filtering, Piracy Surveillance, and Disobedience."

⁴¹⁸ Chris Dent, "Copyright as (Decentered) Regulation: Digital Piracy as a Case Study." *Monash UL Rev.* 35 (2009): 348. P.349.

Bridy, these laws aimed to achieve a dual objective: to safeguard the important contribution of private players like intermediaries to Internet growth, and to deal with massive copyright infringement by scaling up enforcement. To achieve this objective, the laws introduced the safe harbor provisions and notice and takedown procedures, which would allow rights holders to combat infringement on a large scale.⁴¹⁹ They also made it illegal to circumvent measures that control access to copyrighted works like DRM, and criminalized production and dissemination of technology, devices, or services intended to circumvent those measures, whether or not there is actual infringement of copyright itself.⁴²⁰ In addition, the DMCA heightened the penalties for copyright infringement on the Internet.

The industry reacted to the advent of file sharing through the Internet through litigation; they first sued the intermediaries whose “sole purpose it was to enable illegal file sharing”, like Napster. After Napster, RIAA sued other P2P platforms, like Scour, Aimster, AudioGalaxy, Morpheus, Grokster, KaZaA, iMesh, and Limewire.⁴²¹ However, with the fall of each P2P file sharing platform, a new one has arisen, leading to a technological arms race.⁴²²

The notice and takedown provisions would acquit intermediaries of any liability if, upon gaining knowledge of copyright infringing activities by their customers or subscribers, they would act and prevent the copyright infringement. These provisions have been laid out in two main global models, that of the EU (mentioned above) and the US (Digital Millennium Copyright Act).⁴²³ In some member states of the EU, these notice and takedown procedures were further developed through self-regulatory codes of conduct. Another legal instrument in the DMCA granted rights holders the ability to obtain the identities of alleged infringers by serving subpoenas to intermediaries accompanied by a notice of infringement.⁴²⁴

According to Bridy, the notice and takedown was initially successful as an enforcement procedure. Upon receiving a notice by a rights holder that one of the intermediaries’ customers or subscribers is engaged in copyright infringing activities, the intermediary is obligated to remove or takedown the infringing content.⁴²⁵ According to Bridy, the upside of this approach was that it could scale successfully. Rights holders could send thousands of notices to have intermediaries take infringing content down. In fact, intermediaries facilitated this large-scale enforcement by allowing for automated

⁴¹⁹ Bridy, “Is Online Copyright Enforcement Scalable?”

⁴²⁰ Section 1201 (a) (1) of the DMCA states “no person shall circumvent a technological measure that effectively controls access” of a copyrighted work. Sections 1201 (a) (2) and 1201 (b) state that “no person shall manufacture, import, offer to the public, provide, or otherwise.”

⁴²¹ *Through*: Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008), <https://www.eff.org/wp/riaa-v-people-five-years-later>, and: Courtney Macavinta, “Recording Industry Sues Music Start-up, Cites Black Market,” *CNET News.com* (December 7, 1999), <http://www.cnet.com/news/recording-industry-sues-music-start-up-cites-black-market/>. Thomas C. Green, “MPAA, RIAA Sue Scour Over Copyrights,” *The Register*, (July 24, 2000). John Borland, “RIAA Sues Aimster Over File-Swapping,” *CNET News.com* (May 25, 2001). John Borland, “Suit Hits Popular Post-Napster Network,” *CNET News.com* (October 3, 2001). John Borland, “Audiogalaxy hit by RIAA suit,” *CNET News.com* (May 24, 2002). John Borland, “RIAA sues iMesh file-trading firm,” *CNET News.com* (September 19, 2003). Ed Oswald, “RIAA Sues LimeWire Over Piracy,” *BetaNews* (August 4, 2006), <http://betanews.com/2006/08/04/riaa-sues-limewire-over-piracy/>.

⁴²² Lillian Edwards, *Role and responsibility of the Internet intermediaries in the field of copyright and related rights*, (Geneva: World Intellectual Property Organisation, 2011). P.19-21.

⁴²³ Jeremy De Beer and Christopher Clemmer, “Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?.” *Jurimetrics* (2009): 375-409. p.375-376.

⁴²⁴ Bridy, “Is Online Copyright Enforcement Scalable?” P.712-713.

⁴²⁵ De Beer and Clemmer, “Global Trends in Online Copyright Enforcement. P.375-376

notification procedures (YouTube offers an online interface, like Facebook, allowing for notice and takedown in large numbers).⁴²⁶

But the notice and takedown procedure proved unsuccessful to scale for P2P networks. They are distributed networks, and membership to those networks is anonymous and dynamic.⁴²⁷ This led the industry to fall back on one of its first legal reactions to the advent of file sharing through the Internet; to sue users involved in file sharing, whilst continuing to sue P2P platforms. Since the advent of file sharing over the Internet, the entertainment industry in the USA filed over thousands of lawsuits against individual file sharers and P2P intermediaries, to stop file sharing.⁴²⁸

Suing individual users has proven costly in PR terms. According to Rolling Stone magazine, it has made the content industries “the most hated industry since the tobacco industry.”⁴²⁹ Partly, because suing individual users has been prone to error. The industry filed ‘John Doe’ lawsuits, based on IP addresses, in the hope of identifying infringing users in the legal process. But as an IP address is not a user, this led to a number of eye-catching (and often hilarious) indictments, the most notable being the case that was filed against a dead grandmother with no access to Internet,⁴³⁰ a blind man for downloading pornography⁴³¹ and a hockey stadium.⁴³²

However, the lawsuits have not been able to curb massive online infringement. BitTorrent made enforcement difficult, allowing for decentralized protocols which make it incredibly difficult to identify and close down one central chokepoint to prevent users to access content. BitTorrent is an open source protocol, instead of proprietary like Napster, which prevents it from being targeted in a lawsuit. Furthermore, BitTorrent sites pread internationally, which makes it hard to target them in a lawsuit. A well-known example of this is the Pirate Bay, a Swedish website hosting 'torrents'. Even though the Pirate Bay lost a lawsuit in Sweden and was summoned to take the website down, the website was still up at the time of this research. The Pirate Bay moved its site to another jurisdiction after each takedown.

In the EU, rights holders have been hesitant to pursue individual file sharers. In part, this is because of European privacy legislation. In the Promusicae case, the CJEU ruled that rights holders could not force ISPs to hand over subscribers’ identity in a civil copyright suit, but that the Privacy Directive did not prevent member states from creating an obligation to disclose personal data for civil proceedings. However, a fair balance had to be struck with fundamental rights.⁴³³

Some countries tried to increase the penalties that may be awarded to individual users for file sharing. However, this has been ineffective. Sweden introduced IPRED

⁴²⁶ Bridy, “Is Online Copyright Enforcement Scalable?” P.713-714.

⁴²⁷ Bridy, “Is Online Copyright Enforcement Scalable?” P.716.

⁴²⁸ Edwards, *Role and responsibility of the Internet intermediaries*, P.17.

⁴²⁹ “RIAs gaze turns from users to ISPs in piracy fight,” *Rolling Stone Magazine* (December 19, 2012), <http://www.rollingstone.com/rockdaily/index.php/2008/12/19/riaas-gaze-turns-from-users-to-isps-in-piracy-fight/>

⁴³⁰ Peter Yu, “the Graduated Response,” *Florida Law Review* 62 (2010): 1373-1430. P.16-17.

⁴³¹ Keegan Hamilton, “Porn, Piracy and Bit Torrent,” *Seattle Weekly* (August 10, 2011)

<http://www.seattleweekly.com/2011-08-10/news/porn-piracy-bittorrent/>

⁴³² Mike Masnick, “Hurt locker file sharing lawsuit lists hockey stadium IP address,” *Techdirt* (September 28, 2011), <http://www.techdirt.com/articles/20110928/02302616122/hurt-locker-file-sharing-lawsuit-lists-hockey-stadium-ip-address.shtml>

⁴³³ CJEU Case C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, 29 January 2008.

legislation, which in first instance led to a 30% drop in Internet traffic. But 8 months later, file sharing traffic was back to normal. Some argued that there was even more P2P traffic.⁴³⁴ According to a cyber norms sociological research project, file sharers were simply getting better at hiding their identities online.⁴³⁵

Rights holders have therefore looked towards more efficient ways to exert pressure on illegal file sharers online.⁴³⁶ Internet intermediaries distribute, host and locate content, and thus play a vital role in the information society.⁴³⁷ This makes them a suitable candidate to exercise control over what happens in their networks. According to De Beer & Clemmer, intermediaries more actively police their networks, to filter content and voluntarily cooperate in copyright enforcement processes.

Rights holders have for example tried to use the law to force intermediaries to more actively combat infringement. In the CJEU case of *L'Oréal v. eBay* the court stated that the third sentence of Article 11 of the Enforcement Directive "must be interpreted as requiring the Member States to ensure that the national courts with jurisdiction in relation to the protection of intellectual property rights are able to order the operator of an online marketplace to take measures which contribute, not only to bringing to an end infringements of those rights by users of that marketplace, but also to preventing further infringements of that kind. Those injunctions must be effective, proportionate, and dissuasive and must not create barriers to legitimate trade."⁴³⁸

Similarly, rights holders have created new self-regulatory initiatives to combat infringement. These self-regulatory initiatives have practical advantages over legislation, because they are more precisely geared towards the needs industry, generated and revised much quicker and therefore more flexible, and they may be more effective.⁴³⁹ However, he also says they raise human rights objections and suffer from a 'democratic deficit'.⁴⁴⁰

The increased cooperation between rights holders and intermediaries is demonstrated by a shift in laws, agreements, treaties and case law. There are multiple ways in which this more active cooperation between rights holders and intermediaries take form: intermediaries play an active role in regulating the behavior of their clients. They can send warnings to users who infringe upon copyrights, monitor traffic from and to users, cut down services to certain users (slowing their connection for example) or cut them off from the Internet all together. Another way of cooperation is by blocking access to certain websites, like cyber lockers.⁴⁴¹ The OECD distinguishes four different ways of cooperation: Notice and notice, notice and takedown, graduated response and filtering.⁴⁴²

Filtering consists of blocking access to websites that infringe on copyrights, or by examining Internet traffic to see whether or not it contains copyright infringing content

⁴³⁴ Enigmax, "Swedish Internet traffic recovers after initial IPRED scare," *Torrentfreak* (November 13, 2009), <http://torrentfreak.com/swedish-Internet-traffic-recovers-after-initial-ipred-scare-091113/>.

⁴³⁵ Ernesto, "Millions of file-sharers hide their identities online," *Torrentfreak* (November 3, 2009), <http://torrentfreak.com/millions-of-file-sharers-hide-their-identities-online-091103/>.

⁴³⁶ Eliot van Buskirk, "RIAA to stop suing music fans, cut them off instead," *Wired* (December 19, 2008), <http://www.wired.com/epicenter/2008/12/riaa-says-it-pl/>

⁴³⁷ Edwards, *Role and responsibility of the Internet intermediaries*, P.3.

⁴³⁸ CJEU Case C-324/09, *L'Oréal SA v. International AG*, 12 July 2011.

⁴³⁹ Bernt Hugenholtz, "Codes of Conduct and Copyright Enforcement in Cyberspace," *Copyright enforcement and the Internet, Information law series 21* (2012): 303-320. P.307.

⁴⁴⁰ Bernt Hugenholtz, "Codes of Conduct and Copyright Enforcement in Cyberspace," P.319.

⁴⁴¹ Edwards, *Role and responsibility of the Internet intermediaries*, P.22.

⁴⁴² Edwards, *Role and responsibility of the Internet intermediaries*, P.57-69.

(through deep packet inspection (DPI)).⁴⁴³ Both approaches have surfaced as ways to combat online copyright infringement, like in the originally proposed protect IP act in the US. Also, private agreements have surfaced to block cyber lockers and file sharing websites.⁴⁴⁴

There has also been pressure on intermediaries in the EU and the US to use deep packet inspection. This technique has to be implemented by network operators and would work with a fingerprinting model. Using a vendor's software to generate a unique signature for each protected object, DPI analyzes the traffic of an IP network in real time and inspects all the information in the packets. It can recognize objects in a bit stream and can then notify or manipulate. For example, it can for example limit BitTorrent traffic or recognize requests for URLs and censor websites by blocking access to them.⁴⁴⁵

Mueller writes that DPI for copyright enforcement does not serve the economic interests of ISPs. It benefits rights holders, but imposes administrative and hardware costs on the ISPs, undermines their immunities and alienates or cuts off customers. ISPs would therefore not implement DPI out of their own will.⁴⁴⁶ It has also been controversial, and has faced heavy resistance by consumer rights, civil rights and ISPs.⁴⁴⁷ Similarly, in discussions by stakeholders to make the IPR enforcement directive (2004/48/EC) more effective, technical measures like DPI were rejected as ineffective, detrimental to the operation of networks and harmful to innovation.⁴⁴⁸ Engineering studies brought to light the scalability limitations of DPI for copyright enforcement.⁴⁴⁹

Although the E-Commerce directive prohibits a general monitoring obligation, it does allow for specific injunctions against ISPs. Therefore, rightsholders have asked national courts of the EU member states to issue filtering and/or blocking injunctions against ISPs hosting and providing access to copyrighted content. The CJEU in some ground breaking cases has made a clear distinction between filtering measures, which are used to detect copyright infringements but require some form of pre-emptive monitoring of networks, and blocking measures, which basically impede access to copyrighted material. Also, in the *Scarlett v SABAM* case the court ruled that installing DPI to prevent copyright infringements for all electronic communications among all its customers as a preventive measure and for an unlimited time was illegal.⁴⁵⁰

In the US, the DMCA safe harbor prevented the imposition of technical measures like DPI.⁴⁵¹ Rights holders have therefore tried to pressure higher education institutions to implement DPI measures against infringement.⁴⁵² Despite opposition, the final version of the Higher Education Opportunity Act passed July 31, 2008 and was signed into law August 14 of that year. By threatening educational institution's federal funding, this legislation helped to create an incentive structure that nudged many universities into graduated response

⁴⁴³ Edwards, *Role and responsibility of the Internet intermediaries*, P.23.

⁴⁴⁴ "UK ISPs to block the pirate bay and other file sharing sites," *Unite the Cows*, <http://www.unitehecows.com/content/366-uk-isp-s-block-pirate-bay-other-file-sharing-sites.html>, retrieved on 26-10-2011.

⁴⁴⁵ Milton Mueller, Andreas Kuehn, and Stephanie Michelle Santoso, "Policing the network: Using DPI for copyright enforcement," *Surveillance & Society* 9.4 (2012): 348. P.350.

⁴⁴⁶ Milton Mueller, Andreas Kuehn, and Stephanie Michelle Santoso, "Policing the network," P.352.

⁴⁴⁷ Milton Mueller, Andreas Kuehn, and Stephanie Michelle Santoso, "Policing the network," P.354.

⁴⁴⁸ Milton Mueller, Andreas Kuehn, and Stephanie Michelle Santoso, "Policing the network," P.354.

⁴⁴⁹ Milton Mueller, Andreas Kuehn, and Stephanie Michelle Santoso, "Policing the network," P.361.

⁴⁵⁰ CJEU Case C-70/10, *Scarlett Extended SA v. SABAM*, 24 November 2011.

⁴⁵¹ Milton Mueller, Andreas Kuehn, and Stephanie Michelle Santoso, "Policing the network," P.357.

⁴⁵² Milton Mueller, Andreas Kuehn, and Stephanie Michelle Santoso, "Policing the network," P.359.

policies, educational programs and, occasionally, DPI-based technical measures. While many resisted having DPI for copyright imposed on them, many universities nevertheless choose to block file-sharing protocols to conserve bandwidth, or to minimize the transaction costs associated with responding to notice and takedown requirements.⁴⁵³

In the UK and in the Netherlands, anti-piracy organizations have succeeded to get a court order to block access to the Pirate Bay. At the time of this research, the question remained whether this blockade was effective. Although anti-piracy organizations claimed the blockade was effective in fighting copyright infringement, some ISPs claimed that the percentage of file sharing did not diminish.⁴⁵⁴ They claimed it led to even more BitTorrent traffic.⁴⁵⁵ It also led to what some refer to as a whac-a-mole game, where a court order obliges ISPs to block access to the Pirate Bay IP address, but proxies are set up, or the Pirate Bay changes IP address, which requires another court order for blocking.⁴⁵⁶ Others claimed that these court orders only drew more attention to the Pirate Bay and increased the amount of visitors.⁴⁵⁷

The graduated response procedure, the most far-reaching Internet enforcement procedure that involves intermediaries, allows for slowing down or cutting off Internet access for consumers if they infringe on copyrights a number of times.⁴⁵⁸ Variations of this procedure have been adapted in France, the UK, South Korea, and the US and are adopted or debated in other countries.⁴⁵⁹ In the EU, rights holders tried to include graduated response procedures in the “Telecom Package” 2009 – the EU regulatory framework for electronic communications.⁴⁶⁰ However, after much protest, no explicit reference to this procedure was made in the new laws.

There has also been increased pressure to take intermediaries, like cyber lockers, websites, streaming services or Usenet forums, down more easily by suing them or seizing their servers or domains. In 2012 in the USA, the servers of Megaupload, the biggest cyber locker, were seized, and its owners arrested. However, taking down Megaupload did not slow down file sharing. At the end of the day when Megaupload was taken down, traffic had shifted to other cyber lockers, mainly in Europe, according to DeepFields. Sandvine said that users may have shifted to video streaming sites as well.⁴⁶¹

⁴⁵³ Milton Mueller, Andreas Kuehn, and Stephanie Michelle Santoso, "Policing the network," P.362.

⁴⁵⁴ Andreas Udo de Haes, "UvA: Pirate Bay-blokkade heeft geen effect," *Webwereld* (April 13, 2012), <http://webwereld.nl/nieuws/110183/uva--pirate-bay-blokkade-heeft-geen-effect.html>.

⁴⁵⁵ Andreas Udo de Haes, "XS4ALL: torrents toegenomen na Pirate Bay-blokkade," *Webwereld* (July 4, 2012), <http://webwereld.nl/nieuws/111053/xs4all--torrents-toegenomen-na-pirate-bay-blokkade.html>

⁴⁵⁶ Ernesto, "Pirate Bay ready for perpetual IP-address whac-a-mole," *Torrentfreak* (May 28, 2012) <https://torrentfreak.com/pirate-bay-ready-for-perpetual-ip-address-whac-a-mole-120528/>.

⁴⁵⁷ Enigma, "Pirate Bay enjoys 12 million traffic boost, shares unblocking tips," *Torrentfreak* (May 2, 2012), <http://torrentfreak.com/pirate-bay-enjoys-12-million-traffic-boost-shares-unblocking-tips-120502/>.

⁴⁵⁸ Monica Horten, *The Copyright Enforcement Enigma, Internet Politics and the 'Telecoms Package'*, (palgrave MacMillan, 2012), P. 96-97 and P.110-117.

⁴⁵⁹ De Beer and Clemmer, "Global Trends in Online Copyright Enforcement." P.375-376.

⁴⁶⁰ Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communications networks and services, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0140>

⁴⁶¹ Chloe Albanesius, "Megaupload Shutdown Fails to Slow File Sharing," *PCmag* (February 9, 2012), <http://www.pcmag.com/article2/0,2817,2400052,00.asp>.

Similarly, there have been new legislative proposals that would make the taking down or seizing of intermediaries easier. After intense pressure by the US government, this led to the creation of the SINDE law in Spain. In the USA, the controversial SOPA law was proposed, but withdrawn after public resistance.⁴⁶²

Other approaches have focused on the removal of funds for piracy, by “following the money.” These self-regulatory Memoranda of Understanding have been stimulated by the European Commission and aim to reduce the profits of commercial scale IP infringements in the online environment, by involving advertising service providers, payment services and shippers. The UK pioneered this approach by launching a pilot project called Infringing Website List (IWL) in 2013. Rights holders or their representatives can provide a list of infringing sites which will be checked by the City of London Police's Police Intellectual Property Crime Unit (PIPCU), which provides a list of undesirables for advertisers to avoid.

3.3 Different typologies for enforcement strategies

There are different typologies for enforcement strategies. Cohen, Bridy and Danahar, Smith, and Telang all use different typologies that I will describe here shortly. The major copyright industries have been trying to distribute copyright enforcement across a wide range of actors. According to Cohen, the overlap between these strategies deserved consideration as the emerging regime sought to change the infrastructure to allow for more control.⁴⁶³ She says that the rights holders pursued an agenda that sought to control the intellectual consumption and communication, at the expense of individuals and independent technology vendors. That agenda sought to implement a regime, which in turn relied on a group of strategies.

Cohen grouped them on the basis of the behavior they primarily target. Each strategy was internally homogenous, although they used different regulatory modalities. This differed from the approach taken by Lessig.⁴⁶⁴

She distinguished between:

- A. Surface level technological restrictions: These are copy protection technologies like DRM that operate at the level of individual files.
- B. Pressure on independent technology developers: These are pressures on technology developers whose technologies might allow for copyright infringement. Examples are regulatory measures such as in the DMCA that prohibit the production of anti-circumvention measures, the aim to minimize technology that makes copying easier, like the P2P providers.
- C. Trusted systems functionality: These strategies aim to move copyright enforcement functions deeper in to the user's electronic environment. Like implementing controls at the operating level.
- D. Pressure on network gatekeepers: Pressure on ISPs and search engines to implement various measures, like notice-and-takedown and filtering.
- E. End-user initiatives: Lawsuits, or interfering directly with exchange of files on P2P networks (by for example using decoy files).

⁴⁶² Jonathan Zittrain, Kendra Albert and Alicia Solow-Niederman, “A Close Look at SOPA,” *Future of the Internet* (December 2, 2011), <http://futureoftheInternet.org/reading-sopa>.

⁴⁶³ Julie Cohen, “Pervasively distributed copyright enforcement.” *Georgetown Law Journal* 95 (2006). P.2.

⁴⁶⁴ Cohen, “Pervasively distributed copyright enforcement.” P.3-4.

- F. Rhetorical positioning: Use rhetoric to position online copyright infringement as morally objectionable and “socially insidious”.⁴⁶⁵

Her distinction is thorough, and seems to be focused mainly on P2P networks and includes strategies that are outside of enforcement, like anti circumvention measures and rhetoric.

As we saw in the previous sections, because infringement has spread to other ways, I will use a different typology to distinguish between strategies to enforce copyrights on a large scale. As the next sections will show, this fits better with trends in enforcement.

Bridy made another distinction, which is a simpler version of the one by Cohen, and focused on the level of the intervention: the content level, the network level, and the user level.⁴⁶⁶

Interventions at the content level are DRM, interventions at the network level are aimed at technology like P2P software. The latter has been done by courts, and through network surveillance. This has also been done by looking at ISPs.⁴⁶⁷ Interventions at the user level were done through punishment and education.⁴⁶⁸

As I am interested in more enforcement procedures, this would be not useful for my research.

Danahar, Smith, and Telang used a typology along two axes.⁴⁶⁹ They talk about ‘intervention’, and look whether the intervention is regulatory (government-driven) or voluntary (industry-driven) and whether the intervention targets the supply or demand side of piracy.

They distinguish between:

- A. Regulatory interventions aimed at the demand side: HADOPI in France, IPRED in the EU.
- B. Regulatory interventions aimed at the supply side: Megaupload shutdown.
- C. Voluntary interventions aimed at the demand side: Copyright Alert System in the U.S., various industry lawsuits against file-sharers.
- D. Voluntary interventions against the supply side: voluntary changes in search engine ranking algorithms to reduce prominence of piracy in search results.⁴⁷⁰

Although this distinction is clear, it does not take into account the delegation of enforcement, which influences costs and human rights. These effects are relevant for the research question of this study. I have therefore adjusted those existing typologies to one that fits my research.

3.4 A typology of enforcement strategies

Rights holders have a number of strategies to scale up copyright enforcement. For the purpose of this research a strategy to scale up copyright enforcement is a spatially delimited

⁴⁶⁵ Cohen, "Pervasively distributed copyright enforcement." P.4-19.

⁴⁶⁶ Bridy, "Why Pirates (Still) Won't Behave," P.567.

⁴⁶⁷ Bridy, "Why Pirates (Still) Won't Behave," P.597.

⁴⁶⁸ Brett Danaher, Michael D. Smith, and Rahul Telang, "Piracy and Copyright Enforcement Mechanisms" (may 2013), forthcoming in: *Innovation Policy and the Economy*, volume 14, ed. Lerner and Stern, (University of Chicago Press, Chicago, Illinois). P.33.

⁴⁶⁹ Danaher, Smith, and Telang, "Piracy and Copyright Enforcement Mechanisms." P.28.

⁴⁷⁰ Danaher, Smith, and Telang, "Piracy and Copyright Enforcement Mechanisms." P.28-29.

strategy by actors to increase the amount of sanctions for copyright infringement. This ranges from rights holders suing a large number of end users at a court, to notice and takedown as done by intermediaries, to taking down intermediaries. This does not mean that rights holders or governments use one unique strategy at a time. They may use many different strategies at the same time, within or even outside of the country.

In the previous section Julie Cohen distinguished between enforcement strategies on the basis of the behavior they targeted. I have chosen an adapted route, because I am interested in the relation between the scale of sanctions and safeguards. Safeguards and sanctions both apply to legal entities instead of behavior, so I choose to differentiate between enforcement strategies on the basis of their primary target. Within these strategies, big differences remain.

Because I'm interested in the relation between scale en safeguards, I have chosen sanctions as a starting point for these enforcement strategies. By sanctions I mean any form of punishment, so a warning letter is included as well. I have fitted these strategies in a typology, based on the primary targets of enforcement (demand or supply), and whether that target is met directly or indirectly. Targeting directly means that the target is sanctioned, whereas indirectly means that other players are used or threatened to sanction others.

Enforcement strategies	<i>Direct</i>	<i>Indirect</i>
<i>Target demand side</i>	Targeting end users through law suits and settlement requests	Graduated response procedure
<i>Target supply side</i>	Criminal cases against large suppliers /(DRM)	Notice and takedown

Table 3.1: four groups of enforcement strategies

A. Copyright enforcement strategies that target the demand side directly

The first type of strategies aim enforcement at the demand side: individual end users that try to access copyright infringing content. Private players, like rights holders or their representatives, sued end users.

Most of the civil lawsuits have been aimed at individual end users not for accessing, but for sharing content. For BitTorrent anyone who downloads uploads as well. Especially in the US, representatives of the recording and film industries have sued thousands of individual consumers accusing them of making recorded music available to other consumers over the Internet.⁴⁷¹ In the US, § 512(h) of the DMCA originally allowed rights holders to serve subpoenas to service providers to obtain the identities of alleged infringers. This provided an easy way for rights holders to identify and sue large numbers of infringers. However, in the Charter Communications case,⁴⁷² the Eight Circuit of the US concluded that serving subpoenas to service providers excluded § 512(a) providers (mere conduit providers). This made identification significantly more difficult for rights holders, and led

⁴⁷¹ Jessica Litman, "Sharing and stealing." *Hastings communications and entertainment law journal* 27 (2004). P.3, and: RIAA, "Recording Industry Begins Suing P2P File Sharers Who Illegally Offer Copyrighted Music Online," *RIAA website* (Sept. 8, 2003), <http://www.riaa.com/news/newsletter/090803.asp>

⁴⁷² Charter Commc'ns, Inc.m 393 F.3d

them to ‘John Doe lawsuits,’ seeking expedited discovery according to Rule 45 of the Federal Rules of Civil Procedure to identify accused file sharers.⁴⁷³ This way, thousands of end users have been sued by the industry.

As most individual users did not have the financial means to go to court, they settled for smaller sums of money. Over 200,000 people have been sued for allegedly sharing copyrighted material online. Copyright holders or their representatives obtained the personal details of users to settle with them for a few hundred up to a couple of thousand dollars. This meant users avoided trial but also avoided potentially larger fines. Even though 200,000 is a large number, those cases rarely made it to court.⁴⁷⁴ This made suing and settling profitable for copyright holders.⁴⁷⁵

On behalf of rights holders, special law firms threatened users with lawsuits on the basis of their IP address. However, the goal of these warning letters was not to actually make it to court, but to generate quick settlements. For example, The US copyright group (DC area firm of Dunlap, Grubb & Weaver) filed thousands of lawsuits on behalf of independent film makers.⁴⁷⁶ 4500 individuals were sued for using BitTorrent to download the movie *Far Cry*.⁴⁷⁷ 5000 were sued for downloading the movie ‘Hurt Locker.’⁴⁷⁸ The U.S. Copyright Group simply asked people to accept a standardized settlement agreement and pay up. In fact they had a website for sued individuals where they can settle their claims, which displays the phrase “All Major Credit Cards Accepted.”⁴⁷⁹ These were usually small fees, which was tempting for individual end users who wanted to avoid the potentially enormous costs of going to court or being fined statutory damages for copyright infringement. However, it raised questions about procedural safeguards.⁴⁸⁰ Later, judges have started to react negatively to these rights holders, referring to this strategy as “an extortion scheme” whilst some of them have actually tried to reverse expedited recovery to protect individuals.⁴⁸¹ Another judge argued that he could not come to a decision on the basis of subpoenas, and that a trial was required.⁴⁸²

This strategy has been particularly appealing to rights holders in the pornographic industry. They had extra leverage, because, apart from the damages and costly trials, end users would also want to avoid the public shame associated with pornographic content. For example, the ‘adult copyright company’ sued 16,000 John Does for infringing copyright in

⁴⁷³ Bridy, “Is Online Copyright Enforcement Scalable?” P.720.

⁴⁷⁴ Edwards, *Role and responsibility of the Internet intermediaries*, P.21-22.

⁴⁷⁵ Ernesto, “200.000 users sued in the United States,” *Torrentfreak* (August 8, 2011), <http://torrentfreak.com/200000-bittorrent-users-sued-in-the-united-states-110808/>

⁴⁷⁶ Bridy, “Is Online Copyright Enforcement Scalable?” P.721, and: Nate Anderson, “The RIAA? Amateurs, Here’s how you sue 14.000+ P2P users,” *Ars Technica* (June 1, 2010), see: <http://arstechnica.com/tech-policy/news/2010/06/the-riaa-amateurs-heres-how-you-sue-p2p-users.ars>

⁴⁷⁷ Bridy, “Is Online Copyright Enforcement Scalable?” P.721, and: Achte/Neunte Boll Kino Beteiligungs GMBH & Co KG v. Does 1–4,577, No. 1:10-cv-00453, 2010 WL 3522256 (D.D.C. Mar. 18, 2010)

⁴⁷⁸ Bridy, “Is Online Copyright Enforcement Scalable?” P. 721, And: Complaint, Voltage Pictures, LLC v. Does 1–5,000, No. 1:10-cv-00873, 2010 WL 4955131 (D.D.C. May 24, 2010)

⁴⁷⁹ The portal can be accessed at: <http://dlegal.force.com/SiteLogindglegal>, visited on 16-10-2012

⁴⁸⁰ Bridy, “Is Online Copyright Enforcement Scalable?” P.722, and: “USCG v. The People,” *Electronic Frontier Foundation*, <https://www.eff.org/uscg> (last visited Oct. 28, 2010)

⁴⁸¹ Mike Masnick, “Another Judge Blasts Copyright Trolls”, *Techdirt* (September 24, 2012),

<http://www.techdirt.com/articles/20120923/22100820477/another-judge-blasts-copyright-trolls.shtml>.

⁴⁸² SJD, “Judge Baylson wants to test copyright trolls’ evidence in a bellwether trial,” *Fight Copyright Trolls* (October 7, 2012), <http://fightcopyrighttrolls.com/2012/10/07/judge-boylson-wants-to-test-copyright-trolls-evidence-in-a-bellwether-trial/>.

two pornographic films, *Batman XXX: A Porn Parody* and *Teen Anal Nightmare 2*, via P2P networks.⁴⁸³

In Europe, this strategy surfaced as well. Law firms in Germany send out thousands of letters to file sharers requesting payments each year.⁴⁸⁴ In England this strategy has been condemned. Andrew Crossley, from the ACS: Law firm was suspended from his duties for two years and ordered to pay a fine by the Solicitors Regulation Authority, after he sent approximately 20,000 British citizens threatening letters in which he asked them to pay 500 pounds for a settlement.⁴⁸⁵

In the EU ISPs are not required to hand over individual user data, unless the law specifies that they have to. Therefore, the amount of copyright infringement lawsuits in the EU has been lower than in the US.⁴⁸⁶ Also, countries like the Netherlands and Belgium allowed for a private home copying exception, which made small scale downloading of copyright protected content allowed.⁴⁸⁷

A potentially different strategy is when individuals are prosecuted criminally for file sharing. Although this usually happens when individuals facilitate copyright infringement (so in fact, when they act as supply, which is another category), there are cases of people file sharing that were prosecuted (in Sweden). The prosecution initially tried to get the man a prison sentence, but the judge eventually sentenced the man to a fine.⁴⁸⁸ Other people have been sentenced to two year probation for sharing songs. These cases mainly refer to uploading though.⁴⁸⁹ In Japan illegal downloading is a crime that can lead to a two year prison sentence or a fine of two million yen (25,700 dollars).⁴⁹⁰

⁴⁸³ Bridy, "Is Online Copyright Enforcement Scalable?" P.722, and: Debra Cassens Weiss, "Porn Industry Lawyer Is New Copyright King with 16,700 Lawsuits Filed," *ABA Journal* (November 10, 2010), http://www.abajournal.com/news/article/porn_industry_lawyer_is_new_copyright_king_with_16700_lawsuit_filed, Greg Sandoval, "Porn Studios to Subpoena Accused File Sharers," *CNET News.com* (October 2, 2010), http://news.cnet.com/8301-31001_3-20018358-261.html, see also: Complaint, Third World Media, LLC v. Does 1–1243, No. 3:10cv90 (N.D.W. Va. Sept. 24, 2010); Complaint, Patrick Collins, Inc v. Does 1–281, No. 3:10cv91(N.D.W. Va. Sept. 24, 2010); Complaint, Collins, Inc v. Does 1–118, No. 3:10cv92 (N.D.W. Va. Sept. 24, 2010); Complaint, West Coast Prods., Inc., v. Does 1–2010, No. 3:10cv93 (N.D.W. Va. Sept. 24, 2010); Complaint, West Coast Prods., Inc v. Does 1–535, No. 3:10cv94 (N.D.W. Va. Sept. 24, 2010); Complaint, Combat Zone, Inc v. Does 1–1037, No. 3:10cv95 (N.D.W. Va. Sept. 24, 2010); Complaint, Combat Zone, Inc v. Does 1–245, No. 3:10cv96 (N.D.W. Va. Sept. 24, 2010)

⁴⁸⁴ Michael Fritz, "File-sharing in Germany: Could the cost of getting caught be about to come down?," *ZDNet* (August 9, 2013), <http://www.zdnet.com/file-sharing-in-germany-could-the-cost-of-getting-caught-be-about-to-come-down-7000018915/>.

⁴⁸⁵ Jasper Bakker, "'Afpersende' Britse piraterijbestrijder geschorst," *Webwereld* (January 19, 2012), <http://webwereld.nl/nieuws/109247/-afpersende--britse-piraterijbestrijder-geschorst.html>

⁴⁸⁶ Gwen Hinze, "EU Law does not require ISP to hand over customers' identity data in alleged filesharing case," *Electronic Frontier Foundation* (January 30, 2008), <https://www.eff.org/deeplinks/2008/01/eu-law-does-not-require>.

⁴⁸⁷ Art 16b – 1 and Art 16c – 1 of the Dutch copyright law, and art. 22, § 1, 5° of the Belgian copyright law.

⁴⁸⁸ EnigmaX, "World' unluckiest bittorrent pirate fined but avoids jail," *Torrentfreak* (February 12, 2012), <http://torrentfreak.com/worlds-unluckiest-bittorrent-pirate-fined-but-avoids-jail-120212/>.

⁴⁸⁹ Ernesto, "60-year old file-sharer gets 2 years probation and fine," *Torrentfreak* (August 31, 2011), <http://torrentfreak.com/60-year-old-file-sharer-gets-2-years-probation-and-fine-110831/>.

⁴⁹⁰ "Japan introduces piracy penalties for illegal downloads," *BBC* (October 1, 2012), <http://www.bbc.com/news/technology-19767970>.

B. Copyright enforcement strategies that target the demand side indirectly

Rights holders have looked towards ways to enforce copyrights more effectively on the demand side, by using intermediaries and/or government institutions, through a process that aims to combine education with sanctioning. These graduated response procedures are systems that warn the infringing user (the warning is called a 'strike'), and after a number of warnings allow for more stringent punishment, in the form of the slowing of Internet connections, fines, or cutting off Internet access. Graduated response procedures are implemented through a statute, codes of practices, cross-industry agreements, or from remedies ordered by a court.⁴⁹¹

France has taken a legislative approach. The HADOPI bill created the HADOPI authority in charge of the graduated response system. Rights holders could complain to this authority about copyright infringement, and the authority would send warning letters to subscribers through their ISPs. After two warnings the authority could propose more stringent measures, like disconnection for up to a year. Originally, the law did not allow for judicial review, but this was struck down by the French constitutional court, and after that the third strike required a ruling by a judicial authority before more stringent measures could be taken. These measures could be the disconnection of Internet access, a fine of 300,000, and a two-year prison sentence. The data on alleged infringements would be researched by the Trident Media Guard (TMG), provided to an industry association (Societe Civile des Producteurs Phonographiques (SCPP), who would review the data and then transmit it to HADOPI.⁴⁹²

Ireland has taken a non-legislative approach, the result of a legal battle between the representative body of the recording industry in Ireland (IRMA) and the largest ISP in the country, Eircom (40% of the market). The settlement in January 2009 required Eircom to commit to 1. Inform subscribers that their IP address had been detected infringing copyright, 2. Warn them that they could be disconnected, and 3. Disconnect them if they did not listen. This protocol was the result of a contractual agreement, instead of a legislative one. Subscribers agreed to this mechanism, by agreeing to the terms of service. There was no judge involved, and Eircom was the arbiter of innocence or guilt. It did allow for an appeals process, but if the subscriber was found 'guilty', his connection is cut off for 7 days.⁴⁹³ Other ISPs have been sued, and at the times of the research it was unclear whether they would implement the system as well. It was also unclear how rights holders would find infringement, either through DPI or through IP hunting (DtecNet).⁴⁹⁴

In the UK, the Digital Economy Act introduced a graduated response system. ISPs were obligated to notify subscribers that their IP address had been used to download copyrighted material illegally. ISPs had to keep records of the number of notices issued to each subscriber, and had to make lists of subscribers that had received a specific number of notices. Rights holders would be able to obtain a court order and then ask the ISPs to disclose the identities of the subscribers and sue them. OFCOM, the UK communications

⁴⁹¹ Alain Strowel, "The 'Graduated Response' in France: Is It the Good Reply to Online Copyright Infringement." in: *Copyright Enforcement and the Internet*, ed. Stamatoudi (Kluwer Law International, The Netherlands, 2010). P. 147.

⁴⁹² Johnny Ryan and Caitriona Heintz. "Internet Access Controls: Three Strikes' Graduated Response' Initiatives," *The Institute of International and European Affairs* (2010). P.5-6.

⁴⁹³ Annemarie Bridy, "Graduated Response American Style: 'Six Strikes' Measured Against Five Norms." *Fordham Intellectual Property, Media & Entertainment Law Journal* 23.1 (2012): 1-66. P.15-17.

⁴⁹⁴ Ryan and Heintz, "Internet Access Controls," P.7-11.

regulator was at the time of this research expected to create a code with specifications of the process, standards of evidence, etc.⁴⁹⁵ If this approach would turn out to be ineffective, section 124G provided that the secretary of state could take additional measures such as limiting access to subscribers after they received a number of complaints.⁴⁹⁶ The digital economy act was delayed until 2014.⁴⁹⁷

In the US, private parties and ISPs agreed to a memorandum of understanding, with provisions that laid down a privately administered graduated response system. The Memorandum of Understanding created a Center for Copyright Information, a private entity charged with administration and oversight of the Copyright Alert System. The CCI consisted of members of the copyright industry and the participating ISPs. The CAS involved six strikes, where ISPs warned subscribers that they should not infringe, followed by more severe sanctions for those who did not listen. Like in Ireland, subscribers were bound to this system through the ISP terms of service. ISPs delivered a variety of possible sanctions, like slowing down Internet speed and suspending access. Subscribers could appeal in a non-judicial process which included the American Arbitration Association, under contract with CCI.⁴⁹⁸

Other countries implemented different versions of graduated response mechanisms. In South Korea the emphasis seemed to be on users that hosted content, whereas the graduated response systems in Taiwan did not obligate ISPs to terminate user access. The New Zealand system was still under discussion at the time of this research.⁴⁹⁹ In South Korea, the national human rights commissioner recommended to abolish the system.⁵⁰⁰

C. Copyright enforcement strategies that target supply directly

Some strategies aim enforcement at supply. Intermediaries might facilitate infringement on a large scale, and could therefore be more attractive to pursue than individual end users. Private players sued P2P intermediaries,⁵⁰¹ websites that offered content, Cyber lockers, Usenet forums, and websites that link to content. In some cases, lawsuits were unsuccessful, and intermediaries like YouTube were allowed to keep doing business. In other cases intermediaries ceased to exist. The goal of these lawsuits was to put the intermediary out of business, take it down, or change it completely. For example, rights holders have tried to sue the Internet service providers that enabled consumers to trade files.⁵⁰²

Governments have also targeted intermediaries directly, mostly through criminal lawsuits. The US Immigrations and Customs Enforcement (ICE) launched 'Operation in Our Sites' and seized hundreds of domains in the US, often in cooperation with rights holders.⁵⁰³ Operators of large websites and cyber lockers were prosecuted for criminal copyright

⁴⁹⁵ Ryan and Heintz, "Internet Access Controls," P.12

⁴⁹⁶ Ryan and Heintz, "Internet Access Controls," P.13

⁴⁹⁷ Thomas Brewster, "Britain's Anti-Piracy Act Delayed By Cost Dispute," *TechWeek Europe* (April 26, 2012), <http://www.techweekeurope.co.uk/news/copyright-anti-piracy-act-delayed-75259>.

⁴⁹⁸ Bridy, "Graduated Response American Style," P.18-23.

⁴⁹⁹ Ryan and Heintz, "Internet Access Controls," P.14-16

⁵⁰⁰ Hurips, "National Human Rights Body Recommends Abolishing Three-Strike-Out Rule," *Heesob's IP blog* (March 27, 2013), <http://hurips.blogspot.kr/2013/03/national-human-rights-body-recommends.html>.

⁵⁰¹ Jessica Litman, "Sharing and stealing." *Hastings communications and entertainment law journal* 27 (2004). P. 3 and: See *MGM v. Grokster*, 380 F.3d 1154 (9th Cir. 2004); *A&M v. Napster*, 239 F.3d 1004 (9th Cir. 2001); *In re Aimster*, 334 F.3d 643 (7th Cir. 2003)

⁵⁰² Litman, "Sharing and stealing." P. 3, and: See *RIAA v. Verizon*, 351 F.3d 1229 (D.C. Cir. 2003).

⁵⁰³ Joe Karaganis, "Meganomics," *The American Assembly, Columbia University* (January 24, 2012), see: <http://piracy.americanassembly.org/meganomics/>

infringement. Cyberlocker Megaupload was forced to shut down after a coordinated effort between the U.S. government and the government of New Zealand and the Hong Kong customs.

This also involves the government blocking access to domains or ‘taking down’ websites. This has been called ‘notice and action.’ This was in the proposed SOPA law, in the SINDE law in Spain,⁵⁰⁴ and in the Digital Economy act in England. The SINDE law included a commission that evaluated claims that were reviewed by a judge.

To an extent, enforcing on the demand side is directed at end users as well. These enforcers usually perceive uploading as worse than downloading content, which is why most of the lawsuits have been targeted at end users that were uploading on a very large scale. This is why the penalties for uploading are generally worse than for downloading. For example, the Netherlands originally allowed for a home copying exception, whilst keeping uploading illegal. In Japan downloading could lead to a 2 year prison sentence, whilst uploading infringing music and videos could lead to a 10 year prison sentence, and a ten million yen fine (around 100,000 dollars).⁵⁰⁵ In Holland, anti-piracy organization BREIN searched for large-scale uploaders and filed a complaint with the police to start a criminal prosecution.⁵⁰⁶

Other strategies that target the supply side target ‘the scene.’ This is criminal enforcement that aims to shut down those organizations. For example, in 2010, police in 14 European countries conducted coordinated raids, after years of investigations. They seized servers and arrested people.⁵⁰⁷

Technological protection measures, like DRM, also prevent supply, but are less relevant to my thesis, because they do not involve an actual sanctioning moment.

D. Copyright enforcement strategies that target supply indirectly

Sometimes intermediaries are in a better position to obstruct other intermediaries who facilitate copyright infringement. Private players sue those intermediaries in private lawsuits, to employ their assistance. They target access providers to block access to certain content. For example, access providers were sued in the UK and the Netherlands to prevent access to the Pirate Bay. It can also mean that private players sue payment processors to cut off funds to infringing websites, or that private players sue payment processors to learn more about a business entity so that they can sue that entity later.⁵⁰⁸

Enforcement strategies that target the supply side indirectly use intermediaries to prevent the supply of infringing content. This involves notice and takedown, where under threat of legal action, intermediaries are asked to take down certain content of their platform. This scales up, but the question remains whether there are many safeguards for

⁵⁰⁴ Jonathan Zittrain, Kendra Albert and Alicia Solow-Niederman, “A Close Look at SOPA,” *Future of the Internet* (December 2, 2011), <http://futureoftheInternet.org/reading-sopa>.

⁵⁰⁵ “Japan introduces piracy penalties for illegal downloads,” *BBC* (October 1, 2012), <http://www.bbc.com/news/technology-19767970>.

⁵⁰⁶ Henk-Jan Buist, “BREIN stuurt politie af op uploader,” *Webwereld* (May 23, 2012), <http://webwereld.nl/nieuws/110601/brein-stuurt-politie-af-op-uploader.html>.

⁵⁰⁷ Wouter Schilpzand, “Large scale European police action against piracy networks”, *Future of Copyright* (September 19, 2010), <http://www.futureofcopyright.com/home/blog-post/2010/09/14/large-scale-european-police-action-against-piracy-networks.html>.

⁵⁰⁸ Dimitri Reijerman, “Brein krijgt naw-gegevens via betalingsprovider –update,” *Tweakers* (September 26, 2011), <http://tweakers.net/nieuws/77014/brein-krijgt-naw-gegevens-via-betalingsprovider.html>.

users that upload content. There are in some cases consequences for repeat infringers here too: YouTube blocks users from uploading, if they have received too many warnings.

Notice and notice also falls under this category. In Canada, this means that ISPs forward notices from rights holders to users when those users host or share infringing content. However, ISPs do not reveal contact details of their subscribers or take action afterwards.⁵⁰⁹

⁵⁰⁹ Thomas Mennecke, "Canada Plans P2P and file-sharing Crackdown," *Slyck* (March 24, 2005), <http://www.slyck.com/news.php?story=720>.

4. THEORETICAL FRAMEWORK AND RESEARCH DESIGN

4.1 Introduction to this chapter

Chapter 1 introduced the main research question: *“How does large-scale copyright enforcement on the Internet influence procedural safeguards like due process and fair trial, what are its costs and its effectiveness, and what do these findings imply for public policy?”*

Chapter 2 showed that infringement happens on a large scale. Chapter 3 showed how rights holders (and governments) have scaled up copyright enforcement to fight massive infringement.

This chapter will describe the theoretical framework and research design. Theoretically, this problem falls within the field of legal economics. Research on enforcement in other sectors suggests the fears of the opponents of the new strategies are warranted. Legal economics predicts a certain level of effectiveness of enforcement: effective deterrence requires large-scale enforcement and more severe sanctions to increase the costs of breaking the law. Large-scale enforcement (increasing the chance of getting caught) is particularly effective. These theories also describe that scaling up enforcement is costly and that one way to cut costs is to reduce procedural safeguards, because legal procedures are time intensive and expensive. This means there could be a relationship between scale and safeguards. There could also be a relationship with severity, as it is another way to increase effectiveness. How does severity influence safeguards? If consequences of punishments are more severe, mistrial would create larger societal costs. If this applies to copyright enforcement, the consequences would be huge. Infringement happens on a large scale, so for each new enforcement proposal to be effective, costs would be massive or the enforcement strategy detrimental to human rights, the rule of law and innovation. This section will also describe and clarify procedural safeguards as a concept.

This study will use case studies to empirically test whether the predicted relationship between scale, severity and safeguards also holds in the area of online copyright enforcement and how enforcement strategies deal with costs and what their effect on infringement is. Because the predicted relationship between scale, severity and safeguards happens at the sanction level, I will use sub-cases of those enforcement actions when an enforcement strategy contains multiple types of sanctions. This chapter will describe my research methodology, by specifying the methods, my units of analysis (the cases and sub-cases), my variables, my case selection, what data I collected and how, and how this connects to the analysis.

4.2 The economics of enforcement

Legal economics suggest a number of legal solutions to attain the most efficient economic allocations. The most influential legal economist is Ronald Coase, who wrote ‘the problem of social cost,’ an influential article on law and economics.

With his theory, Coase laid the groundwork for “new institutional economics,” an economic approach that focuses on social and legal norms that underlie economic activity.⁵¹⁰

510.Malcolm Rutherford, "Institutional economics: then and now." *Journal of Economic Perspectives* (2001): 173-194., P.173–74.

According to Coase, the legal system has a large influence on the economic system, and legal norms had to be evaluated in ways that led to the most efficient outcome.⁵¹¹

Copyrights are a complex system of economic rights that aim to stimulate creativity. Online piracy has disturbed this traditional economic cost-benefit analysis of copyright. In the analogue environment, distribution of unauthorized copies had limited impact on rights holders, and as a benefit stimulated network effects of the copyrighted good and enlarged its market.⁵¹²

Because copyright holders suffer economic losses, they seek to deter infringement in a way that does not cost them more than the losses they suffer. As infringement happens on a large scale, they must deter cost-effectively.

Many scientific disciplines have studied why people break the law. Psychologists and sociologists have made important contributions because crime runs in families, which raises questions about genetic disposition and the influence of family background on the willingness to commit crimes. Ethnographers have studied how gangs are formed, and have looked at the internal structures of those in many cases criminal enterprises. Criminology is regarded as a separate discipline that studies the nature, extent, causes, and control of criminal behavior. Apart from that there have been debates in law, sociology, and philosophy that have focused on normative concerns that play a big role in defining crime and the appropriate punishment.⁵¹³

Later, the legal economics approach was added to the list of disciplines studying crime. In 1986, University of Chicago economist Gary Becker wrote the seminal paper "Crime and Punishment: An Economic Approach." This paper presented a new approach to crime and punishment by using the economic method. He looked at criminals as rational individuals that seek to maximize their own well-being, but through illegal instead of legal means. Becker recognized that economic insights can provide an interesting analysis of criminal behavior and law enforcement. By modeling an individuals' response to certain incentives, we can improve our understanding of how the certainty and severity of punishments may affect the individuals' decision to engage in illegal activities. Becker suggested using the theory that normally applies to individuals interactions in market environments to provide insights into the analysis of alternative crime control policies.⁵¹⁴ In doing so, he also formulated models that would allow crime policy to be empirically tested. In formulating his theory, Becker was the first economist to apply economic theory to non-market social structures, for which he was awarded the 1992 Nobel Prize in Economic Sciences.⁵¹⁵

This economics approach to crime is focused on constraints rather than on preferences. So it does not take into account certain psychological factors: in Becker's view everyone may become a criminal. This is linked to the classical school of criminology. In particular it is linked to the field of deterrence theory, which deals with the effects of punishment on crime. The idea is that people refrain from committing criminal behavior out of fear of legal punishments. Pioneers in this regard were Cesare Beccaria (1738-94) and

511. Ronald Coase, "The institutional structure of production." *The American Economic Review* (1992): 713-719. P.717-18.

512 Watt, Richard. *Copyright and Economic Theory: Friends or Foes?*. (Edward Elgar Publishing, 2000).

513 Richard Freeman, "The economics of crime." *Handbook of labor economics* 3 (1999): 3529-3571. P.3533.

514 Antonio Merlo, "Introduction to economic models of crime." *International Economic Review* 45.3 (2004): 677-679. P.677.

515 Mahmoud Bahrani, "The economics of crime with Gary Becker," *The Chicago Maroon*, May 25, 2012, <http://chicagomaroon.com/2012/05/25/the-economics-of-crime-with-gary-becker/>

Jeremy Bentham (1748-1832). They were utilitarianists, which means they believed that people's actions are motivated by obtaining pleasure and avoiding pain. If potential offenders expect pleasure from crime, they can be deterred by increasing the potential pain associated with it. In particular, potential offenders are deterred by legal punishments that are: (1) certain, which means potential offenders are likely to get caught and punished, (2) celeritous, which means the punishment is swift, and (3) severe, which refers to the amount of punishment received by an individual.

Becker makes two observations with regard to criminal policy and criminal activities: obedience is not taken for granted, and public and private resources are spent to prevent offenses and apprehend offenders. Also, conviction in itself is not enough; in some cases more severe punishment is necessary.⁵¹⁶ The main question in Becker's article is "how many resources and how much punishment should be used to enforce different kinds of legislation?" In his article, Becker defined the social loss of crime as the sum of: (1) the costs of crime, (2) costs of arrests and convictions, and (3) the costs of sanctions (imprisonment, parole, fines, etc.). The probability and severity of punishment was determined to minimize this sum.⁵¹⁷ Some writers have expanded Becker's definition by for example looking at the costs of crime in the equation. This is the range of benefits and costs that have an effect of people's decisions. People will allocate time to criminal activity until marginal benefits equal marginal costs. For most people marginal benefits of crime will be lower than marginal costs, which will make them not commit crime. Gains may be monetary, psychic or pure satisfaction of wants. Costs may be material, psychic, expected punishment costs, and opportunity costs. Punishment costs are formal and informal sanctions, and pecuniary costs from lawsuits. Opportunity costs of crime are the net benefit of the legal activity forgone while planning, performing and concealing the criminal act. The lower the individual's level of income, the lower his opportunity cost of engaging in illegal activity. The costs to society of crime may be material and hospital costs.⁵¹⁸

He argues that the optimal amount of enforcement depends on, among other things, the cost of catching and convicting offenders, the nature of punishments (fines or prison terms), and the responses of offenders to change after enforcement.⁵¹⁹ In other words: the higher the cost of justice, the more crime there is. An interesting side note in this regard is that although the most important weapons against crime have been tools of arrest and punishment, the theory also seems to suggest that governments can limit the benefits of crime, or follow the sociological literature that says that other economic ways to reduce crime are to look at the access to and rewards of legitimate activities.⁵²⁰

His paper was followed by George Stigler's "the Optimum Enforcement of Laws" and Isaac Ehrlich's "Participation in Illegitimate Activities: A Theoretical and Empirical Investigation." Stigler wrote that behavior is prescribed individually (for example through contracts and agreements) and unilaterally. When prescribed behavior is fixed unilaterally instead of by individual agreement, we have regulation or law, and these have to be enforced. When citizens depart from prescribed behavior this is called a crime or violation.

⁵¹⁶ Gary Becker, "Crime and Punishment: an Economic approach," *The Journal of Political Economy* 76.2 (1968), 169-217. P.169

⁵¹⁷ Becker, "Crime and Punishment." P.169-217.

⁵¹⁸ Erling Eide, "Recent developments in Economics of Crime," *German Working Papers in Law and Economics* 1 (2004). P.12

⁵¹⁹ Becker, "Crime and Punishment." P.170

⁵²⁰ Stephan Panther, "The economics of crime and criminal law: An antithesis to sociological theories?." *European Journal of Law and Economics* 2.4 (1995): 365-378. P.372-4.

However, crime is a “less formidable description” when we talk about trifling offenses or offenses against unjust laws.⁵²¹

The goal of enforcement is to achieve a degree of compliance with a rule or prescribed behavior that society believes it can afford. One reason not to do this is that enforcement can be costly. The extent to which laws are enforced depends on resources devoted to that task. Because of this cost limitation it would be almost impossible to detect and punish all offenders. Offenders are deterred by expected punishments, which are (broadly speaking) the probability times the severity of the punishment.⁵²² The more significant the offense, the more likely society will want to use resources to prevent the offense. This does not necessarily mean that more resources will make punishment more severe, but it means that the offender will be pursued more ‘tenaciously’ to increase the probability of apprehension.⁵²³

Ehrlich conducted empirical research to test whether Becker’s theory was true. His conclusion was that offenders as a group respond to incentives in much the same way as people who are engaged in legitimate activities do. He argued that from his empirical research (with all of its own shortcomings), it seemed plausible that the probability of conviction coupled with the severity of punishment had a deterrent effect on offenders.⁵²⁴

Using these theories in a normative fashion, the economic analysis of crime and criminal law uses a welfare economic analysis to judge the desirability of policy design: a utilitarian perspective. The basic idea is that the welfare of society depends on well-being of individuals of that society as measured by the extent to which their aims have been fulfilled. Distribution of income is not a variable that is taken into account. So it is about the sum of additional benefits by a change. If benefits are larger, that change is ‘good.’⁵²⁵

The economics of crime and criminal law is ‘etioloical’, which means it takes the norms protected by law as a given, and looks at causal determinants of criminal behavior. Norms that are protected are usually those that guarantee the functioning of a market society. Of course public goods, external effects, asymmetric information and transaction costs make the world more complex, but it remains uncertain how they should affect the selection of norms to be protected by criminal sanctions.⁵²⁶

After those papers, the theoretical and empirical economic literature on crime has grown rapidly. Some studies have expanded Becker’s model, and some have provided criticism. I will mention some of those studies briefly. Mathur has done a large empirical investigation that revealed that the more severe the punishment is for a particular crime, the lesser it is probable that the criminal will be punished. This might be based on the fact that for harsher crimes, judges might be more hesitant to award severe punishments, for example in cases of the death penalty. His data also revealed that certainty of punishment is a more important deterrent than severity.⁵²⁷

⁵²¹ George Stigler, “The Optimum Enforcement of Laws,” in: *Essays in the Economics of Crime and Punishment*, ed. Gary Becker and William Landes, (1974), 55-67. P.56.

⁵²² Stigler, “The Optimum Enforcement of Laws,” P.56.

⁵²³ Stigler, “The Optimum Enforcement of Laws,” P.57-58.

⁵²⁴ Isaac Ehrlich, “Participation in Illegitimate Activities: A Theoretical and Empirical Investigation,” *Journal of Political Economy* 81.3 (1973), 521-565. P. 560

⁵²⁵ Panther, “The economics of crime and criminal law,” P.368.

⁵²⁶ Panther, “The economics of crime and criminal law,” P.368.

⁵²⁷ Vijay Mathur, “Economics of crime: an investigation of the deterrent hypothesis for urban areas,” *the review of economics and statistics* 60.3 (1978), 459-466. P.465

Some papers have introduced reasons why punishment should not be set as high as possible, which Becker's model seems to suggest. One reason might be the perceived unfairness that only a limited amount of offenders would be (harshly) punished, while some would suffer no consequences. This problem is worse when we take legal error into account. Another reason might be the wish of retribution.⁵²⁸ Thomas Miceli argues that when we take the unfairness of legal error into account, the optimal punishment might be lower than maximum punishment.⁵²⁹ An interesting variation is by not looking at whether people choose illegitimate behavior over legitimate behavior, but also how intensive they do so.⁵³⁰ Another way of looking at the deterrent effect is that when people perceive the risk of getting sanctioned as higher, they are less likely to engage in criminal behavior.⁵³¹ Nagin writes about this especially. He argues that although empirical tests seem to confirm the existence of a deterrent effect through increasing the certainty and severity of punishments, little is known about risk perception.⁵³² This does not take into account the differences of wealth between individuals.⁵³³

Other papers have focused on the potential measurement errors that empirical research in this field can have. When looking whether or not sanctions are an effective deterrent there will always be a measurement error in crime rates, and simultaneity bias due to potential feedback of the number of offenses on arrests per offense (when crime is on the rise, citizens will want to see more police).

Of course, Becker and his followers cannot deliver the perfect theory to predict crime and the effects of enforcement. For example, in research it was revealed that people that go to church are less likely to commit crimes,⁵³⁴ and that people whose peers commit crimes are more likely to do so.⁵³⁵ Also, attitudes towards risk can be important, because they can steer an individual's response to the threat of punishment for criminal behavior. It also does not take into account rules of thumb, rules of information, habitual behavior, behavior that is emotionally motivated or impulsive behavior, etc. However, one could argue that all these behaviors may be influenced by rational calculations. If you stick by this view, the consequences that a change of policy has may still be best predicted by using the rational actor methodology. In other words: "the average aggregate behavior changes as if people were rational."⁵³⁶

But there's more substantial criticism, of which the two most controversial themes focus on deterrence by sanctions and the question of how extreme sanctions should be.

⁵²⁸ Erling Eide, "Recent developments in Economics of Crime," *German Working Papers in Law and Economics* 1 (2004). P.4

⁵²⁹ Thomas Miceli, "Optimal criminal procedure: fairness and deterrence," *International review of law and economics* 11.1 (1991). P.3-10.

⁵³⁰ Edward Glaeser, "An overview of crime and punishment." *Washington: World Bank. Mimeographed* (1999) P. 8.

⁵³¹ Daniel Nagin, "Criminal deterrence research at the outset of the twenty-first century." *Crime and justice* (1998): 1-42.

⁵³² Nagin, "Criminal deterrence research at the outset of the twenty-first century," P.2-5.

⁵³³ Panther, "The economics of crime and criminal law," P.371.

⁵³⁴ Richard Freeman, "Who Escapes? The Relation of Church-Going & Other Background Factors to the Socio-Economic Performance of Blk. Male Yths. from Inner-City Pvrty Tracts." *National Bureau of Economic Research* No. w1656 (1985).

⁵³⁵ Anne Case and Lawrence Katz, "The company you keep: The effects of family and neighborhood on disadvantaged youths." *National Bureau of Economic Research* No. w3705 (1991).

⁵³⁶ Panther, "The economics of crime and criminal law," P.367.

Regarding deterrence; most of the economic analyses prescribe that either the severity or probability of sanctions will lead to a decrease in criminal offences. So individuals are deterred by sanctions. However, this is subject to criticism. The expected punishment can be interpreted as a decrease in the expected “income” for the criminal activity. This might be true on the individual level, but tells us nothing about the total effect. Cameron shows that higher expected sanctions can have ambiguous effects: There can be positive correlations between legal and illegal income if the legal employment provides information or other useful services for criminal activities, there can be spillover effects (crime can switch region which could lead to higher aggregate crime levels), or there can be a perverse “industry supply” effect (by incarceration, people get to know other criminals which can lead to the formation of “crime firms.”)⁵³⁷

Furthermore, the policy conclusion of Becker’s model implies that sanctions should be as extreme as possible. Especially in cases where it is more expensive to increase the probability of sanctions, severity may be increased. Stigler has shown why this might be inefficient through his explanation of sanctions that “fit the crime.” He argues that there are different types of criminal activities, some more severe than others measured by the social damage they cause. If policy prescribes the severest penalty for the least severe crime, there will be no marginal deterrence for more severe crimes.⁵³⁸ However, Posner argues that this does not take into account the total effect. Sure, more severe crimes may increase in relation to less severe ones, but the total amount of crimes decreases.⁵³⁹ In other words: if punishment were sufficiently severe to make sure no crimes were committed, marginal deterrence would not be necessary. On the other hand, one would expect that this could be perceived as unfair by the democratic electorate.

After Becker’s article, an important contribution was made by John Harris, who writes that the legal framework Becker takes as a constant can be subject to policy choice. In particular in the area of what he calls “rules of the game” (which means standards of evidence, presumption of guilt, rights to counsel, and procedures for arrest and indictment), great variations exist that have implications for the Becker model. Having more of these rules of the game can prevent that guilty persons go unpunished (Type I error) and prevent that innocent persons are punished (Type II error). However, those rules of the game make the cost of apprehending and convicting a given percentage of offenders much higher. That is why in some states of emergency, or in a state of martial law, legal safeguards are relaxed to apprehend a maximum proportion of offenders at minimum cost. But this introduces yet another trade-off: Having less of these safeguards adds social costs to the equation in the form of wrongful punishments. Especially when more harsh punishments are imposed in the wrong way, the social loss is higher. Harris adds that even procedures like “stop and search” or wiretapping, although not convictions, impose forms of punishment on the innocent.⁵⁴⁰

Harris also adds that some of these losses will be perceived differently among social and economic groups within any society. Property owners have more to lose and will perceive the social loss as a result of offenses as much greater than groups who have little to lose. Meanwhile, higher income individuals will feel the costs of enforcement more through taxes. On the other hand the loss of unjust punishment may also impact only specific groups,

⁵³⁷ Panther, “The economics of crime and criminal law,” P.367.

⁵³⁸ Panther, “The economics of crime and criminal law,” P.370.

⁵³⁹ Panther, “The economics of crime and criminal law,” P.370.

⁵⁴⁰ John Harris, “On the Economics of Law and Order,” *Journal of Political Economy* 78.1 (1970), 165-174, P.165-166.

who will in turn attribute more loss to those processes. This should be resolved in the political process.⁵⁴¹

Other authors have added that the conviction of innocent parties increases social costs even more because it encourages crime as it reduces the marginal deterrence to its commission.⁵⁴² And from the other perspective: some researchers have found that making courts and enforcement more accurate increases deterrence as well.⁵⁴³

4.3 Procedural safeguards

There are many terms for these “rules of the game”, the rights connected to procedure. ‘Fair trial,’ ‘fair hearing,’ ‘fairness,’ ‘due process of law,’ ‘procedural due process,’ ‘fair procedure,’ ‘procedural justice,’ ‘procedural safeguards,’ ‘legal safeguards,’ ‘legal rights,’ and ‘natural justice’ are some of the words most commonly used.⁵⁴⁴ The origin of these concepts can be traced back to the Magna Charta in 1215, where in clause 39 it was written that

No freemen shall be taken or imprisoned or disseised or exiled or in any way destroyed, nor will we go upon him nor send upon him, except by the lawful judgment of his peers or by the law of the land⁵⁴⁵

which meant the Magna Carta not only established the rule of law in England, but also laid down certain procedural requirements for the delivery of justice. Although originally intended to prevent arbitrary government power, procedural requirements now have to be guaranteed in civil trials as well.

Throughout history, these rights have evolved into many separate concepts, each with their own scope, application and name. In their core, many of the underlying principles and external concepts overlap.

In his Dictionary of International Human Rights Law,⁵⁴⁶ John Gibson presents 9 categories of human rights. One of those categories he calls legal rights, which stand for the rights granted to individuals within the context of the public order of the state or other political community. All these legal rights are connected in the context of what he calls ‘the due process of the law.’ Although he takes an international perspective and his list is broader than most national laws are, I have chosen this as a starting point because it offers the most comprehensive list of all the legal rights. Most of these are part of the body of law in some shape or form in democratic states, or are directly applicable as international law. I have also chosen this list because it takes a principled approach: it names the principles before going

⁵⁴¹ Harris, “On the Economics of Law and Order,” P.170-171.

⁵⁴² Stigler, “The Optimum Enforcement of Laws,” P.57

⁵⁴³ Louis Kaplow, “The value of accuracy in adjudication: An economic analysis.” *The Journal of Legal Studies* (1994): 307-401.

⁵⁴⁴ Francois Logghe, “Over de “eerlijke behandeling” volgens artikel 6 van het EVRM,” *Jura Falconis* 33.2 (1996-1997): 271-316, accessible online: <http://www.law.kuleuven.be/jura/art/33n2/logghe.htm>.

⁵⁴⁵ <http://www.constitution.org/eng/magnacar.htm>, translation: No free man shall be seized or imprisoned, or stripped of his rights or possessions, or outlawed or exiled, or deprived of his standing in any other way, nor will we proceed with force against him, or send others to do so, except by the lawful judgement of his equals or by the law of the land. (from: <http://www.fordham.edu/halsall/source/magnacarta.asp>)

⁵⁴⁶ John S. Gibson, *Dictionary of International Human Rights Law*, (Lanham, Md.m & London: The Scarecrow Press, Inc. 1996).

into their codification (which means he looks at norms before looking at where those norms are to be found in legal texts).

The foundations for these safeguards include the right to life that every human being has, the right to have an effective remedy when rights or freedoms are violated, and equality before the law and protection from discrimination.⁵⁴⁷

Although all safeguards are different, some share similarities in their nature or in their application to specific phases in the process. Some rights are substantive (e.g. the right to legal assistance), some procedural (e.g. the right to examine witnesses), and some both (e.g. right to equal protection). Some rights apply to the discovery/arrest phase of enforcement (e.g. treatment with humanity and respect), some apply to detention (e.g. habeas corpus), some to the trial (e.g. fair and public hearing), some to after trial (e.g. right to appeal), some to punishment (e.g. no death penalty except for specific reasons or crimes) and some to multiple phases in the process.⁵⁴⁸ Many of the rights are connected. The rights are mentioned in table 4.1.

RIGHT	TYPE OF RIGHT
1. No arbitrary arrest or detention (includes 2-13)	Arrest Due Process
2. Treatment with humanity and respect	Arrest Due Process
3. Basic causes for arrest and detention should be made known (legal rules)	Detention for alleged cause Due Process
4. Information of reasons for arrest and charges	Detention for alleged cause Due Process
5. Right of habeas corpus (when deprived of liberty by arrest or detention, a person is entitled to proceedings before a court on the lawfulness of his detention)	Detention for alleged cause Due Process
6. Hearing before judicial authority	Detention for alleged cause Due Process
7. Hearing without delay	Detention for alleged cause Due Process
8. No coercion	Detention for alleged cause Due Process
9. Bail (The right to be released from detention in exchange for guarantees – usually money- to await trial is connected to the basic right to liberty of the person and the presumption of innocence)	Detention for alleged cause Due Process
10. To a court for judicial determination	Detention for alleged cause Due Process
11. Compensation for error in arrest/detention	Detention for

⁵⁴⁷ Gibson, *Dictionary of International Human Rights Law*, P.86-87.

⁵⁴⁸ Gibson, *Dictionary of International Human Rights Law*, P.86-87.

	alleged cause Due Process
12. Detention conditions	Detention for alleged cause Due Process
13. Presumption of innocence	Trial Due Process
14. Equality before tribunals	Trial Due Process
15. Fair and public hearings	Trial Due Process
16. Competent, independent, and impartial tribunal	Trial Due Process
17. Information of any criminal charge	Trial Due Process
18. Information on nature and cause of charge	Trial Due Process
19. Information in language defendant understands	Trial Due Process
20. Time to prepare defense	Trial Due Process
21. Trial without delay	Trial Due Process
22. To be tried in defendants presence	Trial Due Process
23. Legal assistance	Trial Due Process
24. Information of right to legal assistance	Trial Due Process
25. Legal assistance without payment if defendant lacks sufficient means	Trial Due Process
26. Obtain attendance and examination of witnesses on defendant's behalf on same basis as witnesses against defendant	Trial Due Process
27. Free assistance of an interpreter	Trial Due Process
28. Defendant not compelled to testify against himself or herself (no self-incrimination)	Trial Due Process
29. Defendant not compelled to confess guilt	Trial Due Process
30. Public judgment	Trial Due Process
31. Penalty must be in law	Trial Due Process
32. Penalty must be personal	Trial Due Process
33. Procedure for juveniles	Trial Due Process
34. Compensation for error by miscarriage of justice in conviction process	Post-trial Due Process
35. Protection against double jeopardy (no one can be tried or punished twice for the same offense)	Post-trial Due Process

36. Right of appeal (at higher tribunal to review decision or allow for possible retrial)	Post-trial Due Process
37. Detention punishment to be humane, with respect for inherent dignity of the human person	Punishment Due Process
38. No cruel or unusual punishment	Punishment Due Process
39. No death penalty except for specific reasons or crimes	Punishment Due Process
40. Punishment only of the offender	Punishment Due Process
41. Detention punishment provisions for juveniles	Punishment Due Process
42. Aim of penitentiary system is reformation and social rehabilitation	Punishment Due Process
43. Contract inability will not lead to imprisonment	Other legal right
44. Equal protection of the law	Other legal right
45. Ex Post Facto Law (a person cannot be convicted for something that was not considered an offense under law at the time the act was committed)	Other legal right
46. Privacy (no unlawful interference with it)	Other legal right
47. Torture (is never allowed)	Other legal right

Table 4.1: legal rights by Gibson⁵⁴⁹

These due process rights have roots in strong philosophical traditions.⁵⁵⁰ In 'Two theories of justice', John Rawls writes that

If laws are directives addressed to rational persons for their guidance, courts must be concerned to apply and to enforce those rules in an appropriate way. A conscientious effort must be made to determine whether an infraction has taken place and to impose the correct penalty. Thus a legal system must make provisions for conducting orderly trials and hearings; it must contain rules of evidence that guarantee rational procedures of inquiry. While there are variations in these procedures, the rule of law requires some form of due process: that is, a process reasonably designed to ascertain the truth, in ways consistent with the other ends of the legal system, as to whether a violation has taken place and under what circumstances. For example, judges must be independent and impartial, and no man may judge his own case. Trials must be fair and open, but not prejudiced by public clamor. The precepts of natural justice are to insure that the legal order will be impartially and regularly maintained.⁵⁵¹

There are even strong psychological reasons for due process rights. People want to have the opportunity to influence the outcome of the process.⁵⁵² Social psychologists have researched

⁵⁴⁹ This list is in: Gibson, *Dictionary of International Human Rights Law*, P.86-134

⁵⁵⁰ For example, see: Ronald Dworkin, *Principle, Policy, Procedure in A Matter of Principle* (Harvard University Press, 1985).

⁵⁵¹ John Rawls, *A Theory of Justice* (Oxford University Press, Twelfth Impression, 1992). P.238-239.

⁵⁵² Nancy Welsh, "Remembering the Role of Justice in Resolution: Insights from Procedural and Social Justice Theories." *Journal of Legal Education* (2004): 49-59. P.53.

what people regard a 'fair' process. Allan Lind and Tom Tyler revealed that four elements are regarded as important. In the process, both parties get to express their views, the third party demonstrates consideration of what both parties have said, the third party tries to be fair and impartial, and the third party treats both parties with dignity and respect.⁵⁵³ Other research shows that people want the opportunity to express their opinion, even if they know they cannot influence the outcome. According to Lind and Tyler, this is based on the group value theory.⁵⁵⁴ In sum, fairness is also about people's perceptions of the fairness of the policies and procedures in making decisions.⁵⁵⁵

With this in mind, I will use the following terms and definitions. Even though many concepts are used interchangeably, like due process rights, legal rights, etc., from now on, I will use the term '*procedural safeguards*.' I define procedural safeguards as *the safeguards that aim to protect individuals from arbitrary power and from wrongful punishment, when they face deprivation of property or liberty as a result of enforcement or some form of arbitration like in a court of law.*

Obviously, they are not the only factors that could potentially influence a trial. These safeguards tell us little about the social justice of certain trials. Litigation is expensive, and dominated by attorneys. But those are not questions this thesis aims to answer directly.

4.4 Case study research

There are many different ways to conduct social science research: through experiments, surveys, histories, analyses, etc. They all have their benefits, and depend on a number of things, like the type of research questions, the control the researcher has over events, and to what extent the research aims to cover historical events.⁵⁵⁶

Most methodological debates on social science highlight trade-offs between two competing imperfect methods of analysis. Large-N studies and/or statistical analyses offer more comparative merit by having a larger sample that is more representative of the specific objects of interest, and offer the researcher a chance to make inferences, through deduction, on the basis of usually quantitative evidence.⁵⁵⁷ This method has been criticized for "conceptual stretching"⁵⁵⁸ and for lacking the appropriate tools to examine the specific causal processes associated with big national level outcomes.⁵⁵⁹ Small-N studies and/or intensive case study analyses offer a more in-depth and more contextual analysis of the object of interest, are more inductive in nature, and usually qualitative.⁵⁶⁰ The central

⁵⁵³ Nancy Welsh, "Remembering the Role of Justice in Resolution: Insights from Procedural and Social Justice Theories." *Journal of Legal Education* (2004): 49-59. P.52, and: Allan Lind and Tom Tyler, *The Social Psychology of Procedural Justice*, (Springer Science & Business Media, 1988).

⁵⁵⁴ Welsh, "Remembering the Role of Justice in Resolution. P.52.

⁵⁵⁵ Bradley Alge, "Effects of computer surveillance on perceptions of privacy and procedural justice." *Journal of Applied Psychology* 86.4 (2001): 797.

⁵⁵⁶ Robert Yin, *Case study research, Design and methods*, (third edition, Sage Publications, 2003).

⁵⁵⁷ Todd Landman, *Studying Human Rights*, (New York, Routledge, 2006), P.60.

⁵⁵⁸ Giovanni Sartori, "Concept misinformation in comparative politics," *the American Political Science Review* 64 (1970): 1033-53.

⁵⁵⁹ David Collier, Henry Brady, and Jason Seawright, "Source of leverage in causal inference: toward an alternative view of methodology." In *Rethinking social inquiry: diverse tools, shared standards*, ed. H.E.Brady and D.Collier. (Berkeley, California: Rowman & Littlefield and Berkeley Public Press, 2004).

⁵⁶⁰ Landman, *Studying Human Rights*, P.60.

shortcoming of this method has been called “too many variables, small number of cases,”⁵⁶¹ by which they mean that the outcomes are hard to externalize to other situations.

According to Landman, a sliding scale exists between those two theories, which he calls the ‘epistemological continuum,’ ranging from ‘soft’ hermeneutic approaches to ‘hard’ nomothetic approaches. They all differ by the type of reasoning, the balance between evidence and inference, the nature of the knowledge claims made, and the scope of the empirical coverage.⁵⁶²

This research is a case study research. According to George and Bennett, case studies have many strengths. They allow for exploratory research to derive new hypotheses, they allow for conceptual validity by taking into account context, and they allow the assessment of more complex causal relations.⁵⁶³ This fits, as I aim to investigate the relation between different elements of copyright enforcement: those relations are too complex to assess in an experimental context only. I also have little control over the events. My case studies can add to scientific knowledge by limiting the number of independent and dependent variables, and by situating the research in the context of previous research.⁵⁶⁴ Through description, this research can also contribute by shining light on how enforcement procedures work in practice.

I also test to what extent a predicted causal relationship exists. For this, I need a larger amount of observations. Case study research allows for this structured and focused comparison. Data collection is guided by questions, that make this comparison and cumulation possible.⁵⁶⁵ I intend to be on the middle of Landman’s continuum, and will select a middle-large amount of cases. Gerring has made a typology of covariational research designs (table 4.2).⁵⁶⁶

		Temporal Variation	
		No	Yes
Spatial Variation	None (1 unit)	[Logically impossible]	(a) Case study I
	Within-unit	(b) Case study II	(c) Case study III
	Across-unit	(d) Cross-sectional	(e) Time-series cross-sectional
	Across- and within-unit	(f) Hierarchical	(g) Hierarchical time-series; Comparative-historical

Table 4.2: *typology of covariational research designs.*⁵⁶⁷

In my research, there is no temporal variation, but there is spatial variation. The main research is cross-case study research. For a relatively large sample of different enforcement strategies I will check how they perform on the different variables: scale, severity and safeguards. By comparing the cases on the different variables, I can achieve more external validity. Meanwhile, many cases include different measurement points: some of those cases may yield multiple within case empirical results on the variables, so I will use sub-cases as

⁵⁶¹ Arend Lijphart, “Comparative politics and the comparative method,” *American Political Science Review* 65 (1971), P 682-93.

⁵⁶² Landman, *Studying Human Rights*, P.59.

⁵⁶³ Alexander George and Andrew Bennett, *Case studies and theory development in the social sciences*, (Cambridge, Massachusetts, MIT Press, 2005), P.19-22

⁵⁶⁴ George and Bennett, *Case studies and theory development in the social sciences*, P.73-88

⁵⁶⁵ George and Bennett, *Case studies and theory development in the social sciences*, P.67-72

⁵⁶⁶ John Gerring, *Case study Research, principles and practices* (Cambridge University Press, 2007). P.27

⁵⁶⁷ Figure taken from: John Gerring, *Case study Research, principles and practices* (Cambridge University Press, 2007). P.27

well. I will compare and graph those results because they will hopefully tell me something about the connection between the three variables. Specific information from within the case can tell me more about how different actors choose to act, and how they view their responsibilities in light of the variables.

4.5 Conceptualizing cases

One of the first tasks of a case study researcher is to define what the case in the research is. According to Gerring, a Case is “a spatially defined phenomenon (unit) observed at a single point in time or over some period of time. It comprises the type of phenomenon that an inference attempts to explain.”⁵⁶⁸ These units need to be similar, because I draw inferences based on their comparability.

According to George and Bennett, this means clearly defining the universe, the class, or subclass of events, to overcome criticism of being not 'comparative' enough. Cases must be instances of only one phenomenon. And cases should be chosen on the basis of research objective and strategy. Case studies should also employ variables of theoretical interest for policymakers.⁵⁶⁹

In political science and human rights studies the main unit of analysis is usually the nation state, but because that would be too broad for my research, I have not done that.

To identify cases, I have used what George and Bennett call “typological theorizing,” which is “the development of contingent generalizations about combinations or configurations of variables that constitute theoretical types.”⁵⁷⁰ I have done this already in chapter 3, and created typologies of the different enforcement strategies.

The typologies help comparison. A typology can identify the qualitative types of a single multidimensional dependent or independent variable. Sometimes, typologies generalize on the basis of variance of independent variables, but they can also characterize variants of a given phenomenon in terms of conjunctions of variables.⁵⁷¹

At first instance I will stick to the typology described in chapter 3, the different ways in which rights holders and governments have attempted to scale up copyright enforcement:

1. Target demand directly (direct private lawsuits, sending threatening letters to get users to settle for sums of money without any court intervention).
2. Target demand indirectly (Private graduated response, government graduated response)
3. Target the supply side directly (target intermediaries, or direct criminal lawsuits against the scene for example)
4. Target the supply side indirectly (notice and takedown aimed at hosting providers, SOPA, filtering)

In my research, the typology is based on the primary targets of enforcement (demand or supply), and whether that target is met directly or indirectly. In this regard, targeting directly means that the target is sanctioned, whereas indirectly means that other players are used or threatened to sanction the target.

⁵⁶⁸ Gerring, *Case study Research*, P.19

⁵⁶⁹ George and Bennett, *Case studies and theory development in the social sciences*, P 77-79

⁵⁷⁰ George and Bennett, *Case studies and theory development in the social sciences*, P.233

⁵⁷¹ George and Bennett, *Case studies and theory development in the social sciences*, P.238

In most of the enforcement strategies multiple actors vary and play a determining role where it concerns the level of safeguards offered. This has been taken into account in the analysis. This applies to privately administered judgment in particular: in the case of notice-and-takedown the entities actually 'judging' whether some content is infringing (after a notice) are the intermediaries, and even if it were possible to gather the data on all the intermediaries, those intermediaries perform differently on the variables that I am interested in. For example, in an experiment done by the organization Bits of Freedom in the Netherlands, some service providers performed better at offering safeguards than others.⁵⁷² I have to take this into account in the analysis: some procedures allow for more discretion than others.

There are also differences between the players that initiate the enforcement (some are initiated by private players, some by public players), because they require different safeguards in the initiation process, for example with regards to gathering evidence.

Although I am interested in enforcement procedures, based on the theories in legal economics we know that sanctioning moments are important. They happen on certain scales and have particular severities. Some enforcement procedures have multiple sanctions. The graduated response procedures for example have multiple strikes and increasingly severe penalties. However, they cannot be separate cases, because they are to be understood from within the enforcement strategy. Those subcases are all connected under one case umbrella, and cannot be evaluated separately from this umbrella. Enforcement strategies have a particular impact (on infringement levels) and costs which are evaluated on a broader level. Therefore I make a distinction between cases and subcases: cases being the enforcement procedures in a given country and subcases for the different sanction moments within one enforcement strategy. Subcases are used more often in case study research.⁵⁷³ This creates two levels of analysis.

This creates a large-N for potential case studies but will make measurements precise. Because the case definition is more limited than the nation state assessment I used in the chapter on levels of infringement, where possible, I will include the local infringement levels.

The unit of observation is each individual actor, and the unit of analysis is the enforcement strategy that involves each actor.

4.6 Criteria for case selection

In statistical research, large samples usually involve some degree of randomization to guarantee representation. Usually this randomization is also distributed across the different ranges of the variables. For case study research this is more difficult, because of its small 'N'. Random sampling would be unreliable and might be uninformative.⁵⁷⁴

Therefore case selection is important. Case selection can have logical or pragmatic reasons for case selection – the language, personal entree, special access to data, etc.

⁵⁷⁵ But there has to be some systemization as well, to create external validity. George and Bennett differentiate between different strategies for case selection, as does Gerring. I have described them.

⁵⁷² Bits of Freedom, "Providers verwijderen tekst Multatuli," *Bits of Freedom website* (October 13, 2004). <https://www.bof.nl/2004/10/13/providers-verwijderen-tekst-multatuli/>

⁵⁷³ George and Bennett, *Case studies and theory development in the social sciences*, P 295

⁵⁷⁴ Gerring, *Case study Research*, P.86-91.

⁵⁷⁵ Gerring, *Case study Research*, P.145-150.

George and Bennett say that you can either have (1) cases of the same type (that either validate the types or are deviant) that because they have the same independent variables have similar outcomes, (2) most similar cases that have different outcomes because they have one different independent variable, (3) most likely, least-likely, and crucial cases that have a specific interest like an extreme value, (4) least similar cases that differ on all but one independent variable.⁵⁷⁶

Gerring differentiates nine types of selection that guarantee representativeness and causal leverage (which means they provide variation along dimensions of theoretical interest).⁵⁷⁷

He mentions typical cases (typical examples of some cross case relationship),⁵⁷⁸ diverse cases (which illuminate the full range of variation on variables),⁵⁷⁹ extreme cases (who display extreme or unusual values),⁵⁸⁰ deviant cases (who deviate from some cross-case relationship),⁵⁸¹ influential cases,⁵⁸² crucial cases (most or least likely to exhibit a certain outcome),⁵⁸³ pathway cases (one independent variable is likely to have a certain outcome),⁵⁸⁴ most-similar (have similarities except on one of the variables),⁵⁸⁵ and most-different cases (different on everything except one of the variables).⁵⁸⁶

I chose 8 different cases. They are to an extent diverse, to achieve a minimal representation of the full variation of the population. I chose two large-scale cases initiated by government parties aimed at supply (Sinde, and ICE). I also wanted to get typical/crucial cases, which were the graduated response (HADOPI and Eircom) and notice and takedown cases (Google search/YouTube and the Netherlands). The lawsuits (UK and USA) I chose because they were to an extent typical as well, and controversial. Another reason to choose them is that the RIAA wanted the lawsuits to be a deterrent. I also wanted to differentiate as much as possible between public and private procedures, as costs are carried differently and can be an important factor.

In the Netherlands I had easier access to data, so I chose to do Notice and takedown in the Netherlands. I also chose to look at how Google deals with Notice and takedown in the US, because they have a system that receives complaints on a large scale. Another reason I chose HADOPI in France is that within the EU France is the biggest advocate for more copyright enforcement, and HADOPI is the first government administered graduated response procedure. Eircom in Ireland I chose because it was the first privately administered graduated response. I chose the Sinde procedure in Spain because of the procedure is unique in an international context. I chose mass lawsuits in the UK because of language and because the case was controversial. Finally I chose two extra cases from the USA, because the lawsuit campaigns kicked off there, and because the ICE case would be an interesting small scale variable.

⁵⁷⁶ George and Bennett, *Case studies and theory development in the social sciences*, P.251-253.

⁵⁷⁷ Gerring, *Case study Research*, P.86-91.

⁵⁷⁸ Gerring, *Case study Research*, P.91.

⁵⁷⁹ Gerring, *Case study Research*, P.91.

⁵⁸⁰ Gerring, *Case study Research*, P.101.

⁵⁸¹ Gerring, *Case study Research*, P.105.

⁵⁸² Gerring, *Case study Research*, P.108.

⁵⁸³ Gerring, *Case study Research*, P.115.

⁵⁸⁴ Gerring, *Case study Research*, P.122.

⁵⁸⁵ Gerring, *Case study Research*, P.131.

⁵⁸⁶ Gerring, *Case study Research*, P.139.

As I look at the strategies (cases) and the specific sanctioning moments within those cases (subcases), there will be measurements on two levels and a large number of observations.

The different cases and subcases are in table 4.3. The subcases are also described in the case chapters themselves.

Case	Subcase	Demand /supply	Direct /indirect	Public/privately administered	Large/small scale	“Typical”
Targeting end users directly (US)		Demand	Direct	Private	Semi large scale	
	Settlement letter					
	Court case					
Targeting end users directly (UK)		Demand	Direct	Private	Semi large scale	
	Settlement letter					
	Court case					
HADOPI graduated response (France)		Demand	Indirect	Public	Large scale	X
	1 st warning					
	2 nd warning					
	Court case					
Eircom graduated response (Ireland)		Demand	Indirect	Private	Large scale	X
	1 st warning					
	2 nd warning					
	7-day suspension					
	12-month suspension					
NTD at Google /YouTube		Supply	Indirect	Private	Large scale	X
	NTD Google Search					
	TCRP					
	NTD YouTube					
	Content ID					
NTD in the Netherlands		Supply	Indirect	Private	Large scale	X
	NTD NL ISPs					

	NTD Leaseweb trusted removal program					
Operation 'In Our Sites' (USA)		Supply	Direct	Public	Semi-large scale	
	Seizure					
	Forfeiture					
	Personal trial					
Ley SINDE (Spain)		Supply	Direct	Public	Semi-large scale	
	Voluntary removal					
	Judge mandated removal					

Table 4.3: case selection.

4.7 Variables and data

Regarding the data I need, I can answer a lot of my questions through desk study, but especially the practical side remains unanswered. Those will turn into interview questions. For each other variable, I have included a set of questions I will ask around each case.

Applying economics of crime theory to copyright enforcement reveals interesting insights. However, I do not plan to use Becker's formula to determine the optimum amount of copyright enforcement. There are too many uncertainties about the exact social cost copyright infringement creates, as argued in the previous chapter. Also, it is unsure how many people are involved in infringement (although we know it is a large part of the population) and there are big differences between people to what degree they infringe on copyrights. An additional difficulty is that infringement takes place cross-border, so this would make any equation about optimum levels of enforcement problematic.

To help me solve my research question, some insights in Becker's model are relevant. We have already seen that copyright infringement happens on a large scale, and we know that copyright enforcement seeks to deter potential infringers. To effectively deter, enforcement has to be certain. Another deterrent is the severity of the sanctions. For copyright this means enforcement needs to at least happen on a large scale or have very severe sanctions, as infringement is done by so many people. Changing just one would theoretically mean that enforcement would become disproportional or that enforcement costs would skyrocket. Harris has added to Becker's theory that "rules of the game" make enforcement costs higher. We know that many due process concerns have been raised over new copyright enforcement mechanisms. This could imply that rights holders and governments have attempted to decrease these rules of the game to scale up copyright enforcement in a cost-effective way.

Deterrence theory also describes that the severity of sanctions is relevant. Mathur has done a large empirical investigation that revealed that the more severe the punishment is for a particular crime, the lesser it is probable that the criminal will be punished. This

might be based on the fact that for harsher crimes, judges might be more hesitant to award severe punishments, for example in cases of the death penalty.⁵⁸⁷

Becker makes two observations with regard to criminal policy and criminal activities: obedience is not taken for granted, and public and private resources are spent to prevent offenses and apprehend offenders.⁵⁸⁸ The main question in Becker's article is "how many resources and how much punishment should be used to enforce different kinds of legislation?"

The goal of enforcement is to achieve a degree of compliance with a rule or prescribed behavior that society believes it can afford. Enforcement can be costly. The extent to which laws are enforced depends on resources devoted to that task.⁵⁸⁹

Following this theoretical framework, a number of variables are relevant: scale, severity, safeguards, costs and the deterrent effect of each sanction.

4.7.1 Scale

The first and most important way to deter is by increasing the chance of getting caught. In other words: scale. For the chapter on the level of infringement, scale was measured in many different ways: the amount of users that infringe on copyrights, the number of websites that offer copyright infringing content, the percentage of users that is engaged in copyright infringement, and the percentage of Internet traffic that consists of copyright infringing content. Those are to an extent all measures for scale. In my case, it will mean 'the amount of sanctions:' whenever a legal party (person or intermediary) is sanctioned. Because it revolves around the sanction, scale will be evaluated at the subcase level. Different types of parties are likely to be affected in different ways by sanctions.

For the first and second categories (targeting the demand side directly or indirectly), scale is relatively easy to determine: the amount of users directly sanctioned. There are a number of ways to measure this: how many lawsuits there are per year in a given jurisdiction. For threatening letters sent, this is more difficult. The people responsible have been rather secretive about this.

Targeting individuals indirectly should include warning letters too. Harris writes that not just convictions have to be included as even warnings or procedures like wiretapping and stop and search have consequences and exact forms of punishment.⁵⁹⁰ Because the graduated response procedure involves multiple steps which gradually increase in severity (starting with warning letters), I will have separate measurement points that I will take into account in my results. I can justify this by having the severity variable, which means I take into account the different dimensions of the different steps.

For the supply side, scale can also mean instances of infringement but also the amount of intermediaries sanctioned as a separate measurement point. Again, I can justify having these different measurement points by taking into account the severity of the sanctions.

⁵⁸⁷ Vijay Mathur, "Economics of crime: an investigation of the deterrent hypothesis for urban areas," *the Review of Economics and Statistics* 60.3 (1978), 459-466. P.465.

⁵⁸⁸ Gary Becker, "Crime and Punishment: an Economic approach," *The Journal of Political Economy* 76.2 (1968), 169-217. P.169

⁵⁸⁹ George Stigler, "The Optimum Enforcement of Laws," in: *Essays in the Economics of Crime and Punishment*, ed. Gary Becker and William Landes, (1974), 55-67. P.56.

⁵⁹⁰ Harris, "On the Economics of Law and Order," P.166.

I will graph this after looking at the empirical data. If significant clusters arise, I can graph them on an ordinal scale.

Questions I will ask are: what is the scale on which this procedure takes place? In each step of the procedure, how many claims/sanctions per unit of time? How often is sanctioned in relation to the claims?

In my analysis, I estimated scale performance by comparing it to the population and level of infringement in the region that applies to the enforcement procedure.

4.7.2 Severity

Deterrence theory prescribes that to effectively deter, sanctions do not just have to be certain, but they also have to be severe. A more severe sanction will increase the potential costs of breaking the law, which should discourage offenders if it exceeds the benefit of breaking the law. That is why the case studies also include the severity of sanctions. Because this again relates to the sanction itself, severity will be evaluated at the subcase level. Some procedures have large consequences for targets, some have less. This could also play a role in the effect of up scaling on procedural safeguards.

Unfortunately there is no objective way to turn severity into a variable. There is a large body of research that has attempted to do this, but each from within their own discipline, so for example just criminal sanctions, or just private sanctions. Some of this research is based on philosophy, some on surveys. There is a big difference between the disciplines, because private sanctions are more retributive in nature and therefore usually include sums of money. For criminal sanctions there is a bigger moral aspect involved, and the sanctions include 'immaterial' sanctions like prison sentences and even the death penalty (obviously not for copyright). Administrative sanctions often include sanctions for businesses. There have been no comparisons, at least none that would be relevant to copyright sanctions.

In public administration, a popular work is the so-called 'enforcement pyramid.' This pyramid is a model conceived by John Braithwaite that provides a scale from low to high intervention (figure 5.1). This pyramid ranges from informal measures to heavy measures, whereby criminal sanctions are considered heavier than civil sanctions.

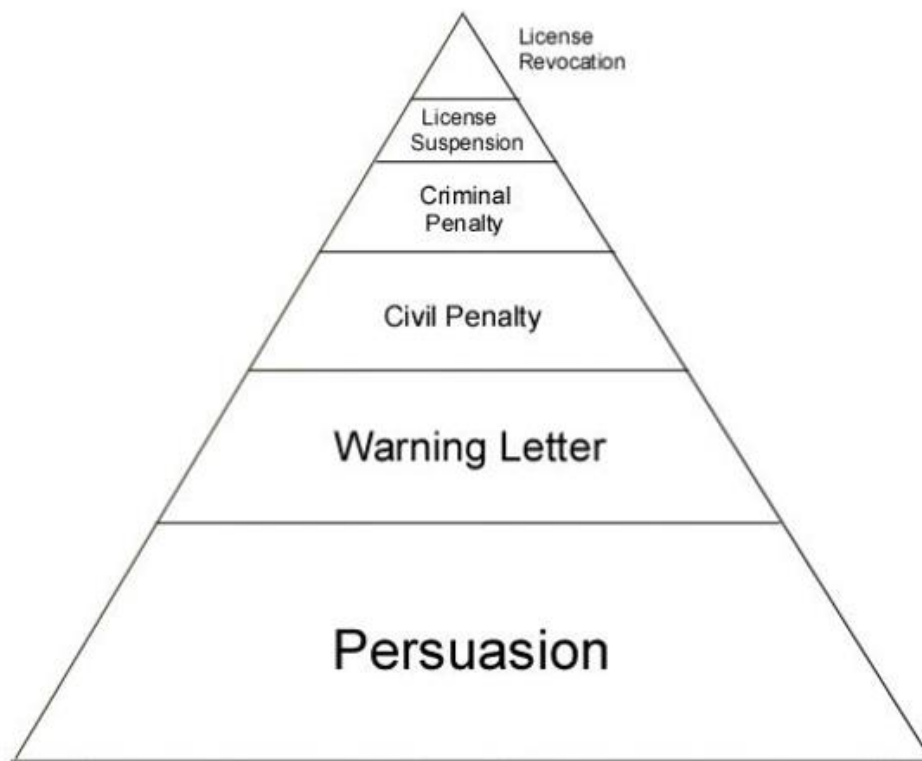


Figure 4.1: A pyramid of enforcement responses.⁵⁹¹

I propose making a similar categorization, on the basis of personal consequences, by which I categorize the degrees of severity ranging from low to high. The potential penalties range from warnings to fines of hundreds of thousands dollars. One problem I face is that the sanctioned parties differ: intermediaries may be sanctioned and people may be sanctioned. This means I will make my pyramid much smaller. Only three variations will exist. In my cases, I will collect the different sanctions and categorize them relative to each other.

Questions I intend to ask are: in each step of the procedure, what is the sanction that follows? How often is sanctioned in a particular way (related to the choice for sanctions of the sanctioning party). In the case of graduated response, although disconnection is the ultimate sanction, the question remains how often this sanction is truly applied.)

4.7.3 Safeguards

Landman distinguishes three ways in which human rights are measured. Firstly, human rights are measured 'in principle.' This is a measurement of a formal commitment, where scholars or practitioners look at human rights as they are laid out in national and international legal documents. To achieve this, they translate qualitative legal information into quantitative information, which is in turn used to track commitment of countries to principles of human

⁵⁹¹ Image source: Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (New York: Oxford University Press, 1992), P.35

rights. That principled commitment can be used to test the practical commitment of countries.⁵⁹²

Another way is to measure human rights 'in practice.' This is a measurement of the rights that are actually enjoyed and exercised by groups and individuals regardless of the formal commitments of the governments (the rights in principle). Since World War II, NGOs have conducted a lot of social research on human rights violations throughout the world.⁵⁹³

Others measure human rights as outcomes of government policy that has a direct bearing on human rights protection.

Measurement itself has taken the form of coding country participation in regional and international human rights regimes, coding national constitutions according to their rights provisions, qualitative reporting of rights violations, survey data on perceptions of rights conditions and experiences, quantitative summaries of rights violations, abstract scales of rights protection based on normative standards, and individual and aggregate measures that map the outcomes of government policies that have consequences for the enjoyment of rights.⁵⁹⁴

For my research, I am mostly interested in what happens in practice. As mentioned, I will make an analysis of the specific copyright enforcement regimes and the safeguards they offer, but those regimes might involve extrajudicial players that are not legally required to provide safeguards to users in the enforcement process. This only makes my practical analysis more interesting. To what extent do those players allow for similar levels of protection?

I immediately confess that this is to an extent arbitrary, constructed by myself without any formal, objective justification, and during the research subject to my own interpretation, but I think its strength lies in its comparability, and the justification will be provided in the case studies themselves and the variety of measurements. Through an extensive explanation in each case, I hope to be transparent about my classification. If I have measurements that vary on the safeguards-variable scale, I have points that form reference points relative to each other.

'Scoring' or 'grading' enforcement regimes on the safeguards scale will be done by gathering empirical data in the different case studies. To grade enforcement I will use the checklist of questions on safeguards. This will allow for more comparison.

There is no full objective way to 'measure' to what extent safeguards are present in an enforcement regime. Legal notions are by their nature formulated in a broad way, and difficult to quantify. It is impossible to determine what a given 'maximum' amount of safeguards is. How do you determine if a judge is 100% independent? And is a 100% independent judge even desirable? In the past, previous research has used reference points to compare results for things like judicial performance. As I am conducting a cross-case analysis, I do the same. The level of safeguards will be measured in cases relative to each other and will be placed on an ordinal scale. This implies that amongst my cases I will include enforcement regimes for which I hypothesize that they will lead to extreme values on my variable scale. In so doing, they will be reference points in themselves.

There is a growing body of literature on the social scientific analysis of human rights problems, with contributions from scholars from a variety of disciplines, as well as from governmental and non-governmental organizations like the United Nations and the World

⁵⁹² Landman, *Studying Human Rights*, P.78-80.

⁵⁹³ Landman, *Studying Human Rights*, P.80-81.

⁵⁹⁴ Landman, *Studying Human Rights*, P.78.

Bank.⁵⁹⁵ To determine what I am looking for, I have analyzed previous attempts to assess similar values. A number of international organizations have made similar analyses in developing countries. Among others, the UN⁵⁹⁶, the World Bank⁵⁹⁷, the World Justice Project⁵⁹⁸, Freedom house⁵⁹⁹, the Vera Institute of Justice⁶⁰⁰, and the Centre for Democracy and Justice⁶⁰¹ have written handbooks and papers that aim to aid development workers in the field. Some of those reports are means of political pressure, others measure progress to help reform programs. They 'grade' countries performance in specific fields. For example, Freedom house delivers the annual 'Freedom in the World' report on the state of civil and political rights in a number of countries in the world, whilst the World Bank has the 'Worldwide Governance Indicators Project,' covering over 200 countries.

Unfortunately, there is not one single set of measures for human rights across different categories and dimensions,⁶⁰² so I have looked at several previous attempts. While some measurement tools raised in those texts might not be relevant to my thesis ("are YouTube representatives democratically elected in a transparent way?"), and while there is a considerable overlap between some of the tools, the reports do provide a helpful guidance for setting up effective measuring points, data sources, and data analysis.

To come to my own perspective on how to measure the amount of safeguards in enforcement regimes, I have also looked at the book 'studying human rights' by Todd Landman, scholarly literature, and I have looked at the most authoritative reports by governmental and non-governmental organizations. This is based on the organizations that issued them, and by referral (what were the reports most commonly referred to in the field). Another great help was Annemarie Bridy, who in an article, evaluated numerous enforcement mechanisms on the basis of similar principles, like procedural fairness.⁶⁰³

Some measurements used in the literature on developing countries fall outside of the scope of my research and are not used. For example, as I do not intend to evaluate the entire legal profession, I will not look at the quality of and accessibility of legal education in a given setting. Also, a lot of the literature focuses mainly on corruption. This means that important indicators are things like judicial salaries and additional privileges granted to judges or whether or not judicial appointments correlate with changes in the national administration. Those also fall outside of the scope of this research.

To be able to determine the effects of the new enforcement strategies on procedural safeguards, we need to conceptualize procedural safeguards more precisely. For safeguards,

⁵⁹⁵ Landman, *Studying Human Rights*, P.75.

⁵⁹⁶ Office of the United Nations High Commissioner for Human Rights, "Rule-of-law tools for post-conflict states, Monitoring legal systems," (United Nations Office on Drugs and Crime, Criminal Justice Assessment Toolkit, Vienna, 2006).

⁵⁹⁷ Daniel Kaufmann, Daniel Aart Kraay, and Massimo Mastruzzi. "The worldwide governance indicators: methodology and analytical issues." *Hague Journal on the Rule of Law* 3.02 (2011): 220-246.; Linn Hammergren, "Diagnosing Judicial Performance: toward a tool to help guide judicial reform programs." Latin America and the Caribbean Region, World Bank, (Washington, DC, 2000).

⁵⁹⁸ Juan Carlos Botero and Alejandro Ponce. "Measuring the rule of law." Available at SSRN 1966257 (2011).

⁵⁹⁹ Freedom house, "Methodology for measuring political rights and civil liberties," on website:

<http://www.freedomhouse.org/report/freedom-world/freedom-world-2012>

⁶⁰⁰ Todd Foglesong, et al. "Measuring Progress toward Safety and Justice: A Global Guide to the Design of Performance Indicators across the Justice Sector." Vera Institute of Justice (2003).

⁶⁰¹ Center for Democracy and Governance, *Handbook of Democracy and Governance Program Indicators* (August 1998).

⁶⁰² Landman, *Studying Human Rights*, P.78.

⁶⁰³ Bridy, "Graduated Response American Style."

I have chosen privacy at first. It not only presents value in itself as a human right, but it is also an important first step to prevent abuse of power in trial. Regarding the more heavy safeguards, I have included demands set on the status of the arbitrator and the trial itself. Finally, I have taken into account the means of the accused. I have included a more external trial safeguard in the form of transparency. I include proportionality as a norm of fairness as well (which is considered punishment due process), as this is necessary for my assessment of penalties in a more general sense. These safeguards again relate to the level of sanctions and are assessed on the subcase level.

Privacy

How is infringement found? On what level (of the physical infrastructure – DPI, or the application layer by participating in the network) is it found? Who finds the infringement? Does a transfer of personal data take place? How does this take place? How is this data stored? Is this data made public? Is it anonymized? Who has access to this data? What kind of barriers exist (legal or technological) to get access to this information?

Impartial, competent, and independent judge/arbitrator

Which authorities judge the infringement? Who make up these authorities? What is their background? Do they have a financial, personal, or professional relation with other parties that are relevant to copyright disputes? What can arbitrating parties lose in the procedure, and what can they win? This latter question especially applies to what these parties lose if they judge incorrectly (for example, in the case of Notice and takedown, ISPs have an incentive to judge in favor of the claimant, because otherwise they might lose their safe harbor).

Presumption of innocence

Who has the burden of proof? How do arbitrators deal with claims/accusations? How does this stand in relation to the amount of claims/accusations? What constitutes evidence of infringement? Do they check the sender of the claim, the person infringing, how infringement takes place, whether it takes place over a long time, or the purpose of the infringement, and to what extent the infringement affects the artist? What kind of questions do arbitrators ask when dealing with complaints? Is there a checklist? Do claims have requirements before they are processed? If a large number of claims are received, and they cannot all be processed, is there a sample procedure used? Is there a difference between how claims from different senders are treated? In what way are claims made? Is it an automated system? What costs are connected to sending a claim? What costs are connected to unjustified claims? What costs are connected to judging a claim? What costs are connected to sanctioning? What do parties that file a claim have to win or lose when they do so unjustified? How do parties deal with the IP address problem (how do we know the IP is used by the alleged infringer)?

Notice, right to be heard (prior to conviction), defenses and appeal

Is there contact between the claiming party and the supposedly infringing party? How much? At what stage? Is there contact between the party that sanctions and the party that is sanctioned? How much? When? Do parties have the possibility to present their views? Can parties appeal the decision? Where and how? Is there a hearing? Can parties request a hearing? What kind of barriers exist for alleged infringers to react to claims (financially? Do they have to risk losing their privacy?), so what do they have to do to react? What authorities deal with reactions to claims? What is the background of the people there? Do they have a relation with any of the parties? How many reactions come in? How do authorities deal with these reactions? How does this relate to the amount of reactions? What constitutes evidence in those reactions? What type of reactions is most common? How are these reactions treated, or how does the organization deal with specific reactions that appear most common (change of policy for example)? What do parties stand to lose when reacting? Can all the parties get all the information on the conflict? E.g. what are alleged infringers suspected of? Can a real judge be involved? What barriers exist to involve an actual judge? Does this change the possible sanction?

Transparency

What does the judgment of the judging authority look like? Is a judgment subject to specific requirements? E.g. are the decisions well motivated? Are these decisions made public? Are there specific decision making rules that the authorities stick to? How was the creation of the mechanism transparent? To what extent were parties able to influence the design of the enforcement mechanism? To what extent is its implementation transparent? Is there for example a website that states how the mechanism works, or where the agreement that created this system is published? Or a code of conduct? Is it clear how the rules are applied? And is it clear who applies the rules?

Proportionality

Is the measure necessary for its goal? Is the measure a suitable means to achieve that goal? Does it not present an excessive burden on the parties it addresses?

4.7.4 Impact on infringement levels

To what extent do enforcement procedures impact infringement levels? It is important that I direct the answer to this question as specific to the enforcement mechanism as possible. In some cases, I also used estimates by parties. However, those answers are highly political (because every party will have an interest in the answer). Regarding effectiveness, it makes more sense to evaluate the effectiveness of the strategy as a whole. This takes place on the case level.

4.7.5 Costs of the system

Another interesting and potentially moderating variable is the cost of the system. As the theory of deterrence is economic in nature, cost is an important consideration for enforcers. In many cases, these costs will remain hidden, because private organizations have the

freedom to refuse to tell me their specific budget details. By constructing the story, I hope to still shine some light on the costs the system has. Because the costs of every sanction at the subcase level cannot be disaggregated, this is evaluated at the case level.

Questions I will ask are: what does it cost to spot infringement? What are the costs to file a claim? How many people work in this system? How much do they cost? What does it cost to judge? How much does it cost to deal with reactions/complaints? How do these costs all relate to the budget of the claiming party/judging party. Extra: What are the costs of all the lawyers and judges involved? Does the enforcement mechanism require an (automated) system that costs money? How much does it cost? And its maintenance?

4.8 Data collection/research tools

The empirical information I need relates to the enforcement mechanism itself. To get valuable answers to my research I use data triangulation, which means I get my data from different methods but also different, sometimes opposing sources. This is important in the context of my research, as most parties have a stake in presenting their answers to their benefit. The different methods I use are interviews, literature study, and legal analysis.

First of all, I included news articles, academic research and reports by NGOs on the practice of mass litigation. I studied local laws and case law as well. I included a list of more specific documents at the introduction of each case study.

Then, I did qualitative Interviews. I included a list of interviewees at the introduction of each case study and a full list in my bibliography. I took most advice from Rubin and Rubin in their book on qualitative interviewing.⁶⁰⁴ This book deals with 'responsive' interviewing; which means that you should ask additional questions until you understand the other person's point of view. This can be differentiated from asking predetermined questions. It prescribes depth interviews instead of more general quantitative ones.

Survey researchers ask standardized questions. Demographers analyze official data. Some social researchers experiment.⁶⁰⁵ Naturalistic, qualitative social researchers gather information by observing and by talking with and listening carefully to people who are being researched. The data is acquired by participant observation and qualitative interviewing.⁶⁰⁶

My previous sections show the information I am looking for. Most of this information I could only get through qualitative interviewing, because some things cannot be answered simply or briefly, or because I sometimes needed more explanation or examples. Qualitative interviewing is useful for describing social and political processes.⁶⁰⁷

According to Rubin and Rubin, the interview takes place by gently guiding the conversational partner in an extended discussion. Depth and detail follow from following up on answers.⁶⁰⁸

This means I started with broad unstructured questions, like: "how does the procedure work in practice, start to finish", and would later go into more narrow questions, after the discovery of patterns. This made the interviews semi structured.⁶⁰⁹

⁶⁰⁴ Herbert Rubin and Irene Rubin, *Qualitative interviewing: The art of hearing data* (Thousand Oaks, California, Sage, 2005), P.1.

⁶⁰⁵ Rubin and Rubin, *Qualitative interviewing*, P.1-3.

⁶⁰⁶ Rubin and Rubin, *Qualitative interviewing*, P.1-3.

⁶⁰⁷ Rubin and Rubin, *Qualitative interviewing*, P.1-3.

⁶⁰⁸ Rubin and Rubin, *Qualitative interviewing*, P.4-9.

⁶⁰⁹ Rubin and Rubin, *Qualitative interviewing*, P.4-9.

Naturally, I followed up those questions with things that seem interesting or relevant. So say a party would say that they cannot handle the scale of claims, I could ask them if they think they could do better with more people, or resources, etc. All data is suspicious, because every party has an interest in overstating the costs.

To be thorough and accurate, I needed to demonstrate that I have not been deceived. I handled this through the before mentioned data triangulation. I asked some of the same questions to different people in separate roles to check interviews for consistency.⁶¹⁰

Some actors could not submit to an interview in person or over the phone, and chose to answer my questions through email.

To strengthen my credibility, I have kept record of all interviews, the recordings, but also the email conversations I have had.

In terms of ethics I have asked all participants to describe their perspective of the procedure, and emailed them how I intended to publish the cases. I gave them a chance to correct possible mistakes.⁶¹¹

The interviewees I have chosen had to provide different, contending perspectives. I made sure they were experienced (by which I mean as much firsthand experience as possible) and knowledgeable in the area. I also tried to vary on key distinctions and made them aware of opposing views, to enhance credibility and quality.⁶¹² After the section on case selection I have included a list with interviewees and a justification for this choice (4.9)

Most of the times this meant I talked to the claimant or their representative, the parties that applied the procedure, and representatives of consumers. The latter was necessary because it was often difficult to actually speak to consumers directly.

I also did literature study and legal analysis. I looked and compared findings with other sources of information, like documents, scientific articles, laws, newspaper stories, court decisions, and testimonies.⁶¹³

4.9 Interviewees

Interviewee selection

For each case, I approached interviewees that could provide different perspectives on enforcement strategies. This meant I wanted to speak to rights holders and anti-piracy authorities first, as they were the parties who initiated the enforcement and had in many cases lobbied for new enforcement procedures. This at times meant I also wanted to speak to government officials, as some procedures are initiated by the government. Closely linked to rights holders are the actors hired by rights holders to enforce on their behalf. Next, I wanted to speak to the actors involved in the application of the sanction in the procedure. I approached intermediaries, judges and at times government officials administering the procedure. Lastly, I approached the side of the internet user/defendant. This included lawyers representing defendants, consumer organizations, and human rights organizations. At times I also included technology experts. I have summarized the interviewees per case on the basis of these categories (table 4.4).

⁶¹⁰ Rubin and Rubin, *Qualitative interviewing*, P.70-75.

⁶¹¹ Rubin and Rubin, *Qualitative interviewing*, P.97.

⁶¹² Rubin and Rubin, *Qualitative interviewing*, P.64-69.

⁶¹³ Rubin and Rubin, *Qualitative interviewing*, P.70-75.

Case	Enforcement	Application	Internet User/Defendant	Other
US Lawsuits	Gill Sperlein	Judge Otis Wright	Mitch Stoltz (EFF)	Delvan Neville
	RIAA	(Former) Judge Nancy Gertner	Corynne McSherry (EFF)	
UK lawsuits				Solicitors disciplinary tribunal
HADOPI	ALPA	Sarah Jacquier (HADOPI)	Jeremie Zimmermann (La Quadrature du Net)	
		SFR (ISP)		
Eircom graduated response	IRMA		Digital Rights Ireland	UPC (ISP)
NTD Google Search	RIAA	Google	EFF	
	Brein			
	Attributor Guardian			
	DTECNET			
NTD Netherlands	Brein	XS4ALL	Bits of Freedom	ECP-ECN
		Ziggo	The Clinic	
		Leaseweb		
ICE	Steven Welk		EFF	
			Mark Lemley	
			Andrew Bridges	
SINDE		Jorge Cancio Melia (Second	AUI	
			Asociatio internautes	

Table 4.4: Interviewees.

These are not the only parties I approached for interviews. On the rights holders side, I have also approached the Movie Picture Association (MPA) (both the US and EU departments) as they are one of the major organizations representing rights holder worldwide. They, unfortunately, repeatedly refused to talk to me. Similarly, I approached law firms that have represented rights holders in lawsuits against end users in the US (relevant to my first case): I approached the Copyright Enforcement Group (CEG) and Guardaley. Although I spoke to the first firm briefly, they refused to submit to an interview.

For the French HADOPI procedure, I did speak to the French anti-piracy authority, but I also wanted to get the practical perspective of the technology company enforcing on their behalf (TMG). They, however, refused. In Ireland, I spoke to the rights holders involved in the graduated response procedure (IRMA). I wanted to get the perspective of the anti-piracy authority as well (INFACT), but they did not respond and eventually their website went offline. It is unclear what happened to their organization.

I approached US government officials to get their perspective on enforcement. I contacted the new commission responsible for graduated response there, and the officials

responsible for the takedowns described in the 'ICE takedowns' case. They never responded. I tried other channels as well, but the US government was in a financial shutdown at the time. The Spanish rights holders were also not able to submit to an interview.

Thankfully, many rights holders and anti-piracy authorities did submit to an interview. The RIAA however only submitted to an email through email, and the tech company Dtecnnet (responsible for enforcement in the graduated response procedure in Ireland) refused to go into detail on Eircom.

On the side of the actors applying the sanctioning in the enforcement procedures, thankfully many were willing and able to speak to me. Unfortunately, Eircom refused to talk about their graduated response procedure. I also approached more judges in the US (including magistrate judges), but they refused. On the consumer/internet user side no one refused.

I had approached numerous actors for the case on the UK, but they all referred me to official documents containing enough factual descriptions to finish my case study.

Mitigating selection bias

Looking at the list of interviewees and in particular the refusals, it is clear that actors operating on the side of rights holders were more hesitant to submit to interviews. It is unfortunate because it introduces potential selection bias which might undermine the outcomes of this research. I will briefly outline how I mitigated selection bias and argue why the relative under-representation of rights holders does not invalidate the findings of this study.

This study observes a relationship between specific variables. To do that, it uses sources that are publicly available and corroborated by independent sources, such as academic research. This information has been supplemented with interviews with practitioners who answer questions about their own practice. These are meant to illustrate the thinking of stakeholders on the impact that enforcement strategies have on them.

In other words, the case studies present two key types of evidence. First, I reconstructed basic properties of the enforcement strategy from neutral sources (e.g., academic research and public records). As will become clear, these descriptions are straightforward and uncontroversial.

Second, when reconstructing the impact of the enforcement on the interests and rights of specific stakeholders, I present the opinion of those stakeholders. The latter type of evidence is clearly demarcated in the text. Rather than presenting these observations as facts, I present them as claims by the stakeholders on how they are impacted and on what they see as the wider impacts. I do not aim to validate or measure the subjective experience of actors involved in enforcement procedures. I do mention when external evidence was available to corroborate their claims. The fact that some stakeholders refused to participate does not invalidate the fact that these other stakeholders hold certain views. As long as the status of these claims is clear, they help develop understand the impact of enforcement strategies.

A final, and important, point is this: While it remains unfortunate that the views of rights holders are included only to a limited extent, we should let not let their decision to not participate block academic research in this area for fear of selection bias. Doing so would de facto provide these stakeholders with veto power over research and impose undesirable limitations on the public debate.

4.10 Analysis

The analysis must guarantee a great degree of internal and external validity.⁶¹⁴ External validity is achieved by ensuring that the case selection is representative of the relationship I intend to explore. Internal validity means that the research design illuminates the causal relationships of interest.

Internal validity is achieved through process tracing. Because case studies rely heavily on contextual evidence, and are quasi experimental, and because they rely on deductive logic to reconstruct causality, it is insufficient to show correlation in outcomes. Process tracing is necessary. Gerring calls it 'detective work.'⁶¹⁵

Process tracing requires exploring all the links in the causal chain, and making them explicit so that each micro mechanism can be proven.⁶¹⁶ All pieces of evidence are relevant to central argument. It does still also rely on general assumptions about the world, theoretical (like nomothetic laws) or pre-theoretical (common sense).⁶¹⁷ It is useful to clarify the argument with each turn, and to verify each stage of the model, along with an estimate of relative uncertainty.⁶¹⁸

In my cases I therefore describe how each step of the procedure takes place and take into account the considerations of all the parties involved. I describe how each enforcement strategy performs on the different variables. These variables are categorized relative to each other in the conclusion, tabled and finally graphed.

⁶¹⁴ Gerring, *Case study Research*, P.151.

⁶¹⁵ Gerring, *Case study Research*, P.172.

⁶¹⁶ Gerring, *Case study Research*, P.181.

⁶¹⁷ Gerring, *Case study Research*, P.178.

⁶¹⁸ Gerring, *Case study Research*, P.184.

PART II: CASE STUDIES

5. TARGETING END USERS DIRECTLY IN THE USA IN 2004-2013

5.1 Introduction

After attempting to bring down infringement by targeting P2P programs like Napster, the Recording Industry Association of America (RIAA) shifted its attention to end users. They targeted end users by connecting to P2P programs and collecting IP addresses uploading copyright protected works. They would then sue unidentified uploaders, use early discovery to ask the courts to authorize subpoenas against the ISPs, to identify the subscribers behind the IP addresses. Afterwards the RIAA lawyers would send letters demanding settlements or amend the lawsuit to name the individual identified. Law firms later copied this tactic and applied it on a larger scale, using the rules of joinder to group many defendants together. This strategy relied on settlement requests and in some cases on an eventual trial. It is therefore divided into two subcases which are different potential phases in the procedure (settlement letter and court case).

This chapter will first provide the legal background to this procedure. For this section I used legal sources and some academic literature. It will then go into the procedure in practice, for which it used legal sources and academic research, supplemented with news articles and reports by NGOs. At the end of that section it will provide some perspectives from practitioners, like Gill Sperlein, a lawyer with numerous clients, who walked me through the process from his perspective and told me the specific problems rights holders are faced with in the pornographic industry. Delvan Neville, a tech expert who served as an expert witness in a number of cases, walked me through the technological process.

After that section, this chapter moves on to the variables. The information mentioned above is supplemented with interviews with Judge Otis Wright and former Judge Nancy Gertner for the judicial perspective from their experience with numerous cases. I also spoke to Mitch Stoltz and Corynne McSherry from the Electronic Frontier Foundation to get a civil rights perspective. Finally, an email conversation with the RIAA gave some of the perspective for large-scale enforcers. Unfortunately, I was unable to speak to most of the law firms targeting end users directly at the time.

The information was collected from January 2012 until the end of 2013.

5.2 Legal background

Although there have been many ways to target end users, all such methods share the aim to target as many users as possible in the most cost-effective way. It was difficult to categorize, because the campaigns happened in different ways. Targeting end users has been done through DMCA subpoenas, through universities, through John Doe lawsuits and pre-settlement letters, and through a later introduced graduated response system called the Copyright Alert System (CAS). The latter was not the subject of this case study.

The Recording Industry of American Association (RIAA) ran a mass end user campaign starting in 2003, and ending in 2008. They stopped because they wanted to seek cooperation with ISPs to deter file sharing (which has led to the copyright alert system).⁶¹⁹

⁶¹⁹ Sarah McBride and Ethan Smith, "Music Industry to Abandon Mass Suits", *The Wall Street Journal* (December 19, 2008), <http://online.wsj.com/article/SB122966038836021137.html>.

Afterwards, other companies took to mass litigation campaigns, which quickly gained notoriety in media coverage and online under the name “copyright trolling.” The name surfaced as a derogatory term to address plaintiffs who sought damages for infringement not to compensate for damages, but as a primary or supplemental revenue stream. It was difficult to determine exactly which firms were “trolling”, and which ones were genuinely trying to compensate for damages.

Although this practice gained notoriety in the past decade (also in relation to patent cases), it was more than a century old. Harry Wall purchased public performance rights in the 1870s that were otherwise unenforced. He then enforced those rights against infringers, finding the statutory penalty of 40 shillings profitable, without going through the creative process himself.⁶²⁰

Targeting end users was possible through US copyright law, which was part of federal law and authorized by the Copyright Clause of the US constitution. Article I, Section 8, Clause 8 said that Congress shall have the power:

“To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.”

The copyright act of 1976 regulated US copyright law, and had been amended by 15 anti-piracy laws since then,⁶²¹ mostly expanding copyright protection, increasing infringement penalties, and creating new enforcement provisions. One of the most important amendments was the Digital Millennium Copyright Act (DMCA) of 1998, which implemented the WIPO copyright directives and added new Internet protection for copyright. It created the safe harbor provisions and created anti-circumvention laws for technological protection measures.⁶²²

Most of US copyright law could be found in title 17 of the United States Code (USC). §106 laid down the exclusive right in copyrighted works for the copyright owner (reproduction, make derivative works, distribution, public performance, publicly display, perform publicly through audio transmission).

Section 501 specified infringement of copyright: anyone who violated any of the exclusive rights of §106 to §122 would be infringing on copyrights. This means there was strict liability. Primary infringement was the main basis for civil suits against individuals. The first file sharing case decided was the *Capitol v. Thomas* case, in which Jammie Thomas was fined 222,000 dollars for “making available” 24 songs over P2P networks.⁶²³

Section 504 provided regulations for damages and profits. An infringer pays the copyright owner’s actual damages or statutory damages. Actual damages are compensatory damages that provide redress for the injuries cause by a wrongdoer and any additional profits the infringer made (the copyright owner is however required to present proof of the

⁶²⁰ James DeBriyn, "Shedding Light on Copyright Trolls: An Analysis of Mass Copyright Litigation in the Age of Statutory Damages." *UCLA Entertainment Law Review* 19.1 (2012). P. 86.

⁶²¹ Amendments: 1982: Piracy and Counterfeiting Amendments Act, 1984: Record Rental Amendment of 1984, 1990: Copyright Remedy Clarification Act, 1990: Computer Software Rental Amendments Act, 1992: Audio Home Recording Act, 1994: Uruguay Round Agreements Act, 1995: The Digital Performance Right in Sound Recordings Act, 1996: Anticounterfeiting Consumer Protection Act of 1996, 1997: No Electronic Theft (NET) Act, 1998: Sonny Bono Copyright Term Extension Act, 1998: Digital Millennium Copyright Act (DMCA), 1999: Digital Theft Deterrence and Copyright Damages Improvement Act of 1999, 2004: Intellectual Property Protection and Courts Amendments Act, 2005: Family Entertainment and Copyright Act, 2008: Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act.

⁶²² 17 USC section 1201 and further.

⁶²³ *Capitol Records Inc. v. Thomas*, 579 F. Supp. 2d 1210, 1213 (D. Minn. 2008)

infringer's gross revenue, whereas the infringer is required to prove his or her deductible expenses and profits that were made not in connection to the infringing work). Statutory damages are unrelated to the harms suffered.⁶²⁴

The choice was in the hands of the copyright owner. Statutory damages were between 750 and 30,000 per infringement, but could increase; if the copyright owner managed to prove that infringement was committed willfully, statutory damages could increase to 150,000. If however the infringer managed to prove that he was not aware and had no reason to believe that his actions constituted an infringement of copyright, the court could reduce the statutory damages to 200 dollars. Other grounds for reducing the damages could be when an infringer believed that his use was fair, in certain jobs under certain conditions. Section 505 provided that in addition, the court could order recovery of the costs and a reasonable attorney's fee. This showed that damages may be very high after copyright infringement cases.

Section 512 provided provisions on liability for material online. They contained safe harbor provisions and provisions that aimed to include ISPs in enforcement. In one part of that section (512(h)), the article provided that a copyright holder "may request that the clerk of any United States district court issue a subpoena to an ISP" to identify an alleged copyright infringer. Rights holders initially relied on this provision to obtain the identities of people allegedly downloading copyright protected material. However, in *Recording Industry Association of America, Inc. v Verizon Internet Services, Inc.*, the United States Court of Appeals for the District of Columbia Circuit put a stop to the record companies' use of § 512(h) subpoenas. The court ruled that under § 512, "a subpoena may be issued only to an ISP engaged in storing on its servers material that is infringing or the subject of infringing activity." In other words, they concluded that subpoenas should not be issued when the ISPs acted as a mere conduit. These ISPs had no power to remove or disable access to copyrighted content and only allowed downloaders the ability to access the Internet.⁶²⁵

The United States Court of Appeals for the Eighth Circuit subsequently agreed with the District of Columbia Circuit, which causes the rights holders to stop pursuing this path to obtain downloaders' identities.⁶²⁶ This meant rights holders were dependant on the rules of discovery to obtain identities on alleged infringers.⁶²⁷

Infringers could also be held criminally liable for infringement. Infringers could be liable in two situations: (1) when the infringement is "for purposes of commercial advantage or private financial gain", or (2) when they distributed "1 or more copies or phonorecords of 1 or more copyrighted works" with a total value greater than \$1,000 within any 180-day period.⁶²⁸ Criminal infringement was punishable by up to ten years in prison (for repeat offenders)⁶²⁹

⁶²⁴ Colin Morrissey, *Behind the Music: Determining the Relevant Constitutional Standard for Statutory Damages in Copyright Infringement Suits*, 78 *Fordham L. Rev.* 3059 (2010). Available at: <http://ir.lawnet.fordham.edu/flr/vol78/iss6/11>

⁶²⁵ *Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc.*, 351 E3d 1229, 1233 (D.C. Cir. 2003), and: Joshua M. Dickman, "Anonymity and the Demands of Civil Procedure in Music Downloading Lawsuits," 82 *TUL. L. REV.* 1049 (2008). P.1053

⁶²⁶ *Charter Commc'ns, Inc., Subpoena Enforcement Matter*, 393 E3d 771, 777 (8th Cir. 2005).

⁶²⁷ Joshua M. Dickman, "Anonymity and the Demands of Civil Procedure in Music Downloading Lawsuits," 82 *TUL. L. REV.* 1049 (2008). P.1058

⁶²⁸ 17 USC section 506

⁶²⁹ 18 USC section 2319

Section 506 described criminal copyright infringement and enforcement. Punishment took place under the rules of section 2319 of title 18. Requirements were that the infringement was willful (which the owner has to prove, simply reproduction or distribution is not enough) and was committed (1) for purposes of commercial advantage or private financial gain, (2) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than 1,000 dollar, or (3) by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public, if such person knew or should have known that the work was intended for commercial distribution. This applied to works of which the copyright owner had a reasonable expectation of commercial distribution, when the copies of the work had not been commercially distributed, or if a motion picture was still in theatres, but copies had not been made available for sale to the general public outside of theatres. Part (b) of this article deals with forfeiture, destruction, and restitution, but referred to section 2323 of title 18.

Title 18 section 2319 dealt with criminal infringement of copyright. It named the punishments for violation of section 506 of title 17. This ranged from jail sentences to large fines.

Targeting multiple individuals at once was enabled by the rules on joinder which were laid down in the Federal Rules of Civil Procedure.⁶³⁰

Rule 19 of the Federal Rules of Civil Procedure addressed situations in which joinder is mandatory, which was "if: (1) complete relief cannot otherwise be granted to those who are already parties, or (2) the person claims an interest relating to the subject of the suit and resolving the suit in the person's absence will either impair the person's ability to protect that interest or leave one or more of the persons already parties to the suit subject to a "substantial risk" of multiple or inconsistent obligations."⁶³¹ Rule 19 did not apply in this case and rights holders have not argued for it in copyright cases.

However, under Rule 20 of the Federal Rules of Civil Procedure, defendants could be joined together in one action under the following conditions:

"(A) Any right to relief is asserted against them jointly, severally, or in the alternative with respect to or arising out of the same transaction, occurrence, or series of transactions or occurrences; and

(B) Any question of law or fact common to all defendants will arise in the action."⁶³²

Meanwhile, Rule 21 simply described that "[m]isjoinder of parties is not ground for dismissal of an action," and that the proper remedy for misjoinder was severance. As a result, on the basis of article 21 courts could sever joinder. This did not mean the action was dismissed, but that the court could drop parties from the action. This happened in

⁶³⁰ 19-21 Federal Rules of Civil Procedure

⁶³¹ Fed. R. Civ. P.19 and Sean B. Karunaratne, "The Case against Combating BitTorrent Piracy through Mass John Doe Copyright Infringement Lawsuits," 111 *Mich. L. Rev.* 283 (2012). P.287. Available at: <http://repository.law.umich.edu/mlr/vol111/iss2/4>

⁶³² Fed. R. Civ. P.20(a)(2) and Sean B. Karunaratne, "The Case against Combating BitTorrent Piracy through Mass John Doe Copyright Infringement Lawsuits," 111 *Mich. L. Rev.* 283 (2012). P.290. Available at: <http://repository.law.umich.edu/mlr/vol111/iss2/4>

numerous cases, where the court argued that merely using the same network was not enough for joinder,⁶³³ or that the case at hand concerned different actions.⁶³⁴

For the BitTorrent lawsuits, the question of joinder proved to be more complicated. This was because BitTorrent made file sharing cooperative.⁶³⁵ It was also decentralized as opposed to earlier P2P file sharing platforms where P2P would establish connections between two users. Copyright holders have therefore argued that BitTorrent "necessitates a concerted action by many people in order to disseminate files" and that therefore joinder should be allowed. They said that joinder was proper because the actions against the joined file sharers arose out of "the same transaction, occurrence, or series of transactions or occurrences."⁶³⁶

Apart from the rules of joinder, this strategy required the rules of discovery to work. After section 512 could not be used for discovery of identities, rights holders moved towards the rules on discovery in the Federal Rules of Civil Procedure. The rules of discovery enabled parties to get access to information and documents relevant to the case. In these cases, rights holders wanted to know the identities, because they only had IP addresses.

They therefore filed a motion for expedited discovery in court. Expedited discovery allows for the discovery of information, before the parties have held a Rule 26(f) discovery conference (the latter can take around three months to commence).⁶³⁷

Rule 26 did not lay down any procedural requirements, but following to case law, judges used two standards to evaluate these requests. A more stringent test that required the showing of some irreparable injury and a more "liberal" test that allowed courts to grant expedited discovery "based on the 'reasonableness of the request in light of all the surrounding circumstances.'"⁶³⁸ Copyright holders argued that they needed expedited

⁶³³ Sean B. Karunaratne, "The Case against Combating BitTorrent Piracy through Mass John Doe Copyright Infringement Lawsuits," 111 *Mich. L. Rev.* 283 (2012). P.290. Available at: <http://repository.law.umich.edu/mlr/vol111/iss2/4> and: *LaFace Records, LLC v. Does 1-38*, No. 5:07-CV-298-BR, 2008 WL 544992, at *1 (E.D.N.C. Feb. 27, 2008); *BMG Music v. Does 1-203*, No. Civ.A. 04-650, 2004 WL 953888, at *1 (E.D. Pa. Apr. 2, 2004); *Interscope Records v. Does 1-25*, No. 6:04-cv-197Orl-22DAB, 2004 U.S. Dist. LEXIS 27782, at *19-20 (M.D. Fla. Apr. 1, 2004). But see, e.g., *Arista Records LLC v. Does 1-19*, 551 E Supp. 2d 1, 11-12 (D.D.C. 2008); *London-Sire Records, Inc. v. Doe 1*, 542 F. Supp. 2d 153, 180-81 (D. Mass. 2008).)

⁶³⁴ Sean B. Karunaratne, "The Case against Combating BitTorrent Piracy through Mass John Doe Copyright Infringement Lawsuits," 111 *Mich. L. Rev.* 283 (2012). P.290. Available at: <http://repository.law.umich.edu/mlr/vol111/iss2/4> and: *BMG Music*, 2004 WL 953888, at *1; see also *Interscope Records*, 2004 U.S. Dist. LEXIS 27782, at *11.

⁶³⁵ Sean B. Karunaratne, "The Case against Combating BitTorrent Piracy through Mass John Doe Copyright Infringement Lawsuits," 111 *Mich. L. Rev.* 283 (2012). P.290. Available at: <http://repository.law.umich.edu/mlr/vol111/iss2/4>

⁶³⁶ *Complaint at 5, Pac. Century Int'l, Ltd. v. Does 1-101*, No. C-1 1-02533 (DMR) (N.D. Cal. July 8, 2011), 2011 WL 246114, and: Sean B. Karunaratne, "The Case against Combating BitTorrent Piracy through Mass John Doe Copyright Infringement Lawsuits," 111 *Mich. L. Rev.* 283 (2012). P.290. Available at: <http://repository.law.umich.edu/mlr/vol111/iss2/4>

⁶³⁷ see also *AF Holdings, LLC v. Does 1-97*, No. C-11-03067-CW (DMR), 2011 WL 2912909, at *1 (N.D. Cal. July 20, 2011), and: Sean B. Karunaratne, "The Case against Combating BitTorrent Piracy through Mass John Doe Copyright Infringement Lawsuits," 111 *Mich. L. Rev.* 283 (2012). P.291. Available at: <http://repository.law.umich.edu/mlr/vol111/iss2/4>

⁶³⁸ *In re Fannie Mae Derivative Litig.*, 227 F.R.D. 142, 142 (D.D.C. 2005) (quoting *Entm't Tech. Corp. v. Walt Disney Imagineering*, No. 03-3546, 2003 WL 22519440, at *3 (E.D. Pa. Oct. 2, 2003)) and Sean B. Karunaratne, "The Case against Combating BitTorrent Piracy through Mass John Doe Copyright Infringement Lawsuits," 111 *Mich. L. Rev.* 283 (2012). P.291. Available at: <http://repository.law.umich.edu/mlr/vol111/iss2/4>

discovery because they could not identify the defendants beyond their IP addresses without subpoenaing the ISPs for the identifying information attached to each address.⁶³⁹

The procedural validity of these lawsuits was evaluated at the motion for expedited discovery⁶⁴⁰ or after it had been granted, on a defendant's or ISPs motion to quash a subpoena requesting the name associated with the IP address.⁶⁴¹

This is relevant, as there was an ongoing discussion on the limits of joinder as applied to these mass lawsuits. So discovery could have been granted without procedural validity because the rules of joinder had been wrongfully applied. Some authors said that judges should consider whether or not defendants were part of the same swarm at the same time as one another, and issues like personal jurisdiction. If those have not been satisfied, the judge should consider severing the cases.⁶⁴²

5.3 The procedure in practice

Rights holders and their representatives have found different ways to target end users directly in the US. This case focused on settlement requests and lawsuits, but also shortly describes the original process through DMCA subpoenas and how rights holders used universities to target students.

DMCA Subpoenas

As a reaction to massive file sharing, The Recording Industry Association of America (RIAA) originally kicked off the large-scale litigation campaigns. Their main goal was to curb illegal content distribution.⁶⁴³

The RIAA started by accessing P2P networks and collecting IP addresses that were uploading/offering recordings owned by their clients.⁶⁴⁴ They needed the help of ISPs to identify the subscribers that matched the IP addresses so they used a subpoena provision included in the DMCA. The RIAA was convinced that the mere allegation of infringement, without judicial oversight, would grant them the power to discover identities of alleged infringers.⁶⁴⁵

⁶³⁹ E.g., *Pac. Century Int'l, Inc. v. Does 1-101*, No. C-11-02533 (DMR), 2011 WL 2690142, at *1 (N.D. Cal. July 8, 2011) and Sean B. Karunaratne, "The Case against Combating BitTorrent Piracy through Mass John Doe Copyright Infringement Lawsuits," 111 *Mich. L. Rev.* 283 (2012). P.291. Available at: <http://repository.law.umich.edu/mlr/vol111/iss2/4>

⁶⁴⁰ E.g., *Nu Image, 799 F. Supp. 2d 34*; *New Sensations, Inc. v. Does 1-1474*, No. C 11-2770 MEJ, 2011 WL 4407222 (N.D. Cal. Sept. 22, 2011) and Sean B. Karunaratne, "The Case against Combating BitTorrent Piracy through Mass John Doe Copyright Infringement Lawsuits," 111 *Mich. L. Rev.* 283 (2012). P.291-292. Available at: <http://repository.law.umich.edu/mlr/vol111/iss2/4>

⁶⁴¹ E.g., *Hard Drive Prods., Inc. v. Does 1-188*, 809 E Supp. 2d 1150 (N.D. Cal. 2011) and Sean B. Karunaratne, "The Case against Combating BitTorrent Piracy through Mass John Doe Copyright Infringement Lawsuits," 111 *Mich. L. Rev.* 283 (2012). P.291. Available at: <http://repository.law.umich.edu/mlr/vol111/iss2/4>

⁶⁴² Sean B. Karunaratne, "The Case against Combating BitTorrent Piracy through Mass John Doe Copyright Infringement Lawsuits," 111 *Mich. L. Rev.* 283 (2012). P.294. Available at: <http://repository.law.umich.edu/mlr/vol111/iss2/4>

⁶⁴³ DeBriyn, "Shedding Light on Copyright Trolls," P. 84.

⁶⁴⁴ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P. 2. And: Lisa Bowman, "Labels aim big guns at file swappers," *CNET News.com* (June 25, 2003).

⁶⁴⁵ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.2, and: 17 USC. 512 (h)

They served subpoenas to numerous ISPs, but Verizon (and Charter Communications and Pacific Bell Internet Services) refused.⁶⁴⁶ Verizon and the others lost the first round in court, so the RIAA issued thousands of subpoenas, reaching more than 1,500 between August and September 2003.⁶⁴⁷ In September 8, 2003, this led to the first 261 lawsuits. The goal of this was deterrence: “It is simply to get peer-to-peer users to stop offering music that does not belong to them,” and: “not to be vindictive or punitive,” all according to then RIAA president Cary Sherman.⁶⁴⁸

Others, like Titan Media (gay hard-core pornographic videos) used the subpoena process to identify and contact individuals, offering them “amnesty” to avoid a potentially embarrassing lawsuit.⁶⁴⁹

After some criticism, the RIAA moved towards sending letters. In October 2003, they sent 204 letters,⁶⁵⁰ offering settlements around 3,000 dollars.⁶⁵¹ 80 people did not accept these settlements and were sued a few weeks later.⁶⁵²

On December 19, 2003, the mass subpoena campaign was brought to a halt when a federal court decided that the DMCA provision only allowed rights holders to seek discovery if the infringing material was stored on an ISP’s network, and not for information stored on subscribers’ computers.⁶⁵³ By that time, the RIAA had already issued more than 3,000 subpoenas⁶⁵⁴, leading to 400 lawsuits, and hundreds of settlements.⁶⁵⁵

Going after students

As part of their new “Deterrence and education initiative”, the RIAA started targeting college students, from February 28, 2007.⁶⁵⁶

They would send out “pre-litigation letters”⁶⁵⁷ to universities with the request that

⁶⁴⁶ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.3.

⁶⁴⁷ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.3, and: Katie Dean, “Senator takes a swing at RIAA,” *Wired* (Sept 17, 2003).

⁶⁴⁸ David Kravets, “File Sparing Lawsuits at a Crossroads, After 5 Years of RIAA Litigation,” *Wired* (September 4, 2008), <http://www.wired.com/threatlevel/2008/09/proving-file-sh/>.

⁶⁴⁹ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.3, and: Grant Gross, “Congress scrutinizes RIAA Tactics,” *IDG News* (September 17, 2003).

⁶⁵⁰ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.3, and: John Borland, “Record Industry warns of new lawsuits,” *CNET News.com* (October 17, 2003).

⁶⁵¹ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.3, and: Paul Roberts, “RIAA Sues 532 John Does,” *IDG News* (January 21, 2004).

⁶⁵² Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.3, and: John Borland, “RIAA files 80 new file-swapping suits,” *CNET News.com* (October 30, 2003).

⁶⁵³ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.3, and *RIAA v. Verizon*, 351 F.3d 1229 (D.C.Cir.2003).

⁶⁵⁴ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.3, and: Roy Mark, “High Court Bounces Latest RIAA Effort,” *InternetNews.com* (October 12, 2004).

⁶⁵⁵ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.4, and: Roy Mark, “High Court Bounces Latest RIAA Effort,” *InternetNews.com* (October 12, 2004).

⁶⁵⁶ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.7, and: Elliot van Buskirk, “A poison pen from the RIAA,” *Wired* (February 28, 2007).

⁶⁵⁷ “RIAA releases yearend anti-piracy statistics,” *Negativland & The RIAA*, http://www.negativland.com/archives/014riaa/piracy_stats.html (the original link was on the RIAA website, but it has disappeared: http://www.riaa.com/newsitem.php?news_year_filter=&resultpage=140&id=876C1BEF-6ACE-E99D-2755-71A875EF2A66)

they would be forwarded to unidentified alleged file sharing students.⁶⁵⁸ In those letters, the RIAA mentioned the IP address and threatens further action unless a settlement is agreed of around 3,000 dollars within 20 days of receiving the letter.⁶⁵⁹

RIAA launched a website to facilitate easy settlements: www.P2Plawsuits.com. Individuals receiving pre-litigation letters could settle their cases there, even by paying with credit card.⁶⁶⁰ Some universities refused to cooperate.⁶⁶¹

John Doe lawsuits by the RIAA, and pre-settlement letters

DirecTV was the first party to ever engage in a mass scale lawsuit campaign. The satellite TV company launched lawsuits against “middlemen” who help others to get free access to their signals. In May 2001, law officers together with DirecTV officials did 3 raids of Internet companies. They seized millions of dollars worth of illegal devices, but also more than 100,000 credit card receipts.⁶⁶²

They then launched an “end-user campaign” by sending mails to 100,000 people who were suspected customers of those middlemen.⁶⁶³ In those mails, customers were contacted by lawyers. The letters cited federal statutes that outlaw piracy or possession of signal theft equipment. They gave recipients a couple of weeks to contact DirecTV or face lawsuits.

When they called the number included in the letter, people would get a settlement offer,⁶⁶⁴ made by a lawyer who would ask them to agree to maintain service with DirecTV for a subscription fee, sign a letter that they would never “steal” DirecTV programming in the future, and pay a financial restitution of between 2,500 and 4,000 dollars. If not, they would be taken to civil court. The letters reached the Internet forums relatively quickly.⁶⁶⁵ In the letters they threatened to sue for 100,000 dollars. The EFF called it a “classic shakedown venture.” DirecTV grouped multiple defendants in one filing to reduce their own costs.⁶⁶⁶ In the process, they filed about 24,000 lawsuits.⁶⁶⁷

It is said that the RIAA copied this practice in 2001, and expanded it as DMCA subpoenas were ruled out by the US courts. On January 21, 2004 the RIAA moved towards “John Doe” lawsuits, starting with 532 people.⁶⁶⁸ The RIAA would sue unidentified uploaders, asking the courts to authorize subpoenas against the ISPs, to identify the subscribers behind

⁶⁵⁸ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.7, and: Thomas Mennecke, “RIAA Announces new campus lawsuit strategy,” *Slyck* (February 28, 2007).

⁶⁵⁹ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.7, and: Ken Fisher, “Students largely ignore RIAA instant settlement offers,” *Ars Technica* (March 26, 2007).

⁶⁶⁰ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.8.

⁶⁶¹ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.8.

⁶⁶² Graham Brink, “DirecTV turns to state courts for piracy suits,” *St. Petersburg Times Online* (November 1, 2003), http://www.sptimes.com/2003/11/01/State/DirecTV_turns_to_stat.shtml.

⁶⁶³ Admin, “DirecTV prepares to sue,” *Geek* (July 31, 2001), <http://www.geek.com/news/directv-prepares-to-sue-545136/>.

⁶⁶⁴ Kevin Poulsen, “DirecTV dragnet snares innocent techies,” *SecurityFocus* (July 7, 2003), <http://www.securityfocus.com/news/6402>.

⁶⁶⁵ “DirecTV Lawsuit on End Users,” *FreeAdvice* (February 10, 2001), <http://forum.freeadvice.com/civil-litigation-46/directv-lawsuit-end-users-77220.html>.

⁶⁶⁶ “DirecTV accuses thousands of signal theft,” *The Baltimore Sun* (November 30, 2003), http://articles.baltimoresun.com/2003-11-30/business/0311290123_1_directv-satellite-television-piracy.

⁶⁶⁷ “DirecTV to Narrow Anti-Piracy Campaign,” *The Electronic Frontier Foundation* (June 16, 2004), <https://www.eff.org/effector/17/22>

⁶⁶⁸ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.4, and: John Schwartz, “Recording Industry is accusing 532 people of Music piracy,” *New York Times* (January 21, 2004).

the IP addresses. Afterwards the RIAA lawyers would send letters demanding settlements or amend the lawsuit to name the individual identified.⁶⁶⁹ Some speculated that they reached about 30,000 people by October 2007.⁶⁷⁰

In those letters, the RIAA pushed for settlements ranging between 3,000 dollars and 11,000 dollars.⁶⁷¹

In practice, this strategy relied on permissive joinder, discovery and statutory damages, which have all been mentioned in the previous section. In some cases, the nature of the copyright protected content played a role as well.

Initially, rights holders like the RIAA would obtain the IP addresses of alleged infringers by using the P2P programs used for infringement and searching for copyrighted works. They would collect the IP addresses of users sharing the work.⁶⁷²

The main problem rights holders faced was that to target these users, they needed to ascertain their true identities.⁶⁷³ The collected IP address only revealed the subscriber's ISP, but only the ISP itself will be able to link the IP to a name and address.⁶⁷⁴

After collecting the IP addresses, the record companies would not name the defendants individually, but they would file a suit against a group of anonymous "John Doe" downloaders sharing the same ISP, stating that the listed John Does had infringed on their copyright. Whilst filing this suit, they also filed motions for expedited discovery to subpoena the Does' ISP to discover the Does' real names and information. They started using this approach after the D.C. Circuit Court of Appeals shut down their strategy of using the DMCA to subpoena ISPs to obtain identifying information of users uploading files, as mentioned in the previous section.⁶⁷⁵ Many courts simply agreed and issued subpoenas. Firms kept costs low by filing claims in a single complaint. Normally plaintiffs would have to file a lawsuit against each IP address to get the power to subpoena ISPs to get the identities, which costs 350 dollars per complaint. Dealing with larger numbers of Does saved millions of dollars. This streamlined the discovery process. Normally, a rights holder filed a complaint naming each defendant as a "John Doe" defendant. When the identity was later discovered, the complaint was amended to include the real party to the complaint.⁶⁷⁶

However, these cases rarely went to court. Uncovering the identities was the end goal,⁶⁷⁷ because plaintiffs would aim for settlements.⁶⁷⁸ Their litigation strategy hinged on

⁶⁶⁹ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.4.

⁶⁷⁰ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.5, and: Jeff Leeds, "Labels win suit against song sharer," *New York Times* (October 5, 2007).

⁶⁷¹ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.5, and: Ted Bridis, "Some strange twists in music piracy lawsuits," *Associated Press* (August 23, 2004).

⁶⁷² Sean B. Karunaratne, "The Case against Combating BitTorrent Piracy through Mass John Doe Copyright Infringement Lawsuits," 111 *Mich. L. Rev.* 283 (2012). P.286-287. Available at: <http://repository.law.umich.edu/mlr/vol111/iss2/4>

⁶⁷³ Joshua M. Dickman, "Anonymity and the Demands of Civil Procedure in Music Downloading Lawsuits," 82 *TUL. L. REV.* 1049 (2008). P.1056

⁶⁷⁴ *Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc.*, 351 F3d 1229, 1232 (D.C. Cir. 2003)

⁶⁷⁵ Joshua M. Dickman, "Anonymity and the Demands of Civil Procedure in Music Downloading Lawsuits," 82 *TUL. L. REV.* 1049 (2008). P.1053

⁶⁷⁶ DeBriyn, "Shedding Light on Copyright Trolls," P.95.

⁶⁷⁷ Memorandum of Amicus Curiae Electronic Frontier Foundation in Support of Third Party Time Warner Cable's Motion to Quash or Modify Subpoena at 1, *Third World Media LLC v. Does 1-1243*, No. 3:10-cv-0090, (N.D. W. Va. Nov. 23, 2010), available at <https://www.eff.org/files/filenode/wvcopyrighttroll/thirdworldmediavdoesamicus.PDF>

the defendants' acceptance of their settlement offer. After learning the true identity of the alleged infringer, the lawyer or rights holder could send out a pre-settlement letter, in which they asked them to pay an amount if they did not want to be named in a suit.⁶⁷⁹ The offer was designed in such a way as to "push" the defendant to settle, even if they have strong defenses.⁶⁸⁰

Part of this push was based on the threat of being named in a suit and facing higher damages in court (including legal costs for the defense). This push was particularly effective because of the high statutory damages the law provided for copyright infringement and because of a few high profile cases in the past in which large sums of money were awarded as punishment. In their settlement letters, some lawyers explicitly refer to these statutory damages.⁶⁸¹ The lawyer then offers a significantly lower settlement amount,⁶⁸² sometimes even through an automated online payment portal.⁶⁸³ Lawyer Steele for example threatened with statutory damages and attorney's fees: "Under the Copyright Law of the United States, copyright owners may recover up to \$150,000 in statutory damages (...) per infringing file plus attorney's fees in cases (...) In at least one case where the Copyright Law has been applied to digital piracy and statutory damages were applicable, juries have awarded over \$20,000 per pirated file."⁶⁸⁴

Another part of this push at times involved the nature of the copyright protected work in question. Many cases involved pornographic material which could make people more inclined to settle to prevent the public exposure of a lawsuit.

"Trolls?"

In the context of mass litigation, the term "copyright troll" surfaced as a derogatory term referring to some law firms enforcing copyright on a large scale. Professor Shyamkrishna Balganesh defined them as follows: "A copyright troll refers to an entity whose business revolves around the systematic legal enforcement of copyrights in which it has acquired a limited ownership interest."⁶⁸⁵

⁶⁷⁸ Sean B. Karunaratne, "The Case against Combating BitTorrent Piracy through Mass John Doe Copyright Infringement Lawsuits," 111 *Mich. L. Rev.* 283 (2012). P.284-285. Available at: <http://repository.law.umich.edu/mlr/vol111/iss2/4>

⁶⁷⁹ DeBriyn, "Shedding Light on Copyright Trolls," P. 98, and: Julie Cohen, "Pervasively distributed copyright enforcement." *Georgetown Law Journal* 95 (2006). P.17.

⁶⁸⁰ Sean B. Karunaratne, "The Case against Combating BitTorrent Piracy through Mass John Doe Copyright Infringement Lawsuits," 111 *Mich. L. Rev.* 283 (2012). P.285. Available at: <http://repository.law.umich.edu/mlr/vol111/iss2/4>

⁶⁸¹ DeBriyn, "Shedding Light on Copyright Trolls," P.99.

⁶⁸² Julie Cohen, "Pervasively distributed copyright enforcement." *Georgetown Law Journal* 95 (2006). P.17.

⁶⁸³ See "Defendant Record ID Login," *Copyright settlements*, <http://dglegal.force.com/SiteLogindglegal> (last visited Feb. 10, 2012) ("All Major Credit Cards Accepted"). <http://www.copyrightsettlements.com/>

⁶⁸⁴ See, e.g., Settlement Letter from John L. Steele, Attorney, Steele Hansmeier, PLLC (May 16, 2011), http://msnbcmedia.msn.com/i/MSNBC/Sections/NEWS/z_Personal/AJohnson/110719_Steele_Hansmeier_Settlement_Letter.pdf (explaining statutory damages and offering to settle \$2900). Plus here: <https://dietrolldie.files.wordpress.com/2011/09/57230736-settlement-letter.pdf>

⁶⁸⁵ Shyamkrishna Balganesh, The Uneasy Case Against Copyright Trolls, 86 *S. CAL. L. REV.* 723, 739–40 (2013). P.732.

James DeBriyn has written an article on “trolls” who enforce copyrights as a business model. He distinguishes three different types.⁶⁸⁶ The sample troll, the online news troll, and the troll that uses mass file sharing litigation as a business model.

The sample troll makes millions by suing (mostly popular) artists who have used a part of a copyrighted work (a sample) in their own songs. There are examples where trolls bought the rights to commercially unsuccessful songs and enforced them against others who used the sample and only after those new songs became commercially successful, generating massive profits. They more often sue for actual damages (instead of statutory damages) because they are motivated by the commercial success of the derivative work. As an example, Drive-In Music Company sued Sony BMG entertainment, because Cypress Hill’s song ‘How I Could Just Kill a Man’ used a sample from ‘Come On In’ by Music Machine.⁶⁸⁷

One of the first new copyright trolls was an online news troll, called Righthaven. Righthaven purchased the copyrights of various newspapers’ content, and sued users that reposted old articles on other websites. Righthaven sued for permanent injunctions, statutory damages, attorney fees, and costs, and demanded ownership of the domain name of the infringing website. They allowed the people they sued to settle for 5,000 dollars, which is less than the potential statutory damages, or the cost of hiring an attorney to defend against infringement claims. However, their campaign has been described as a failure because some judges have ordered Righthaven to pay legal and attorney fees, rendering their model less profitable.⁶⁸⁸

The most famous of the mass file sharing law firms (called mass litigation trolls by DeBriyn) was the firm ‘Dunlap, Grubb & Weaver,’ also known as the ‘Copyright Group.’ This firm sought to “create a revenue stream and monetize the equivalent of an alternative distribution channel,” according to DeBriyn.⁶⁸⁹ They first represented Voltage pictures and sought statutory damages from a large number of unknown defendants for infringement of the Award winning movie ‘The Hurt Locker.’ The business model aimed to generate profits through the threat of statutory damages, by seeking settlements. After representing Voltage pictures, they represented other movie studios in mass litigation (though never the MPAA).⁶⁹⁰

I tried to contact them. When they answered the phone, they immediately asked “are you calling because you received a notification?” They refused to comment further.

Another firm, the Adult Copyright Company (“Hardcore protection”), used the nature of the content to leverage settlements. To avoid the stigma of being named in a pornography lawsuit, individuals could be more quickly to settle.⁶⁹¹

Apart from those groups, there were also actual scams that played into the large-scale enforcement business, like the “Internet copyright law enforcement agency.” They claimed to be an “international organization that helps to enforce copyright laws on the Internet worldwide by informing potential copyright law violators regarding the serious criminal and/or civil liability they may face, and providing them with an opportunity to help them comply with copyright laws.”

⁶⁸⁶ DeBriyn, “Shedding Light on Copyright Trolls,” P.86.

⁶⁸⁷ DeBriyn, “Shedding Light on Copyright Trolls,” P.86-88.

⁶⁸⁸ DeBriyn, “Shedding Light on Copyright Trolls,” P.88-90.

⁶⁸⁹ DeBriyn, “Shedding Light on Copyright Trolls,” P.90.

⁶⁹⁰ DeBriyn, “Shedding Light on Copyright Trolls,” P.90.

⁶⁹¹ Greg Sandoval, “Porn studios’ copyright lawyer: ‘I will sue’ (Q&A), *Cnet* (Oct 5, 2010), and: James DeBriyn, “Shedding Light on Copyright Trolls: An Analysis of Mass Copyright Litigation in the Age of Statutory Damages.” *UCLA Entertainment Law Review* 19.1 (2012). P.91.

This 'agency' sent out numerous copyright infringement notices to users, asking them to pay up to 495 dollars or face felony charges and jail time for infringement. This agency was later revealed to be a scam that intended to shake down users for money.⁶⁹²

Practicioners and experts

For my research, I got the perspectives of praticioners through interviews. They said that a lot of the BitTorrent litigation has centered on independent movies or adult movies.⁶⁹³ The litigation campaigns were, however, highly lawyer-driven. "Lawyers came up with a model that was not just a deterrent but also meant to return some profits lost to infringement. They needed to keep litigation costs low." "So they sued large numbers, offer relatively low settlements and then lawyers would be paid a percentage of those settlements and rights holders would get a percentage too."⁶⁹⁴ According to Delvan Neville, there was a number of more large-scale 'trolling' operations, which he referred to as "lawsuit factories."⁶⁹⁵

Prenda Law was the most famous one (at the time of the interview) but was running into trouble.⁶⁹⁶ It was driven by two lawyers, who were filing "all over the country."⁶⁹⁷

According to Delvan Neville, "Prenda has lied all over the place. It's difficult to know how much is real. They have no shame about saying things that are not true at all."⁶⁹⁸

Apart from that, there is the above mentioned Copyright Enforcement Group (CEG)⁶⁹⁹, Guardaley⁷⁰⁰, the IPP⁷⁰¹ (which stands for Intellectual Property Protection – which mainly helps photographers), and the Crystal Bay Corporation⁷⁰². According to Delvan Neville, the last two used Guardaley software. "They present themselves as separate entities, but use the same software and business."⁷⁰³

In these interviews, the practitioners gave their perspectives on the procedure as it involved or impacted them. For example, they said that generally, lawyers had a tech company in-house, or that they hired one to spot and gather information on infringing users. They did this on P2P software, like BitTorrent and eDonkey.⁷⁰⁴

This tech company then gathered information on the infringing IP and provided it to the attorney. They usually attached a time date stamp. Sometimes they also added the seed (the logarithm that identifies the seed), and sometimes they added information on the user.⁷⁰⁵

⁶⁹² AnnePMitchell, "Is the "Internet Copyright Law Enforcement Agency" Real or a Scam? Here's What We Know," *The Internet Patrol* (February 21, 2013), <http://www.theInternetpatrol.com/is-the-Internet-copyright-law-enforcement-agency-real-or-a-scam-heres-what-we-know/>, and: Timothy B. Lee, "New troll scam: Pay us \$495 or face felony charges and jail time," *Ars Technica* (February 22, 2013), <http://arstechnica.com/tech-policy/2013/02/new-troll-scam-pay-us-495-or-face-felony-charges-and-jail-time/>.

⁶⁹³ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁶⁹⁴ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁶⁹⁵ Delvan Neville (technologist), interviewed by author, September 2013.

⁶⁹⁶ Delvan Neville (technologist), interviewed by author, September 2013.

⁶⁹⁷ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁶⁹⁸ Delvan Neville (technologist), interviewed by author, September 2013.

⁶⁹⁹ Delvan Neville (technologist), interviewed by author, September 2013.

⁷⁰⁰ Delvan Neville (technologist), interviewed by author, September 2013.

⁷⁰¹ Delvan Neville (technologist), interviewed by author, September 2013.

⁷⁰² Delvan Neville (technologist), interviewed by author, September 2013.

⁷⁰³ Delvan Neville (technologist), interviewed by author, September 2013.

⁷⁰⁴ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁷⁰⁵ Gill Sperlein (Lawyer) interviewed by author, September 2013.

According to Sperlein, the method to collecting IP's this way was accurate. He said IP spoofing did not work because it required someone to know the correct address to get it to work. People might have put fake IP addresses in the seed file, "but if the tech investigator is any good at all they will ping the IP address. So you will eliminate the spoofed ones."⁷⁰⁶ Sperlein also said that false positives were avoided because the "IP address is the source of the infringing file."⁷⁰⁷

The Prenda law firm has used in-house technology. They used a modified BitTorrent client to get IP addresses.⁷⁰⁸

About the procedure in practice, Sperlein also addressed his experience with the rules of joinder. "One can only join cases if it will reduce the work on the court." He mentioned that this was only possible if the transaction occurred as part of the same transaction. Right holders would generally join people from the same swarm (not just ISPs). They were in the same transaction.⁷⁰⁹

After getting the IP addresses, it was possible to spot at which ISP those addresses were based, so the lawyers lumped those together. They sued against does 1-50, and tried to get early discovery at the judge.⁷¹⁰

Early discovery was possible because if someone cannot serve summons and complaints they have to be able to identify. If a court allowed it they would send a subpoena to an ISP like ATNT with a list of IP addresses.⁷¹¹ The ISP would then send you back a list with all the names and addresses. According to Sperlein "they will charge you for it– not legally – but they would."⁷¹²

Then they looked at the people participating within a certain time frame. For example, they could log how long it would take for one person to download a file, and log all the people participating in that swarm at that same time.⁷¹³

According to Neville, the Copyright Enforcement Group system differed from the others. They recorded the infringement, but they did not only pursue people in court through early discovery. "They send notices via ISPs to individuals (basically a DMCA notice) giving those users a code: saying here's a specialized code, if you punch it in, pay a 200 dollar fee, the issue will be settled outside of court. So they don't do the whole discovery thing Prenda does. Then if an individual goes to a website they identify themselves in that way."⁷¹⁴ No one could tell me who the ISPs were that CEG used. According to Sperlein, there were one or two ISPs who have done it. He said ISPs generally refused to cooperate.⁷¹⁵ The Copyright Enforcement Group unfortunately refused to verify this.

The interviewees also went into the content of the letters that were sent out by themselves or the other law firms. Gill Sperlein would send a subpoena, plus a letter with factual information, which would include information on how to contact EFF, and tell them their rights to object to the subpoena. This information would be based on litigation with the

⁷⁰⁶ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁷⁰⁷ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁷⁰⁸ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁷⁰⁹ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁷¹⁰ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁷¹¹ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁷¹² Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁷¹³ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁷¹⁴ Delvan Neville (technologist), interviewed by author, September 2013.

⁷¹⁵ Gill Sperlein (Lawyer) interviewed by author, September 2013.

RIAA, where ISPs stood in place of count holders. Most courts did not require it, but Sperlein put it in.⁷¹⁶

Sperlein said that sending the letter was often difficult because he would only have the name of the account holder. “This is the problem of the proverbial grandmother: you never know who actually committed infringement. But we know it came from that account. This is still the beginning of an investigation. We could theoretically do forensic analysis of those computers in the house or look for actual file, which would take around 5,000 dollars when we look to settle for less. For either side it does not make sense to go through that. This became a judgment call.” Sperlein would try to figure out whether alleged infringers were lying or he would have them sign a declaration under penalty of perjury.⁷¹⁷ “But it’s the account holder, so not the actual infringer. It’s not that it didn’t happen, but you do not always identify the infringer at the first step.”⁷¹⁸

The large-scale firms took another approach. Malibu Media (IPP) would ask for a few thousand dollars, so under what it would cost to fight the case. CEG would ask for a couple of hundred dollars. In CEG’s case, there were no real counterclaims, because there was not a case filed. The defendant could not accomplish anything in CEG cases. It was difficult to figure out how many people were targeted, because there was no paper trail.⁷¹⁹

People often settled out of embarrassment (especially where it concerned pornographic content). Sperlein said some of the other law firms wanted to use the nature of the content as a means to leverage settlements. He said that Prenda and others would go after things like transvestite pornography or particularly “salacious” material to get a higher settlement. According to Sperlein this was bad. It also became the mantra of the other side, he said.⁷²⁰

Tech expert Delvan Neville said people also settled because the settlement amounts were often much lower than the cost of legal representation. These threats work, because of famous cases like the Jammie Thomas case, where the defendant was ordered to pay large amounts of money. Some large-scale actors in the stock-photo area have gone for judgments first, so they could use them as leverage later. Masterfiles.com was one of those large-scale actors that asked for around 3-4,000 dollars now.⁷²¹ “Many people don’t realize that the statutory damages or the higher damages are the maximum,” says Delvan Neville. “Doesn’t realize or understand this. But attorney fees and costs are still there. In the Bellwether case, where actors went through trial first, it was 300,000 dollars for that part (the attorney fees and costs) alone.”⁷²²

People also settled because copyright infringement is strict liability. “Although the circumstances might affect the level of damages, whether you understood the law or not, it does not matter: you copied it, you’re responsible,” Sperlein says.⁷²³ “Why would you risk all the fees? I would send out letters with link, with settlement agreement and allow them to pay through PayPal. People would do it, so they are clearly guilty,” again Sperlein.⁷²⁴ He said

⁷¹⁶ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁷¹⁷ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁷¹⁸ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁷¹⁹ Delvan Neville (technologist), interviewed by author, September 2013.

⁷²⁰ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁷²¹ Delvan Neville (technologist), interviewed by author, September 2013.

⁷²² Delvan Neville (technologist), interviewed by author, September 2013.

⁷²³ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁷²⁴ Gill Sperlein (Lawyer) interviewed by author, September 2013.

he did take the personal circumstances into account, “because I wanted to do it in a way that is smart and morally right.”⁷²⁵

5.4 Scale, severity and procedural safeguards

Scale

Righthaven had filed numerous lawsuits expecting huge amounts of money ranging around 75,000 dollars. The website <http://www.righthavenlawsuits.com/> kept track of all of this.

In the first six months the RIAA targeted students, they sent letters to 2.926 students at 100 different campuses in the US.⁷²⁶ After a year, this became over 5.400 letters to 160 different schools.⁷²⁷ The RIAA expanded their practice as DMCA subpoenas were ruled out by the US courts. On the 21st of January 2004, the RIAA started their “John Doe” lawsuits, starting with 532 people.⁷²⁸ The RIAA would sue unidentified uploaders, asking the courts to authorize subpoenas against the ISPs, to identify the subscribers behind the IP addresses. Afterwards the RIAA lawyers would send letters demanding settlements or amend the lawsuit to name the individual identified.⁷²⁹

In 2004, the RIAA filed 5.460 lawsuits.⁷³⁰ By the end of 2005, the total number of RIAA lawsuits had risen to 16.087.⁷³¹ After February 2006, when the counter had reached 17.587, the RIAA stopped making announcements on the exact number of suits. Some speculated that this number ranged in the 30,000 by October 2007.⁷³² It took the RIAA five years to sue 35,000 individuals according to others.⁷³³ Of those cases only two cases actually went to trial.⁷³⁴ The RIAA themselves said they only brought action against 18,000 individuals. They also said that the majority led to settlements.⁷³⁵

Law firms sued over 100,000 does in only thirteen months, starting on January 1, 2010.⁷³⁶ Ars Technica immediately wrote an article about how their numbers surpassed the RIAA in less time.⁷³⁷

⁷²⁵ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁷²⁶ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.8, and: Susan Butler, “Sixth Wave of RIAA Pre-Litigation Letters Sent to Colleges,” *The Hollywood Reporter Esquire* (July 19, 2007).

⁷²⁷ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.8, and: Eric Bangeman, “Pass or Fail? RIAA’s College Litigation Campaign Turns One,” *Ars Technica* (February 27, 2008).

⁷²⁸ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.4, and: John Schwartz, “Recording Industry is accusing 532 people of Music piracy,” *New York Times* (January 21, 2004).

⁷²⁹ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.4.

⁷³⁰ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.4, and: “RIAA Brings lawsuits against 762 file sharers,” *RIAA press release* (September 30, 2004).

⁷³¹ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.4.

⁷³² Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.5, and: Jeff Leeds, “Labels win suit against song sharer,” *New York Times* (October 5, 2007).

⁷³³ DeBriyn, “Shedding Light on Copyright Trolls,” P.91.

⁷³⁴ DeBriyn, “Shedding Light on Copyright Trolls,” P.91.

⁷³⁵ Cara Duckworth (Communications at the Recording Industry Association of America) email to author (October 2013).

⁷³⁶ James DeBriyn, “Shedding Light on Copyright Trolls: An Analysis of Mass Copyright Litigation in the Age of Statutory Damages.” *UCLA Entertainment Law Review* 19.1 (2012). P.91.

⁷³⁷ Nate Anderson, “US anti-P2P law firms sue more in 2010 than RIAA ever did,” *Ars Technica* (October 7, 2010), <http://arstechnica.com/tech-policy/2010/10/us-anti-p2p-law-firms-sue-more-in-2010-than-riaa-ever-did/>.

Although it is difficult to find concrete data on the exact number of people targeted, EFF said there were well over 100,000 John Does. Also, there were over 2,000 actual case filings.⁷³⁸ By August 2011, there were already over 200,000 John Does.⁷³⁹ For the CEG it was difficult to determine how many there had been, because they also used ISPs to send notices to Internet users directly. There was no paper trail.

On a subcase level, this means the amount of settlement letters ranged in the hundreds of thousands in the USA as a whole, while there were only very few actual trials.

Severity

There were different types of sanctions. The actual damages awarded by courts, and the settlements requested by law firms or rights holders and actually paid for by users. The actual damages awarded by courts (the few times a verdict was actually reached) were high, because of the system of statutory damages. The most famous one is the first ever file sharing case, against Jammie Thomas, who was ordered to pay \$222,000 in damages.⁷⁴⁰ Very few suits led to a verdict. The Thomas case was redone after a faulty jury instruction and a second jury found Thomas liable for a larger \$1.92 million statutory damage award.⁷⁴¹ The case would eventually total multiple court cases, with as a final judgement by the appeals court reinstating the original verdict of \$222,000 in damages and deeming the high damages as constitutional.⁷⁴² The other major suit (against Tenenbaum), filed by Sony, awarded the record labels \$22,500 per song for thirty songs for a judgment totaling \$675,000.⁷⁴³

Other judgments were less high, but nonetheless incredibly high for individual users. A court awarded a 22,500 dollar judgment against a Chicago woman.⁷⁴⁴ Another court awarded 40,850 in damages against an Arizona man who attempted defense without a lawyer.⁷⁴⁵ Ignoring lawsuits can be more expensive than settling. One judge has by default awarded 6,200 dollars.⁷⁴⁶

With regards to settlements, the RIAA settled for amounts ranging between 3,000 dollars and 11,000 dollars.⁷⁴⁷ Malibu Media (IPP) would ask for a few thousand dollars which is under what it would cost to fight the case. "The CEG just asked for a couple of hundred dollars" according to Delvan Neville.⁷⁴⁸

⁷³⁸ Mitch Stoltz (Staff attorney at Electronic Frontier Foundation) interviewed by author, September 2013.

⁷³⁹ Ernesto, "200,000 Bittorrent users sued in the United States," *Torrentfreak* (August 8, 2011), <http://torrentfreak.com/200000-bittorrent-users-sued-in-the-united-states-110808/>.

⁷⁴⁰ Capitol Records Inc. v. Thomas, 579 F. Supp. 2d 1210, 1213 (D. Minn. 2008), and: Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.5, and: Eric Bangeman, "RIAA Trial Verdict Is In: Jury Finds Thomas Liable for Infringement," *Ars Technica* (October 4, 2007).

⁷⁴¹ Capitol Records Inc. v. Thomas-Rasset, No. 06cv-1497 (D. Minn. Jan. 22, 2010).

⁷⁴² Capitol Records Inc. v. Thomas-Rasset, No. 11-2820 (United States Court of Appeals for the Fifth Circuit. September 11, 2012).

⁷⁴³ Sony BMG Music Entm't v. Tenenbaum, No. 07cv1 1446-NG (D. Mass. Dec. 7, 2009)

⁷⁴⁴ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.5, and: Bob Mehr, "Gnat, Meet Cannon," *Chicago Reader* (February 4, 2005).

⁷⁴⁵ Electronic Frontier Foundation, "RIAA v The People: Five years later" (2008). P.5, and: Jon Healey, "Another File-sharer Faces Costly Day of Reckoning," *L.A. Times Technology Blog* (September 2, 2008).

⁷⁴⁶ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.5, and: Ted Bridis, "Some Strange Twists in Music Piracy Lawsuits," *Associated Press* (August 23, 2004).

⁷⁴⁷ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.5, and: Ted Bridis, "Some strange twists in music piracy lawsuits," *Associated Press* (August 23, 2004).

⁷⁴⁸ Delvan Neville (technologist), interviewed by author, September 2013.

Safeguards

Privacy

Whether or not this enforcement strategy interfered with privacy rights, depended on whether personal data was processed. This usually happens when infringement is found, and when enforcing parties have access to personal data.

In this case, infringement was found by participating in the P2P network. The RIAA and MPAA used MediaSentry to collect information about IP addresses that potentially infringed files via P2P networks. They created lists of potentially infringing files and checked that with files offered for download by IP addresses. They also actually downloaded from an IP address, and added dates and times of observations.

There was some controversy over MediaSentry, because in some US states it was not officially licensed as a private investigator, which caused some defendants to argue to disregard any evidence collected by MediaSentry.⁷⁴⁹

Originally RIAA wanted to get the identities of file sharing IP addresses by sending subpoenas to ISPs to sue those customers. However, when Verizon resisted the subpoenas validity on procedural and privacy grounds, the appeals court finally held that the DMCA regulation only applies to data hosted by an Internet service provider, and not to data on a customer's computer. As a result, the RIAA and other enforcers had to file individual civil suits against each accused file sharer, and can find out the name under supervision of a court. There were now more ways for users and ISPs to prevent this access to personal data by enforcing parties.⁷⁵⁰

Soon after getting to know the identity of those users, they were often sent settlement forms where they could agree to pay several thousand dollars to the RIAA and sign an agreement not to engage in any further file sharing. This procedure has been protested, because it allowed for the stripping of anonymity without the possibility to challenge this in court.⁷⁵¹

The lawyers used tech companies or had in-house technology to identify users. The only barriers they faced were ISPs and judges. The firms needed to supply a user's IP address and the time the infringement occurred to an ISP to get the identity of an infringer. The copyright group used a company to monitor P2P networks for illegal distribution of the Hurt Locker, but the method used was a secret.⁷⁵² However, it was not that difficult but also not

⁷⁴⁹ Thomas Mennecke, "RIAA Not Impressed with Legal Concerns Surrounding MediaSentry," *Slyck* (February 6, 2008),

<http://www.slyck.com/story1657> RIAA Not Impressed with Legal Concerns Surrounding MediaSentry, and: Eric Bangeman, "MediaSentry site redesign drops references to litigation," *Ars Technica* (February 20, 2008), <http://arstechnica.com/tech-policy/2008/02/mediasentry-site-redesigned-loses-references-to-litigation/>.

⁷⁵⁰ "Subpoena Defense: Defending the constitutional rights of Internet users and ISPs," *Subpoena Defense*, <http://www.subpoenadefense.org/>, last visited on April 12, 2011.

⁷⁵¹ "Citing Right to Anonymity Online, ACLU Asks Boston Court to Block Recording Industry Subpoena," *American Civil Liberties Union* (September 29, 2003), <http://www.aclu.org/technology-and-liberty/citing-right-anonymity-online-aclu-asks-boston-court-block-recording-industry>, and: "Record Industry Cuts Corners in Crusade Against File-Sharers," *Public Citizen* (February 2, 2004), <http://www.citizen.org/pressroom/pressroomredirect.cfm?ID=1636>.

⁷⁵² DeBriyn, "Shedding Light on Copyright Trolls," P. 91, and: DGW hired Guardaley Ltd. to collect data using a "proprietary tracing software program to trace the IP address for each Defendant." Id. Guardaley gathered the

that reliable.⁷⁵³ These addresses were then checked for quality and chance of success (for example, addresses outside of the jurisdiction could be dropped).⁷⁵⁴ These IP addresses could be cross referenced against IP log databases controlled by the ISP. However, not all ISPs were willing to share this information. This meant that copyright holders had to file a complaint to get the power to subpoena.⁷⁵⁵

In my interviews, former judge Nancy Gernter said she did not like this process. “I didn’t like that the RIAA went to universities when they found an IP address which was listed at a university. This took place without the owner of the IP address knowing that this was going on. When they came to me for subpoenas, I put in place a requirement that required them to tell the university that they had to tell the IP owner that they could contest it. I wanted a procedure in place to allow people whose identity would be disclosed the right to fight it. I did that on my own. There was no defendant so I had to protect potential defendants.”⁷⁵⁶

Impartial, competent and independent judge

There were numerous opportunities for review during this enforcement strategy: in the settlement letter phase and later in the potential trial phase. To start with the latter, I had no reason to doubt the impartiality, independence or competence of the judges eventually involved in the court cases on copyright infringement.

In the settlement phase, review on the merits of the case was only done by the parties bringing the claim. Gill Sperlein for example mentioned that he would take personal circumstances into account. He wanted to “do it in a way that is smart and morally right.”⁷⁵⁷ This was admirable, but there were no real legal incentives to make sure enforcement happened in such a way. The incentives all pointed in the other way as law firms bringing the claim could stand to benefit financially from these claims. They also had little to lose from their assertions.

The settlement phase also included review by a judge to assess whether early discovery and joinder were allowed. I also had no reason to doubt their impartiality, independence or competence.

IP address of the suspect user, the time of the infringement, the ISP of the user and a note of the property being distributed. Exhibit C to Motion for Leave for Discovery (Hurt Locker), Voltage Pictures, LLC v. Does 1–5,000, No. 1:10-cv-00873 (D.D.C. June 7, 2010), ECF No. 4-3. The data collected concerning the Hurt Locker was gathered in about one week. Id.

⁷⁵³ DeBriyn, “Shedding Light on Copyright Trolls,” P. 91. and: Ben Jones, “How Any BitTorrent User Can Collect Lawsuit Evidence,” *Torrentfreak* (September 3, 2010), <http://torrentfreak.com/how-any-bittorrent-user-can-collect-lawsuit-evidence-100903/>; Jones also opines that the data gathered may not be particularly reliable. Id. Gaurdaley explained that to identify infringers they download portions of the copyrighted property from a user. Declaration of Patrick Achache in Support of Plaintiff’s Motion for Leave to Take Discovery Prior to Rule 26(f) Conference at ¶¶ 8-9, Voltage Pictures, LLC v. Does 1–5,000, No. 1:10-cv-00873 (D.D.C. June 7, 2010), ECF No. 4-2.

⁷⁵⁴ DeBriyn, “Shedding Light on Copyright Trolls,” P.93-94.

⁷⁵⁵ DeBriyn, “Shedding Light on Copyright Trolls,” P.94.

⁷⁵⁶ Nancy Gertner (Professor at Harvard Law School) interviewed by author, October 2013.

⁷⁵⁷ Gill Sperlein (Lawyer) interviewed by author, September 2013.

Presumption of innocence

As mentioned in the section above, the merits of the case could only be judicially reviewed if alleged infringers protested the settlement request brought forwards by the plaintiffs. This protest was however actively discouraged, by creating economic incentives to settle. This potentially reversed the presumption of innocence.

This procedure placed little burden of proof on the accusing parties. This was because the judicial review that took place in the settlement phase was intended to evaluate whether there were sufficient grounds to grant early discovery and allow for joinder. It was not the same test as a full trial on copyright would have.

Even for just discovery and joinder, some authors claimed there were strong procedural reasons to reject these claims. There might be improper joinder and a lack of personal jurisdiction by the court.⁷⁵⁸ The same writer said that when those issues were raised, district courts were "split on whether to allow discovery of the anonymous defendants' identities."⁷⁵⁹

The rights holders generally filed the Doe lawsuits in the jurisdictions where the ISP connected to the Does had their headquarters or some other significant presence. This made sense as the the rights holders did not know where the Does live. However, courts needed to have personal jurisdiction over a defendant to be able to deliver a judgement.⁷⁶⁰ Meanwhile, joinder could need to be severed when the requirmenets of joinder were not fulfilled.⁷⁶¹ For example, the district court in *Dragon Quest Products, LLC v. Does 1–100* held that: [T]he initial seeder, other seeders, the various peers, and the Defendants may have participated in this swarm months apart from each other. While the four categories of individuals, the initial seeder, the other seeders, the peers, and the Defendants, may be connected by the same initial seed file, the Court finds that this connection alone is not sufficient to establish joinder."⁷⁶²

The settlement requests placed the burden of proof on the defendants. It is unclear how much evidence was provided by the plaintiffs, in those settlement requests, but they were designed in a way to incentivize settlements instead of proper weighing of the evidence. The requests asked for smaller amounts of money that it would take to get legal aid or fight the case, at times they referred to the potential of very high statutory damages and in some cases they used the nature of the content to leverage settlements.

This was problematic. Because they had to keep administrative costs low, plaintiffs have been described as "not so meticulous" in their search for targets."[S]ince an innocent John Doe is just as likely to pay up as a guilty one," the lawyers did not need to take much

⁷⁵⁸ Sean B. Karunaratne, "The Case against Combating BitTorrent Piracy through Mass John Doe Copyright Infringement Lawsuits," 111 *Mich. L. Rev.* 283 (2012). P.285. Available at: <http://repository.law.umich.edu/mlr/vol111/iss2/4>

⁷⁵⁹ Sean B. Karunaratne, "The Case against Combating BitTorrent Piracy through Mass John Doe Copyright Infringement Lawsuits," 111 *Mich. L. Rev.* 283 (2012). P.285. Available at: <http://repository.law.umich.edu/mlr/vol111/iss2/4>

⁷⁶⁰ Joshua M. Dickman, "Anonymity and the Demands of Civil Procedure in Music Downloading Lawsuits," 82 *TUL. L. REv.* 1049 (2008). P.1068

⁷⁶¹ Joshua M. Dickman, "Anonymity and the Demands of Civil Procedure in Music Downloading Lawsuits," 82 *TUL. L. REv.* 1049 (2008). P.1104

⁷⁶² *Dragon Quest Prods., LLC v. Does 1–100*, Civ. Nos. 12–6611 (JHR/AMD), 12–6633 (NLH/AMD), 13–482 (NLH/AMD), 13–483 (NLH/AMD), 13–484 (NLH/AMD), 13–485 (NLH/AMD), 13–486 (NLH/AMD), 13–487 (NLH/AMD), 2013 WL 2949407, at *6 (D.N.J. June 14, 2013).

care in ensuring that the John Doe actually was engaged in infringing activity. The strategy has been described as "shoot first, and identify ... targets later."⁷⁶³

My interviewees confirmed this picture. Even though the subpoena was required because of due process rights, discovery was granted easily, according to Delvan Neville.⁷⁶⁴

Judge Otis Wright said that the accusing party had to give evidence on how the subpoena request would translate into the identity of an infringer. "They have to make that connection, with a degree of certainty that gives me comfort."⁷⁶⁵

When I asked whether he considered granting subpoenas 'rubber stamping', he said: "it's a simple thing. Everyone is entitled to discovery in litigation. Third party discovery is almost routinely granted, if it appears to be reasonable in its face. For something like that it's reasonable to find out the identity. The easiest way is to go to an ISP."⁷⁶⁶

When I asked how he evaluated discovery requests, he also said "I didn't subject it to a great deal of scrutiny. I can't speak for anybody else."⁷⁶⁷ He did say "I was judge to handle all of the cases, in that process to – I had seen half of district judges and magistrate judges had granted the request for the issuance of a subpoena for the ISP to obtain the identity of a subscriber. So some do, some don't. It isn't a situation that is going to get, demand, or require much thought."⁷⁶⁸

When I asked how much thought, Judge Otis Wright said that "generally in the past there hasn't been. Now that we have come to understand the wide scale abuse that has taken place, they will get a lot more scrutiny, certainly from me. There are things I'm going to be more curious about knowing. I want to know about the nature of the alleged infringed product." As an example, he mentioned the difference between a Disney and a pornographic movie.⁷⁶⁹

Former judge Nancy Gertner said she did not want to rubber stamp, which is why she went through extra lengths to arrange for extra defenses for defendants.⁷⁷⁰

Mitch Stoltz from the EFF says that the burden of proof rests heavily on users that receive letters. This is because the only formal arbitrators in the procedure, judges who grant discovery, do not evaluate the evidence thoroughly. "Courts are really busy. They have to make tough decisions about life and death. They are underfunded and pressed for time. When they see something that looks straightforward, and there's no opposition and no defendants, it looks legit. The judge has no incentive to dig deeper, because that would be more work for them. A judge therefore counts on the honesty and good will of lawyers. The whole system depends on that. That's why they (FK: these law firms) were able to do this for so long."⁷⁷¹

⁷⁶³ See Keegan Hamilton, *Porn, Piracy, & BitTorrent*, SEATTLE WKLY. (Aug. 10, 2011), <http://www.seattleweekly.com2011-08-10/news/porn-piracy-bittorrent/>. And Sean B. Karunaratne, "The Case against Combating BitTorrent Piracy through Mass John Doe Copyright Infringement Lawsuits," 111 *Mich. L. Rev.* 283 (2012). P.304. Available at: <http://repository.law.umich.edu/mlr/vol111/iss2/4>

⁷⁶⁴ Delvan Neville (technologist), interviewed by author, September 2013.

⁷⁶⁵ Otis D. Wright, II (District Judge) interviewed by author, September 2013.

⁷⁶⁶ Otis D. Wright, II (District Judge) interviewed by author, September 2013.

⁷⁶⁷ Otis D. Wright, II (District Judge) interviewed by author, September 2013.

⁷⁶⁸ Otis D. Wright, II (District Judge) interviewed by author, September 2013.

⁷⁶⁹ Otis D. Wright, II (District Judge) interviewed by author, September 2013.

⁷⁷⁰ Nancy Gertner (Professor at Harvard Law School) interviewed by author, October 2013.

⁷⁷¹ Mitch Stoltz (Staff attorney at Electronic Frontier Foundation) interviewed by author, September 2013.

However, later judges have started questioning this process. Malibu media ran into trouble. Prenda law as well.⁷⁷² The EFF also said some judges started to notice these red flags.⁷⁷³

This followed a large consumer backlash. This backlash was mainly directed against Prenda law, who had filed lawsuits all over the US. It resulted in multiple allegations against John Steele, one of its main lawyers. According to Sperlein, this created a bad name for all adult entertainment lawyers.⁷⁷⁴

He says that the new people who were doing it for adult industries were lawyers who did not understand the business and who had never represented the adult industry before.⁷⁷⁵ According to Sperlein, “Federal judges started getting wind of these tactics.” Also, he says “EFF and its supporters were really good at avoiding question of liability in those copyright cases, and focused on the process.”⁷⁷⁶

Because of this, courts became more reluctant to grant discovery. Gill Sperlein says: “It’s over. No one’s doing it anymore.”⁷⁷⁷ He said federal courts have said that they do not want this type of litigation, because it is “inherently sleazy.”⁷⁷⁸

Judge Otis Wright said in the future these request will be subject of much more scrutiny. He would for example check “If that is the product in question. Then the first question I’m going to have is: is this case really about protecting the IP rights? Or is this literally a shakedown, in which they are enlisting the assistance of the court?”⁷⁷⁹

According to him, it was not “over”, but “I simply think there will be no rubber stamps anymore. People will take a look. The subject material becomes important now. I can’t say I ever enquired into the subject material. I probably never knew. Now, because of the abuses. There’s going to be a hard look. We are just going to ask some questions now.”⁷⁸⁰

He said one of the things they will look at is the type of product. “I am going to be curious as to whether or not the 80 year old great grandmother is going to be interested in Vin Diesel. I am going to require a bit more evidence, in order to be satisfied that –one- it isn’t a shakedown, - two - that once you get this info, it is more likely that the identity of the infringer is actually found. Trolls have done a disservice to entire industry. They have caused this practice to come under greater scrutiny, because it has been abused. There have been situations where they have no intention whatsoever of trying these cases. The goal is to simply extract a settlement. The best way to do that is to cause or threaten to cause the John Doe defendant as much embarrassment as possible.”⁷⁸¹ Mitch Stoltz of the EFF also said that the threat of public accusing someone of downloading porn is much stronger. “It just is. That’s a fact of life.”⁷⁸²

Judge Otis Wright said that in future cases, he would also look at the evidence that was supplied. He said that in the past various kinds of evidence had been used. Sometimes

⁷⁷² Delvan Neville (technologist), interviewed by author, September 2013.

⁷⁷³ Mitch Stoltz (Staff attorney at Electronic Frontier Foundation) interviewed by author, September 2013.

⁷⁷⁴ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁷⁷⁵ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁷⁷⁶ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁷⁷⁷ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁷⁷⁸ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁷⁷⁹ Otis D. Wright, II (District Judge) interviewed by author, September 2013.

⁷⁸⁰ Otis D. Wright, II (District Judge) interviewed by author, September 2013.

⁷⁸¹ Otis D. Wright, II (District Judge) interviewed by author, September 2013.

⁷⁸² Mitch Stoltz (Staff attorney at Electronic Frontier Foundation) interviewed by author, September 2013.

there was no evidence at all, sometimes they simply said that they have made a phone call, and that there was only one person in the household. “What has never been answered to my satisfaction is: how do you know that the Internet was not accessed by someone not in the household? You can’t be certain that simply because a particular subscriber’s Wi-Fi was accessed for something illegal, that the subscriber is responsible. You can’t establish with certainty that it was someone in the household at all.”⁷⁸³

Corynne McSherry of the EFF said that even though it is hard to dispute that a lot of the people do unauthorized copying, trolls set up a system thoroughly biased against defendants. “It’s designed to extract settlements, because they know equally likely that people pay up when they are not guilty.”⁷⁸⁴ About the evidence, she says that because copyright is strict liability, there is a low standard of evidence.⁷⁸⁵

The EFF doubted that the high settlement amounts were necessarily an indication of ‘guilt.’ They said that it was hard to tell whether or not there were a lot of false positives. “My feeling is that because the incentives to settle are so high and the incentives to identify the right people are so low, and because they are just identifying subscribers and not the users, that there has to be a high rate of false positives.”⁷⁸⁶ There were also numerous defenses that could not be brought forward now. “So even signing something saying that you did it, does not mean you did it. Even if 90% or 99% did it. I care about the other 1%. I think we have a responsibility as citizens and lawyers that those people aren’t paying money they should not be paying,” Mitch Stoltz of the EFF said.⁷⁸⁷

Notice, right to be heard (prior to conviction), defenses and appeal

Parties are notified, but this is already the settlement request. The judicial review that took place was when plaintiffs first filed a motion for expedited discovery. However, John Does could not contest a motion for expedited discovery, and therefore these motions only provided one side of the story.⁷⁸⁸

Because the game ended after discovery most of the time, this was problematic.⁷⁸⁹

Technically there was a right to be heard prior to conviction, but the system was used by large-scale players to incentivize settlements, as mentioned before. As some authors have put it: “For the plaintiffs in mass lawsuits against BitTorrent file sharers, the game is

⁷⁸³ Otis D. Wright, II (District Judge) interviewed by author, September 2013.

⁷⁸⁴ Corynne McSherry (Intellectual Property Director Electronic Frontier Foundation) interviewed by author, September 2013.

⁷⁸⁵ Corynne McSherry (Intellectual Property Director Electronic Frontier Foundation) interviewed by author, September 2013.

⁷⁸⁶ Mitch Stoltz (Staff attorney at Electronic Frontier Foundation) interviewed by author, September 2013.

⁷⁸⁷ Mitch Stoltz (Staff attorney at Electronic Frontier Foundation) interviewed by author, September 2013.

⁷⁸⁸ Millennium TGA, Inc. v. Does 1-21, No. 11-2258 SC, 2011 WL 1812786, at *3 (N.D. Cal. May 12, 2011), and: Sean B. Karunaratne, “The Case against Combating BitTorrent Piracy through Mass John Doe Copyright Infringement Lawsuits,” 111 *Mich. L. Rev.* 283 (2012). P.292. Available at: <http://repository.law.umich.edu/mlr/vol111/iss2/4>

⁷⁸⁹ 10 Grp., Inc. v. Does 1-435, No. CIO-04382 SI, 2011 WL 445043, at *6 (N.D. Cal. Feb. 3, 2011), and: Sean B. Karunaratne, “The Case against Combating BitTorrent Piracy through Mass John Doe Copyright Infringement Lawsuits,” 111 *Mich. L. Rev.* 283 (2012). P.292. Available at: <http://repository.law.umich.edu/mlr/vol111/iss2/4>

essentially won or lost at the expedited discovery stage.⁷⁹⁰ Defenses were possible, but potentially costly. Appeal was also possible, but would mean trial.

My interviewees confirm this perspective. When talking about the money it could potentially cost to go to trial, Judge Otis Wrights said: “you won’t risk it. That’s why it is such a wonderful scheme.”⁷⁹¹ Corynne McSherry said that this process wreaks havoc on rules of civil procedure. “As a lawyer I care about that.”⁷⁹² According to former judge Nancy Gertner, who was involved in a lot of the RIAA litigation, most of those cases settled: because of the threat – without a doubt.⁷⁹³ That is why she put in place multiple systems to protect users, like the opportunity for them to object to a discovery request.⁷⁹⁴

She would also periodically hold conferences in which she would invite all the defendants and try to explain the law to them. She would give them a list of free counsel. She said: “I certainly had to do more than I would if there had been lawyers on the other side.”⁷⁹⁵ She said “the hearing is something I chose to do to communicate with defendants.” It was for “kids, who were ignoring court messages or orders.”⁷⁹⁶ “I took time out of my schedule –I gave them 2 minute lessons in the law.”⁷⁹⁷

Alleged infringers had little defenses. Former judge Nancy Gertner said that for the RIAA cases, “most of the time -around 99% - people were not represented by lawyers. The vast majority settled, because they had no resources to defend. They also settled because the record companies often had them: there was nothing to defend.”⁷⁹⁸ Other people were represented by lawyers, but even those settled. Only Tenenbaum went to trial.⁷⁹⁹

She said there was “not a more clear case of unequal resources than this case. There would be 4-5 lawyers on one side representing the RIAA, and on the other side an individual with his mother or friend.”⁸⁰⁰ “Nobody had the resources to hire a lawyer – so navigating through discovery requirements was often times impossible, the settlements ranged from a couple of thousands to 8,000 or 9,000.”⁸⁰¹

She might have considered defenses, “I thought: there might be an argument if it had been downloaded before it was available legally online. Or someone on 1 or 2 cases. Fair use might comprise.”⁸⁰² So there may have been defenses. “I knew them broadly, but they were never raised before me, and in Tenenbaum they were raised badly.”⁸⁰³

Because the practice became well known throughout the Internet, users allegedly file sharing stopped paying the pre-settlement money, and became familiar with several

⁷⁹⁰ Sean B. Karunaratne, “The Case against Combating BitTorrent Piracy through Mass John Doe Copyright Infringement Lawsuits,” 111 *Mich. L. Rev.* 283 (2012). P.291. Available at: <http://repository.law.umich.edu/mlr/vol111/iss2/4>

⁷⁹¹ Otis D. Wright, II (District Judge) interviewed by author, September 2013.

⁷⁹² Corynne McSherry (Intellectual Property Director Electronic Frontier Foundation) interviewed by author, September 2013.

⁷⁹³ Nancy Gertner (Professor at Harvard Law School) interviewed by author, October 2013.

⁷⁹⁴ Nancy Gertner (Professor at Harvard Law School) interviewed by author, October 2013.

⁷⁹⁵ Nancy Gertner (Professor at Harvard Law School) interviewed by author, October 2013.

⁷⁹⁶ Nancy Gertner (Professor at Harvard Law School) interviewed by author, October 2013.

⁷⁹⁷ Nancy Gertner (Professor at Harvard Law School) interviewed by author, October 2013.

⁷⁹⁸ Nancy Gertner (Professor at Harvard Law School) interviewed by author, October 2013.

⁷⁹⁹ Nancy Gertner (Professor at Harvard Law School) interviewed by author, October 2013.

⁸⁰⁰ Nancy Gertner (Professor at Harvard Law School) interviewed by author, October 2013.

⁸⁰¹ Nancy Gertner (Professor at Harvard Law School) interviewed by author, October 2013.

⁸⁰² Nancy Gertner (Professor at Harvard Law School) interviewed by author, October 2013.

⁸⁰³ Nancy Gertner (Professor at Harvard Law School) interviewed by author, October 2013.

defenses against the allegations (like: my Wi-Fi is unsecure).⁸⁰⁴ Sperlein says that the IP only identifies the account holder, so not the actual infringer. “It’s not that it didn’t happen,” he says, “but you don’t always identify the infringer at the first step. Steele (from Prenda Law) and others never had the intention to go to the next step.”⁸⁰⁵ Then people started responding less. “Grubb, Weaver (of the Copyright Enforcement Group) and Steele would take just what they could and then move on. They were just looking for fast money to pocket. They weren’t looking for the long term perspectives of their clients.”⁸⁰⁶

Transparency

This system is opaque. The only paper trail was at the courts, which granted discovery. This gave details on the discovery process only, but not on the specifics of the cases, and whether or not there was proof that the users actually infringed on copyrights.

For the Copyright group, there was even less paper trail, as they apparently did not even use the help of courts to get contact details and simply got some ISPs to forward settlement requests for them.

Proportionality

Proportionality requires that the measure is necessary for its goal, suitable and no excessive burden on individual rights.

One of the first ways to assess whether the measure is proportional is whether the measure is necessary for its goal. In this case, that remained questionable. It was difficult to determine the exact losses of the separate studios, and whether money was actually flowing back to those studios rights now. It was certainly suitable to get a refund for the larger scale law firms, but the RIAA themselves viewed it as an educational system only. It did present an excessive burden on the parties it addresses. Statutory damages had no relationship to the harm of infringement. Fines ere much higher than they would be for similar offenses, and much higher than the losses incurred by studios. During the RIAA campaign for example, the EFF mentioned that ‘Tammy Lafky faced 500,000 dollars in penalties (RIAA offered to settle for 4,000 dollars), but she made only 21,000 dollars per year, had no child support and was a single mom.⁸⁰⁷ Cassi Hunt, another alleged infringer, faced a 3,750 dollars settlement, but already had student debt. The RIAA argued that she should drop out to pay off the settlement.⁸⁰⁸ These in some cases severe penalties have been the subject of discussion.⁸⁰⁹ Some American scholars have debated the constitutionality of statutory damages for copyright.⁸¹⁰ Some have tried to fight the constitutionality of these damages in court.⁸¹¹ It

⁸⁰⁴ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁸⁰⁵ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁸⁰⁶ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁸⁰⁷ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.5, and: “Minnesota Woman Caught in Crackdown on Music Downloaders,” *USA Today* (June 11, 2004).

⁸⁰⁸ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.6, and: Cassi Hunt, “Run Over by the RIAA Don’t Tap the Glass,” *The Tech* (April 4, 2006).

⁸⁰⁹ See for example: Colin Morrissey, “Behind the Music: Determining the Relevant Constitutional Standard for Statutory Damages in Copyright Infringement Suits,” *78 Fordham L. Rev.* 3059 (2010), <http://ir.lawnet.fordham.edu/flr/vol78/iss6/11>

⁸¹⁰ Colin Morrissey, “Behind the Music: Determining the Relevant Constitutional Standard for Statutory Damages in Copyright Infringement Suits,” *78 FordhamL. Rev.* 3059 (2010),

was interesting that during the Thomas Rasset trial, music industry executives and musicians themselves were surprised by the size of the verdicts.⁸¹²

5.5 Impact on infringement levels

Bridy wrote that mass litigation against end users had only limited deterrent effects.⁸¹³ There was only a “transitory deterrent effect.” Surveys conducted done at the end of 2003 and at the beginning of 2004, after the RIAA began their campaign, showed a decrease of file sharing in the US. But follow on surveys showed that percentage had rebounded by 2005.⁸¹⁴ For the thousands of people who got sued, there were millions who were not.⁸¹⁵ The fear about being prosecuted declined among users.⁸¹⁶

Another study showed that lawsuits against end users produced a negative effect and intensified the development of new tech to make it harder to identify the user.⁸¹⁷

After the RIAA’s lawsuits, P2P activity continued growing.⁸¹⁸ According to BitChampagne, P2P traffic doubled since the start of the lawsuits by RIAA.⁸¹⁹ The amount of users as well:⁸²⁰ by 2007 and 2008 that number had continued to grow.⁸²¹ The amount of people that share illegally remained fairly constant until 2008, at around 19 %.⁸²²

<http://ir.lawnet.fordham.edu/flr/vol78/iss6/11>, and: Pamela Samuelson & Ben Sheffher, Debate, “Unconstitutionally Excessive Statutory Damage Awards in Copyright Cases,” 158 *U. PA. L. REV. PENNUMBRA* 53 (2009), <http://www.pennumbra.com/debates/pdfs/CopyrightDamages.pdf>

⁸¹¹ Colin Morrissey, “Behind the Music: Determining the Relevant Constitutional Standard for Statutory Damages in Copyright Infringement Suits,” 78 *FordhamL. Rev.* 3059 (2010), <http://ir.lawnet.fordham.edu/flr/vol78/iss6/11>, and: See, e.g., Motion for a New Trial, Remittitur, and to Alter or Amend the Judgment at 2, 4-5, *Capitol Records Inc. v. Thomas-Rasset*, No. 06-cv-1497 (D. Minn. July 6, 2009)

⁸¹² Colin Morrissey, “Behind the Music: Determining the Relevant Constitutional Standard for Statutory Damages in Copyright Infringement Suits,” 78 *FordhamL. Rev.* 3059 (2010), <http://ir.lawnet.fordham.edu/flr/vol78/iss6/11>, and: Copyrights & Campaigns ((June 20, 2009), <http://copyrightsandcampaigns.blogspot.com/2009/06/sony-bmg-attomey-we-were-shocked-by.html>, Daniel Kreps, “Richard Marx “Ashamed” He’s Linked to \$1.92 Million RIAA Fine Against Minnesota Mom,” *Rolling Stone magazine*, (June 24, 2009), <http://www.rollingstone.com/rockdaily/index.php/2009/06/24/richard-marx-ashamed-hes-linked-to-192-million-riaa-fineagainst-minnesota-mom>, Posting of Moby to Moby.com (June 20, 2009), <http://www.moby.com/journal/2009-0620/riaa-have-sued-jammie-thomas-rasset-minn.html>

⁸¹³ Bridy, “Why Pirates (Still) Won’t Behave,” P.590-596.

⁸¹⁴ Lee Rainie, et al., “Pew Internet Project and Comscore Media Metrix Data memo, The state of Music Downloading and File-Sharing Online,” *Pew Research Center* (2004) P.1-2., http://www.pewInternet.org/~media/Files/Reports/2004/PIP_FilesSharing_April_04.pdf.pdf
through: Bridy, “Why Pirates (Still) Won’t Behave,” P.604.

⁸¹⁵ Bridy, “Why Pirates (Still) Won’t Behave,” P.604.

⁸¹⁶ Bridy, “Why Pirates (Still) Won’t Behave,” P.604.

⁸¹⁷ Bridy, “Why Pirates (Still) Won’t Behave,” P.604.

⁸¹⁸ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.9, and: Andre Broido et al, “Is P2P dying or just hiding?,” *Global Internet and Next Generation Networks*, (November/December 2004).

⁸¹⁹ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.9, and: “P2P Volume Climbs Again in June, User Levels Near 9 Million,” *Digital Music News Blog* (July 8, 2005).

⁸²⁰ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.9-10, and: John Boudreau, “Illegal file sharing showing no letup,” *San Jose Mercury News* (July 3, 2006).

⁸²¹ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.10, and: Eric Bangeman, “P2P Traffic Shifts Away From Music, Towards Movies,” *Ars Technica* (July 5, 2007).

⁸²² Sarah McBride and Ethan Smith, “Music Industry to Abandon Mass Suits,” *The Wall Street Journal* (December 19, 2008), <http://online.wsj.com/article/SB122966038836021137.html>.

My interviewees had their own perspectives on the effectiveness of mass litigation campaigns. Gill Sperlein for example said that “another reason to stop doing it was that it was teaching more people that BitTorrent existed.”⁸²³

The RIAA said: “the campaign had run its course. In the beginning, we set out to change the public perception around sites like Napster which were championing the idea that if it was available on the Internet for free it must be legal. Fast forward to 2008 (when we discontinued the lawsuit program) and there were hundreds of legitimate services worldwide offering fans millions of authorized songs in convenient ways and people knew that getting music off of sites like LimeWire was illegal. We succeeded in raising awareness about the problems of piracy. Now we’re focused on promoting the burgeoning legitimate music marketplace, which now boasts more than 500 authorized services worldwide where fans can get their favorite music at the click of a mouse or the tap of a finger. That’s why we partnered with music retailer organization the Music Business Association to create an informational website www.whymusicmatters.com that offers fans a one-stop guide on where to get their favorite legal music.”

The RIAA said it did not want to pursue the pre-settlement letters made popular by a number of US law firms. They said: “We’re not interested in pursuing that route. Instead, we’re focused on educational warnings to prevent illegal downloading via the Copyright Alert System, and promoting the wide array of legitimate services available to fans today via whymusicmatters.com and other efforts.”⁸²⁴

On the graduated response system, they said: “We do prefer this program, in part because it offers users several opportunities to do the right thing. It is premised on the notion that users may not know that illegal downloading is occurring in their house, so it takes an educational approach by sending the account holder warnings about illegal activity on their account. These warnings also provide users a list of authorized music services (via whymusicmatters.com). We know hardcore downloaders will not be deterred by this program, and will likely never be deterred, but to the extent that we can peel off some casual downloaders and get them interested in one of the many legitimate services out there, that’s a win.”⁸²⁵

But apart from deterrence, or “raising awareness”, litigation could have had other functions. Gill Sperlein, a lawyer who has represented the pornography industry, said litigation could also be seen as a “first line of defense” until rights holders figured out their business models. In the copyright domain, this was common according to Sperlein. He said that every technological advancement faced initial resistance by copyright owners.⁸²⁶ He advised his clients about three ways to deal with these advancements: litigate, educate, and change business models. “You must do all three.” “Litigation is the least attractive: it’s the most expensive and most time consuming.”⁸²⁷ He said “litigation slows developments down until technology or legislation catches up as well. The DMCA was passed twenty years ago, before P2P was invented.”⁸²⁸ It also allowed rights holders to “slow things down so they can

⁸²³ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁸²⁴ Cara Duckworth (Communications at the Recording Industry Association of America) email to author, October 2013.

⁸²⁵ Cara Duckworth (Communications at the Recording Industry Association of America) email to author, October 2013.

⁸²⁶ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁸²⁷ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁸²⁸ Gill Sperlein (Lawyer) interviewed by author, September 2013.

figure out their business models” in a way that allowed them to “continue to monetize their creative process.”⁸²⁹

Another reason for mass litigation campaigns is that they could be used as a genuine retrieval of damages. According to Sperlein, mass copyright infringement was more damaging to the pornography industry than to the other creative industries. This was because there were many economic differences between both. First of all, there were no box office runs for porn. “These are just like mainstream movies that go straight to DVD and make no money at all.”⁸³⁰

He said the pornography industry also benefitted less from advertising than other content producers do, and advertising was one of the main new models for the retrieval of funds online. The top 100 most popular websites contained 6-8 adult orientated tube sites, so the potential would be big, but there were difficulties with advertising, he said. The big companies did not want to be associated with adult content. So those websites mostly contained advertisement for scams: fake Viagra, or advertisement for other porn sites like live cam sites. Most free content aimed to get users to those cam sites. Sperlein said that under the current model “no money goes back to content producers.” “However, there were ways in which one could compete. On tube sites the resolution was not that good and HD is better.” It was however more difficult to compete with BitTorrent infringement, he said. “The saving grace is that BitTorrent is not something the average user is comfortable with.”⁸³¹ Although he said some Tube sites were “playing along” with rights holders now, although there were still “underground groups.”⁸³² Also, the pornographic industry was much more decentralized. Playboy and Hustler were exceptions, all the other studios were much smaller. There was no RIAA or MPAA. “The RIAA represents 90% of music titles. We can represent one title only.”⁸³³

Nonetheless, it caused the industry to “focus on P2P infringement.” And because the torrent tracker websites were mostly located in other countries, they were “difficult to go after.” So, the “only practical way is to sue the end users” to retrieve funds.⁸³⁴ Especially, Sperlein says, because the newly developed Copyright alert system (CAS) did not deal with the adult entertainment industry. “Disney is at the table.”⁸³⁵

The lawyers that sent out thousands of demand letters on behalf of the producers of the Movie “the hurt locker” confirmed that their litigation campaign was not intended as a compensation or as deterrence but to “creat[e] a revenue stream and monetiz[e] the equivalent of an alternative distribution channel.”⁸³⁶

Because of the notoriety of those practices, less people settled. Sperlein estimates that at first 80% of the cases were resolved in the pre-trial phase, whereas nowadays this number is “probably less than 20%.”⁸³⁷

⁸²⁹ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁸³⁰ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁸³¹ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁸³² Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁸³³ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁸³⁴ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁸³⁵ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁸³⁶ Eriq Gardner, New Litigation Campaign Quietly Targets Tens of Thousands of Movie Downloaders, HOLLYWOOD REP. (Dec. 21, 2010, 10:56 AM), <http://www.hollywoodreporter.com/blogs/thr-esq/litigation-campaign-quietly-targets-tens-63769>.

⁸³⁷ Gill Sperlein (Lawyer) interviewed by author, September 2013.

5.6 The costs of the system

Costs were an important factor in this strategy. For rights holders, their representatives, and the large-scale firms, economic feasibility predicted whether they would actually engage in litigation like strategies.

According to some, for the RIAA, the massive lawsuits RIAA were a “money pit.”⁸³⁸ In the five year period the RIAA spent 90 million dollars on legal fees, whilst only recovering 2.5 million dollars. According to those sources, this is why the RIAA stopped.⁸³⁹

The large-scale firms had to be able to continue, so they made the strategy economically feasible. They did this by keeping costs low. They filed claims in a single complaint. Normally plaintiffs would have to file a lawsuit against each IP address to get the power to subpoena ISPs to get the identities, which would cost around 350 dollars per complaint. Since they dealt with larger numbers of does, they saved millions of dollars. This streamlined the discovery process. Normally, a rights holder would file a complaint naming each defendant as a “John Doe” defendant. When the identity would be later discovered, the complaint was amended to include the real party to the complaint.⁸⁴⁰ DirecTV grouped multiple defendants in one filing to reduce their own costs.⁸⁴¹ In the process, they filed about 24,000 lawsuits.⁸⁴² In essence, mass lawsuits were “a strong tool for leveraging settlements—a tool whose efficiency is largely derived from the plaintiffs’ success in avoiding the filing fees for multiple suits and gaining early access en masse to the identities of the alleged infringers.”⁸⁴³

Some judges were not happy with the process and have said that by circumventing joinder and personal jurisdiction rules, these plaintiffs used copyright laws to implement a low-cost, high-volume litigation strategy that was tantamount to a “massive collection scheme.”⁸⁴⁴ Some of them also were not happy with the evasion of filing fees. In one case, the court estimated that “plaintiffs have improperly avoided more than \$25,000 in filing fees by employing its swarm joinder theory. . . . Nationwide, these plaintiffs have availed themselves of the resources of the court system on a scale rarely seen. It seems improper that they should profit without paying statutorily required fees.”⁸⁴⁵

Rights holders have also used other techniques to keep costs low. Righthaven used a model complaint it reused as a template for pleading.⁸⁴⁶

⁸³⁸ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). P.10-11.

⁸³⁹ DeBriyn, “Shedding Light on Copyright Trolls,” P.85: cites numerous IRS forms over period between 2004-2008.

⁸⁴⁰ DeBriyn, “Shedding Light on Copyright Trolls,” P.95.

⁸⁴¹ “DirecTV accuses thousands of signal theft,” *The Baltimore Sun* (November 30, 2003), http://articles.baltimoresun.com/2003-11-30/business/0311290123_1_directv-satellite-television-piracy.

⁸⁴² “DirecTV to Narrow Anti-Piracy Campaign,” *The Electronic Frontier Foundation* (June 16, 2004), <https://www.eff.org/effector/17/22>

⁸⁴³ *MCGIP, LLC v. Does 1-149*, No. C 11-02331 LB, 2011 WL 4352110, at *4 n.5 (N.D. Cal. Sept. 16, 2011). And: Sean B. Karunaratne, “The Case against Combating BitTorrent Piracy through Mass John Doe Copyright Infringement Lawsuits,” 111 *Mich. L. Rev.* 283 (2012). P.304. Available at: <http://repository.law.umich.edu/mlr/vol111/iss2/4>

⁸⁴⁴ *On the Cheap, LLC v. Does 1-501t*, No. C10-4472 BZ, 2011 WL 4018258, at *5 n.6 (N.D. Cal. Sept. 6, 2011), and: Sean B. Karunaratne, “The Case against Combating BitTorrent Piracy through Mass John Doe Copyright Infringement Lawsuits,” 111 *Mich. L. Rev.* 283 (2012). P.292. Available at: <http://repository.law.umich.edu/mlr/vol111/iss2/4>

⁸⁴⁵ E.g., *In re BitTorrent Adult Film Copyright Infringement Cases*, 296 F.R.D. 80, 92 (E.D.N.Y. 2012).

⁸⁴⁶ DeBriyn, “Shedding Light on Copyright Trolls,” P.95.

Meanwhile, some authors have argued that this system affects the way copyright is supposed to function. In an article on “copyright trolls”, Professor Balganesch argues that copyright trolls disrupt the “enforcement equilibrium” central to copyright’s function as an institution.⁸⁴⁷ In short, he argued that this strategy forces a disconnection between the incentive to create new content and the incentive to litigate. Originally, this connection would exist in all copyright holders. As the incentive to enforce is based on a cost-benefit analysis, some claims are tolerated despite being actionable as such. Because “trolls” have no interest in the creation, distribution or use of creative works, this equilibrium is disrupted.⁸⁴⁸

My interviewee also discussed the costs of the procedure. They said that joinder was also beneficial because it saved legal costs. In fact, the rules of joinder were designed to prevent an excessive burden on courts. As judge Otis Wright puts it: “there have been occasions in the past where the courts have been presented with a large number of cases often brought by the same plaintiff or alleged copyright owner. It is much more efficient if one judge handles all of those cases.”⁸⁴⁹

It was still a burden on courts nonetheless. Former judge Nancy Gertner said: “any time you have large numbers of people who are not represented by counsel it is tremendously burdensome. There were things I did to protect the plaintiffs, but I had to think of them on my own.”⁸⁵⁰

Courts were slowly putting a stop to these large-scale pre-settlement campaigns, by looking at the economics. According to Gill Sperlein, they therefore ordered that cases could not be joined. “Litigation becomes economically unfeasible for right holders, unless they use litigation as a deterrent. RIAA did that and could because they spread money around a large industry.”⁸⁵¹ Sperlein said that the filing fee is 400 dollars. “It’s a lot of money. And a lot of these IP addresses are not fruitful – people move – or the case is not morally attractive -.”⁸⁵²

And actually proceeding to court instead of going for settlements was expensive too. Sperlein said that as a defense “everybody says they have an open wireless now. But nobody does. And you can prove it, but it would be too expensive.”⁸⁵³

According to Sperlein the best way to stop this practice was economically: by ordering that cases cannot be joined. Doing so would make litigation economically unfeasible for right holders.⁸⁵⁴ This mattered, because success of this procedure is measured by identification of large numbers of does.⁸⁵⁵

Corynne McSherry said these high prices were “their problem”. “The Rules of civil procedure apply to everyone. Litigation is expensive. If you don’t like it, then you should consider answers in other places like your business model.”⁸⁵⁶

⁸⁴⁷ Shyamkrishna Balganesch, *The Uneasy Case Against Copyright Trolls*, 86 S. CAL. L. REV. 723, 739–40 (2013). P.728-729.

⁸⁴⁸ Shyamkrishna Balganesch, *The Uneasy Case Against Copyright Trolls*, 86 S. CAL. L. REV. 723, 739–40 (2013). P.739-740.

⁸⁴⁹ Otis D. Wright, II (District Judge) interviewed by author, September 2013.

⁸⁵⁰ Nancy Gertner (Professor at Harvard Law School) interviewed by author, October 2013.

⁸⁵¹ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁸⁵² Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁸⁵³ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁸⁵⁴ Gill Sperlein (Lawyer) interviewed by author, September 2013.

⁸⁵⁵ DeBriyn, “Shedding Light on Copyright Trolls,” P.96.

⁸⁵⁶ Corynne McSherry (Intellectual Property Director Electronic Frontier Foundation) interviewed by author, September 2013.

5.7 Conclusion

The case showed how rights holders and law firms targeted allegedly infringing users directly. They first collected IP addresses by participating in the P2P network. In order to identify users connected to those IP addresses, they needed help of ISPs. They either asked ISPs to forward their claims or they got a subpoena from a local judge to force ISPs to give out contact details using the rules of early discovery. They used the rules of joinder to group multiple defendants at once. While the RIAA originally sued users leading to few court cases, law firms aimed for settlements directly.

For the evaluation of performance on the variables, the case has been divided into 2 subcases, which were all different potential phases in the procedure (settlement letter and court case).

Although there were only few actual court cases for the RIAA, the law firms have targeted hundreds of thousands of people with settlement requests. The severity of the court cases ranged into the hundreds of thousands of dollars, while settlement requests ranged between the hundreds and thousands of dollars.

The safeguards in the court cases were as they would be in a regular trial, but settlement requests offered less. Some ISPs forwarded the settlement requests to users, without the interference of a judge, while in other cases the judge was involved only in the process of early discovery and joinder. That remained the only involvement, unless the procedure led to a trial. Settlement requests were however designed in a way to discourage court cases. The burden of proof therefore rested heavily on the accused. Although users were sent a notice, this was already the settlement request. Technically there was a right to be heard or appeal, but that was discouraged because it could lead to high costs. Accused parties had unequal access to defenses. There was little transparency and the punishments were not proportional.

There was little to no impact on file sharing. The case also showed that targeting end users on a large scale was expensive, but that grouping defendants and aiming for settlements saved costs. Some have called this strategy economically problematic. These outcomes will be highlighted again in the conclusion and compared with the outcomes of the other cases.

6. TARGETING END USERS DIRECTLY IN THE UK IN 2006-2011

6.1 Introduction

In the UK, two law firms launched similar strategies to target end users directly. They collected infringing IP addresses and would take this information to court to seek Norwich Pharmacal Orders, to identify infringers at the ISP level. After identification they would send out letters to allegedly infringing users connected to those IP addresses. Two lawyers from Davenport Lyons (Miller and Gore) and one lawyer from law firm ACS:Law (Crossley) were later punished and suspended by the Solicitors Disciplinary Tribunal for applying this strategy. This strategy relied on settlement requests and in some cases on an eventual trial. It is therefore divided into two subcases which are different potential phases in the procedure (settlement letter and court case).

The first section will detail the history of this procedure whilst also providing the relevant legal background. It will then go into the procedure in practice. For that, I relied on two cases before the Solicitors Disciplinary Tribunal, against (1) Miller & Gore, and (2) Crossley. They have been the most famous cases of this type of mass copyright enforcement, and because their cases went to the Solicitors Disciplinary Tribunal, there are detailed descriptions of how they went to work. In fact, so detailed, that when I approached consumer organization 'Which?' and when I approached the Solicitors Regulation Authority, both referred me to the disciplinary tribunal, who sent me the court cases. For additional questions on the cases I contacted the disciplinary tribunal again. Although I am aware that after these two law firms engaged in this type of mass copyright enforcement the practice resurfaced when Golden Eye and others started sending letters to other users in 2012, those latter cases only feature in this study to a minor extent.

This information resurfaces in the section on the variables. Additional information was found in case law and through the book by Andrew Murray, on Information Technology Law. In addition to this, I included news articles, academic research and reports by NGOs on the practice of mass litigation. The reason I use the term 'speculative invoicing' instead of targeting end users directly is that the law firms involved have been fined for this procedure, as they employed contingency fees and targeted end users as a business model. Although the term is not neutral, other academics like Andrew Murray use it as well, and I think it describes the practice in this case more accurately.

The information was collected from January 2012 until mid 2013.

6.2 Legal background

In the UK, rights holders have generally shied away from large-scale enforcement aimed at individual users, with the exception of some that engaged in what Murray refers to as 'volume litigation.'⁸⁵⁷ Later, he started calling it 'speculative invoicing.'⁸⁵⁸ Although this term is not neutral, it does adequately describe the procedure. Between 2006 and 2011, these law firms pursued thousands of file sharers allegedly acting in breach of the Copyright, Designs, and Patents Act 1988, until they were ordered to stop their work by the Solicitors

⁸⁵⁷ Andrew Murray, *Information Technology Law: the Law and Society* (Oxford University Press, 2010).

⁸⁵⁸ Andrew Murray, *Information Technology law: the Law and Society* (Oxford University Press, 2013). P.287.

Disciplinary Tribunal. In case 10619-2010, Miller and Gore, two lawyers (and partners) of the firm Davenport Lyons were found to be breaching the Solicitors' Code of Conduct. In case 10726-2011, Crossley, the main partner and only registered solicitor for the firm ACS:Law was also found to be breaching the Solicitor's Code of Conduct.

The lawyers used monitoring firms like the Swiss anti-piracy company Logistep to spot infringers. They tracked down eMule or eDonkey users they claimed were sharing their content, and gathered information on them. With this information, they requested a court order to get ISPs to give up the names and addresses connected to those IP addresses. In each English case Davenport Lyons obtained a 'Norwich Pharmacal Order,' which relates to the obtaining of information regarding infringements from parties who may not themselves be involved in the infringement, i.e. the ISP. In the original Norwich Pharmacal Co and Others v Customs & Excise Commissioners case in 1973/74, it was ruled that a party who became even innocently involved in someone else's wrong doing, was under obligation to provide the injured party with information to identify the wrong doer.⁸⁵⁹ After the contact details were obtained, those people were then sent 'pre settlement letters' in which users were asked to pay a small settlement fee to avoid trial.⁸⁶⁰

During the volume litigation process in the UK, a lawyer named Elizabeth Martin, who represented Logistep, was banned from practicing law in France for six months by the Paris Bar council for sending out similar letters, while Logistep itself got into trouble in Italy and Switzerland.⁸⁶¹

One of the clients of Davenport Lyons, Zuxxez entertainment, a video game developer, already had used a similar strategy in Germany in 2005, when they filed thousands of claims against Germans who allegedly shared one of their video games on the eDonkey network. After some time, ISPs stopped responding to those claims.

At Davenport Lyons, two lawyers operated the process. Miller was responsible for the relationship with clients, while Gore was the litigation partner.⁸⁶²

In 2005, Miller presented a paper to the Entertainment and Leisure Software Publishers Association (ELSPA) on tackling online piracy, in which he advocated a procedure of volume litigation. They would obtain Norwich Pharmacal Orders to get names and addresses of a person whose IP address appeared to have been used for illegal file sharing. He suggested that instead of or before taking those people to trial, letters seeking damages should be sent to the infringers before in which they would threaten an injunction.

The paper mentioned the economies of scale that could be achieved, calling it a "cost effective method" because "most cases settle early on", and "we do not believe a full trial will ever be necessary." They also advocated only pursuing persistent infringers (up- or downloading five or more computer games).⁸⁶³ These practices initially appeared attractive to copyright holders. They were sought by Topware Interactive, Codemasters, Reality Pump, Techland, and Atari.⁸⁶⁴

⁸⁵⁹ Enigmax, "You're Caught Downloading "Dream Pinball", Settle Now or Go Broke," *Torrentfreak* (March 31, 2007), <http://torrentfreak.com/youre-caught-downloading-dream-pinball-settle-now-or-go-broke/>.

⁸⁶⁰ Enigmax, "You're caught downloading "Dream Pinball," settle now or go broke," *TorrentFreak* (March 31, 2007).

⁸⁶¹ Mike Masnick, "File Sharing Pre-Settlement Letters In Europe Get Lawyer Banned For Six Months," *Techdirt* (April 7, 2008), <http://www.techdirt.com/articles/20080407/002030770.shtml>.

⁸⁶² Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶19.

⁸⁶³ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶12 – 15.

⁸⁶⁴ Andrew Murray, *Information Technology law: the Law and Society* (Oxford University Press, 2013). P. 188.

Miller approached Logistep that had developed a software package to identify IP addresses allegedly sharing copyright-protected content.⁸⁶⁵ After that, he attended the Leipzig Game show in the summer of 2006 to attract potential clients.⁸⁶⁶

Between 2006 and 5 May 2009, Davenport Lyons acted for six clients (referred to as Tw, Cm, RP, T, A, and Dp in the case before the Solicitors Disciplinary Tribunal.)⁸⁶⁷ All clients represented computer games. A and Dp were German, and Dp had acquired some rights owners that also represented films, music and pornography. Therefore the number of letters sent on behalf of Dp is much higher. The British Phonographic Industry (BPI) was only involved in 33 claims.⁸⁶⁸

Miller had approached those clients to ask them if they wanted to retrieve funds and if they wanted to share those varying percentages with Logistep and the firm. For example, he used a report, prepared by Logistep, to show German client A that their games were downloaded frequently in the UK. Davenport represented A for three of their games.⁸⁶⁹

In the agreements, recoveries would be divided among Davenport Lyons, Logistep or another monitoring agency, and the rights owners (usually split around 33% each), plus some money for expenses. The disciplinary trial case described that they knew they were going to do this as a large-scale operation involving thousands of members of the public.⁸⁷⁰

But then bad publicity started to influence the process causing clients to drop out. It started when it became clear that allegations were made on the basis of IP addresses alone. Also, some people sought out the media. Ken and Gill Murdoch, an elderly couple, had received a letter on behalf of Atari but had never played a video game before. They contacted consumer organization 'Which?'. Publicity got really bad, when Davenport Lyons also started representing pornography companies, and sent letters to "respectable" elderly citizens.⁸⁷¹ For example, a seventy year old woman was accused of sharing "Army Fuckers", a gay pornography involving "muscled soldier men in Czechoslovakia."⁸⁷²

A number of recipients had sought out legal advice. At one point a firm represented around 250 alleged infringers.⁸⁷³ The settlement letters led to some uproar, especially when complaints were made to consumer magazine "Which?", and after the involvement of the BBC in the programme Watchdog (on Monday December 8, 2008).⁸⁷⁴ Eventually, some clients, like Cm.⁸⁷⁵ and A.⁸⁷⁶, withdrew from the mass litigation campaign after negative publicity.

Complaints were first filed at Legal Complaints Service (July 29 2008), but they said the actions undertaken by Davenport Lyons were legal. Then, complainants went to the legal services ombudsman,⁸⁷⁷ who said it should be decided by courts.

⁸⁶⁵ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶16.

⁸⁶⁶ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶17.

⁸⁶⁷ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶18.

⁸⁶⁸ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶124.

⁸⁶⁹ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶28.

⁸⁷⁰ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶124.

⁸⁷¹ Andrew Murray, *Information Technology law: the Law and Society* (Oxford University Press, 2013). P.188.

⁸⁷² Christopher Williams, "Filesharing ambulance chasers get into the gay smut racket," *The Register* (November 19, 2008), http://www.theregister.co.uk/2008/11/19/davenport_lyons_filesharing/.

⁸⁷³ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶64.

⁸⁷⁴ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶21.

⁸⁷⁵ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶42-43.

⁸⁷⁶ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶53.

⁸⁷⁷ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶57.

When the case eventually reached the Solicitors Disciplinary Tribunal, the Tribunal ruled that Miller and Gore allowed their independence to be compromised, because they had a new system developed in which they had a clear financial interest in the end result, making the scheme pay was an important element of it, they did not verify the validity of the claim (instead they had their own interpretation of the law), were not concerned about loss of reputation of clients, but persisted.⁸⁷⁸ They also did not act in the best interest of their clients (as it was all about the interest of the firm).⁸⁷⁹ A more serious violation was that they acted in a way to decrease trust in legal profession.⁸⁸⁰ They also entered into arrangements to receive contingency fees where they should not have,⁸⁸¹ had conflicts of interest with the interest of their clients,⁸⁸² and abused their position to take advantage of other people.⁸⁸³

As a result, Miller and Gore were suspended for three months, and both were ordered to pay a fine of 20,000 pounds.⁸⁸⁴ Meanwhile, Crossley faced the same allegations in front of the Solicitors disciplinary tribunal. Between February 2006 and February 2011 he practiced on his own account under the name of ACS:Law.⁸⁸⁵ In fact, ACS:Law signed a deal with Davenport Lyons at the start of 2009, transferring some of the work and employees to ACS: Law.⁸⁸⁶ According to Gore, they transferred the work because they: “were losing money in carrying out this work and particularly in the current economic climate it was not financially viable.”⁸⁸⁷

In the agreement between both law firms, they transferred all the remaining work, and ACS:Law would continue working on those cases. All the clients of Miller and Gore were transferred to ACS:Law.⁸⁸⁸

Recoveries would be distributed among the client, the firm and the monitoring firm (around 33% each, but at times, for example in the case of T, only 25% for the client.⁸⁸⁹ Company MCAT owned and operated by existing client of the respondent named LB. MCAT signed up owners, MCAT would pursue infringers on their behalf.⁸⁹⁰ They are copyright monitoring companies licensed by rights holders to pursue file sharers.

In October of 2010, ISPs like BT and Sky started refusing to hand over details. Not only did an Internet attack on ACS: Law cause personal details of alleged file sharers to leak online, but the ISPs also feared that people would not actually be sued.⁸⁹¹

Few cases actually did make it to court. Some of Davenport Lyons’ cases had made court, but only through default judgements, which excluded a hearing or notice.⁸⁹² None of the ACS:Law cases went through a proper hearing that included defendants. In the only case

⁸⁷⁸ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶178.

⁸⁷⁹ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶182.

⁸⁸⁰ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶187-188.

⁸⁸¹ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶194.

⁸⁸² Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶198.

⁸⁸³ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶209.

⁸⁸⁴ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶231-232.

⁸⁸⁵ Solicitors Disciplinary Tribunal, Case No. 10726-2011, Crossley. ¶7.

⁸⁸⁶ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶65.

⁸⁸⁷ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶66.

⁸⁸⁸ Solicitors Disciplinary Tribunal, Case No. 10726-2011, Crossley. ¶15.

⁸⁸⁹ Solicitors Disciplinary Tribunal, Case No. 10726-2011, Crossley. ¶38.

⁸⁹⁰ Solicitors Disciplinary Tribunal, Case No. 10726-2011, Crossley. ¶44.

⁸⁹¹ Josh Halliday, “Illegal filesharing: is this the end of 'speculative invoicing'?” *The Guardian* (January 27, 2011), <http://www.theguardian.com/technology/blog/2011/jan/27/illegal-file-sharing-acslaw>.

⁸⁹² *Media CAT Ltd v Adams & Ors* [2011] EWPC 6 (08 February 2011). ¶53 and 54.

to make it to court Media CAT, a company assisted by Crossley, commenced 27 cases before the Patents County Court for copyright infringement.

They applied for default verdicts using a 'request for judgement,' which did not include notice, and in this case did not include a hearing. These default judgements were eventually denied.⁸⁹³ In that case, Judge Birss QC was damning of the process, as the judge found that the Norwich Pharmacal order was not the place to test novel legal claims about copyright infringement, that the claims far exceeded any damages likely to have accrued. Even before the case would reach the solicitors disciplinary tribunal, this judge of the patent court condemned Crossley, saying that he breached the solicitors code of conduct, and that he "brought the legal profession into disrepute."⁸⁹⁴ The judge also said: "one odd thing is that if tens of thousands of letters have been sent threatening legal action, where are all the legal actions?"⁸⁹⁵

The main cause for breaching the code was that Crossley asked for contingency fees for prosecuting (conditional fees that granted him a percentage of the winnings if the case was won). A year later, Crossley would face the solicitors disciplinary tribunal.⁸⁹⁶

Crossley would be suspended for the same reasons as Miller and Gore. He had been more aggressive in his pursuit, and would be suspended for two years, and ordered to pay 76,326.55 pounds.⁸⁹⁷

In March 2012 the practice resurfaced. Instead of using a copyright monitoring company, rights holders themselves chased infringers. However, ISPs initially refused. It led to court case Golden Eye (international) Ltd v Telefónica UK Ltd [2012] EWHC. 723 (Ch), which has numerous similarities to the Media cat case cited earlier.⁸⁹⁸

Golden Eye sought 9.124 personal details under order to be served on Telefónica, operator of O2 broadband network. They wanted to demand payment of 700 pounds for their own work and under agreement for 12 other claimants who had contractually agreed for Golden Eye to represent them in the case in return for a proportion of any damages received. This mainly concerned adult content produced by Golden Eye and Ben Dover Productions that was shared on BitTorrent networks.⁸⁹⁹ At first hearing judge Arnold J examined the relationship between Golden Eye and their legal representatives and other claimants. The judge determined that case was distinguishable from Media Cat and awarded the order to 'Golden Eye' and 'Ben Dover.' The judge refused to issue the order for the other 12 claimants. He said there was no fair balance because other claimants surrendered control of litigation to Golden Eye in exchange for 75% of revenues. To the judge it seemed like a court sanctioning the sale of privacy and data protection rights to the highest bidder.

The judge also criticized the amount of money requested. Golden Eye claimed it had to be set so high because some people would not pay up. To the judge this suggested the cases were not about recovering damages, but about maximizing revenue.

Golden Eye appealed this decision, and although the Open Rights Group intervened, in December 2012 a Court of Appeal reversed it: judge Patten LJ said that revenue distribution did not jeopardize or undermine the proper administration of justice. These

⁸⁹³ Media CAT Ltd v Adams & Ors [2011] EWPC 6 (08 February 2011). ¶123.

⁸⁹⁴ Media CAT Ltd v Adams & Ors [2011] EWPC 6 (08 February 2011).

⁸⁹⁵ Media CAT Ltd v Adams & Ors [2011] EWPC 6 (08 February 2011). ¶122.

⁸⁹⁶ Josh Halliday, "ACS:Law solicitor 'breached code with files sharing claims'," *The Guardian* (April 19, 2011), <http://www.theguardian.com/technology/2011/apr/19/acs-law-solicitor-files-sharing-claims>.

⁸⁹⁷ Solicitors Disciplinary Tribunal, Case No. 10726-2011, Crossley. ¶109.

⁸⁹⁸ Andrew Murray, *Information Technology law: the Law and Society* (Oxford University Press, 2010). P.290.

⁸⁹⁹ Andrew Murray, *Information Technology law: the Law and Society* (Oxford University Press, 2010). P.290.

cases were, according to the court of appeals, not “simply a money-making exercise designed to take advantage of the vulnerability of the subscribers rather than a genuine attempt to protect the rights of the other claimants,” therefore, the court said, “I can see no justification for refusing relief based on a disapproval of those arrangements. Indeed it is difficult to articulate what that disapproval can be based on.” Andrew Murray said this last verdict left the door open for “speculative invoicing.”⁹⁰⁰ Golden Eye has started sending out more letters, through their solicitor Wagner. Here too, people claimed to be innocent and stepped forward.⁹⁰¹

Another result is that some scams started using the same tactics. Although they represented no rights holders, they sent letters demanding payments and based themselves on the new Digital Economy Act.⁹⁰²

6.3 The procedure in practice

The law firms targeted infringement carried out over eMule (or eDonkey) and BitTorrent.⁹⁰³ To detect infringement, they used forensic anti-piracy agencies like Swiss company Logistep or NG3 Systems Ltd who conducted an exercise of “monitoring the unauthorised exploitation of the work on the P2P network”⁹⁰⁴

These agencies would gather information and evidence on infringers, usually consisting of the content uploaded, the IP address of the alleged infringer, the user’s eMule/eDonkey user ID, and a timestamp. Davenport Lyons never admitted to using Logistep in these cases, but the Internet Piracy Portal stated that they were partners.⁹⁰⁵ The Solicitors Disciplinary Tribunal case mentions that Davenport Lyons used ‘Ls’ (Switzerland) for five clients, and Dr (Germany) for Dp.⁹⁰⁶

Forensic agencies like Logistep accessed P2P sites and pretended to be users that wished to access copyright protected material. They made connections with individuals offering data. Then they registered the download and compared it to the original material to see whether or not it was copyrighted.⁹⁰⁷ ACS: Law used four different companies for monitoring IP, depending on the clients. Those companies would also act as peers on P2P sites, used their software to make connections with individuals and then compared it with original material to see if it was copyrighted.⁹⁰⁸

The law firms would take this information to court to seek Norwich Pharmacal Orders, to identify infringers at the ISP level. ISPs did not object but sought recovery of their

⁹⁰⁰ Andrew Murray, *Information Technology law: the Law and Society* (Oxford University Press, 2010). P.291.

⁹⁰¹ Enigmax, “Golden Eye Hit UK With Piracy Letters, First Innocent Step Forward,” *Torrentfreak* (February 1, 2013), <http://torrentfreak.com/golden-eye-hit-uk-with-piracy-letters-first-innocents-step-forward-130201/>.

⁹⁰² Mark Jackson, “Fake UK ISP Internet Piracy Warning Letters Expose Obvious DEAct Flaw,” *ISPReview* (July 2, 2012), <http://www.ispreview.co.uk/index.php/2012/07/fake-uk-isp-Internet-piracy-warning-letters-expose-obvious-deact-flaw.html?>

⁹⁰³ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶123.

⁹⁰⁴ Media CAT Ltd v Adams & Ors [2011] EWPC 6 (08 February 2011). ¶16.

⁹⁰⁵ Enigmax, “You’re Caught Downloading “Dream Pinball”, Settle Now or Go Broke,” *Torrentfreak* (March 31, 2007), <http://torrentfreak.com/youre-caught-downloading-dream-pinball-settle-now-or-go-broke/>.

⁹⁰⁶ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶126-27.

⁹⁰⁷ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶126-27.

⁹⁰⁸ Solicitors Disciplinary Tribunal, Case No. 10726-2011, Crossley. ¶17.

legal costs which was generally agreed to by the firm on behalf of their clients.⁹⁰⁹ Also, ISPs would sometimes manually check requests, because of small error rates.⁹¹⁰

Having identified the users allegedly infringing, the law firms would send out letters to those users. None of the letters were actually addressed to an individual, but general in commencement.⁹¹¹ These letters would contain:

- “a letter of claim, demanding that Mrs M pay compensation of £500 plus the ISPs costs of £25;
- a statement report detailing, amongst other things, the name of the ISP and the IP address;
- a copy of a letter to the ISP requesting disclosure of the details of the subscriber to whom a specific IP address related;
- a copy of the relevant section of a spreadsheet sent to the ISP in relation to the alleged infringer’s address;
- a document requiring the alleged infringer to give an undertaking not to upload, download or otherwise make available the client’s game, to delete any copies of the game from the alleged infringer’s computer and to pay £525 to the Firm by way of damages and costs (or a variant on such a sum);
- a payment form;
- a credit/debit card transaction form;
- a document entitled “Note on Evidence”;
- a copy of the Norwich Pharmacal order obtained on behalf of the client;
- a document entitled “Code of Practice for Pre-Action Conduct in Intellectual Property Disputes”.⁹¹²

Legal charges would for example be limited to: “Based on the evidence supplied to us, your Internet connection has been used to make the Work available on peer to peer network(s), either through your own acts or by permitting others to do so, for third parties on the same network(s) to download. Such activity constitutes a breach of the provisions of sections 16(1)(d) and 20 of the Copyright, Designs & Patents Act 1998 (sic) (“the Act”). Where our client’s Work has been copied on to the hard drive of the personal (or office) computer (“PC”) used to make the Work available on P2P network, there will also have been a breach of the provisions of sections 16(1)(a) and 17 of the Act.”⁹¹³

According to Torrentfreak, notes on evidence would for example say: “Our client has retained forensic computer analysts to search for and identify Internet addresses from which their games are being made available on so called “peer to peer” (P2P) Internet sites for the purposes of making them available for download by third parties without our client's consent or license.

Our client is in possession of compelling evidence that on the following date and time 15.09.2006 12:15:22 [made up date/time for illustration purposes] (captured in the German time zone), the Game was made available from the Internet protocol (or IP) address XXX.XXX.XXX.XX specifically for the purpose of downloading by third parties. Pursuant to a High Court Order, the Internet service provider XXXXXXXXXXXXXXX identified you as the

⁹⁰⁹ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶129.

⁹¹⁰ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶168.

⁹¹¹ Enigmax, “You’re Caught Downloading “Dream Pinball”, Settle Now or Go Broke,” *Torrentfreak* (March 31, 2007), <http://torrentfreak.com/youre-caught-downloading-dream-pinball-settle-now-or-go-broke/>.

⁹¹² Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶130.

⁹¹³ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶167.

subscriber associated with that IP address at the time in question."⁹¹⁴ The letters referred by Torrentfreak had been taken online, so I could not verify their authenticity.

The letters sent by ACS: Law were similar to the Davenport Lyons ones, and only subject to stylistic changes, like removing reference to administration fees when infringers were offered to pay by installments.⁹¹⁵

Envelopes on adult content letters were marked "strictly private and confidential" and the heading of the material was not placed in the heading of the letter, after advice taken from a defamation partner.⁹¹⁶

The letters were intended to scare people into quick settlements. This is why the price needed to be low. Miller suggested 500 pounds, because "it needs to be like an "expensive parking ticket" to maximize recovery and at the same time, be a sufficient sting to warn (most of) them not to do it again..." If recoveries were too low, they wanted to start suing.⁹¹⁷

In those letters, Davenport Lyons asked for 500 pounds in compensation, plus the ISP administration costs of 25 pounds. The wording of the letters suggested that the amounts would be much higher in court.⁹¹⁸

6.4 Scale, severity and procedural safeguards

Scale

Davenport Lyons sent out 6.113 letters to individuals.⁹¹⁹ However, they intended to send out at least 13.745 letters. Miller had said that 50% of all letters went unanswered, and were placed in a pool to consider litigation action.⁹²⁰ Although they claimed to have a recovery rate of 50%, that amount seems to be much lower, looking at the figures provided per client in the tribunal case, which seems to lie between 19,9% (for client 'T')⁹²¹ and 38% (for client 'Tw').⁹²² The costs were often much higher, than the recovery.⁹²³

In some cases, people disputed the claims. Davenport continued in all but one case (an 11 year old autistic grandson).⁹²⁴ The idea generally was to start suing afterwards, but that stage was not sufficiently reached.⁹²⁵ Litigation had proceeded in only 5 cases, and at 6 May 2009 they were considering a further 6.⁹²⁶ Legal proceedings on behalf of client Tw against 5 infringers led to summary judgments (3 uncontested) and two challenged after summary judgment.⁹²⁷

⁹¹⁴ Enigmax, "You're Caught Downloading "Dream Pinball", Settle Now or Go Broke," *Torrentfreak* (March 31, 2007), <http://torrentfreak.com/youre-caught-downloading-dream-pinball-settle-now-or-go-broke/>.

⁹¹⁵ Solicitors Disciplinary Tribunal, Case No. 10726-2011, Crossley. ¶122.

⁹¹⁶ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶183.

⁹¹⁷ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶141.

⁹¹⁸ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶199.

⁹¹⁹ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶119.

⁹²⁰ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶183.

⁹²¹ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶149.

⁹²² Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶144.

⁹²³ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶144.

⁹²⁴ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶135.

⁹²⁵ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶141.

⁹²⁶ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶161.

⁹²⁷ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶163.

Later on, 30 cases were discontinued. In 9 cases because of infringers representations and 27 of those 30 eventually received a written apology. Most of the discontinuing happened because of two ISPs who had had technical issues about IP addresses and suggested a lack of integrity with the data.⁹²⁸

Because the case was filed the firm did not make another intended 7,000 claims. They were paid 357,000 pounds as a result of 1,561 claims, and 4,000 claims were still outstanding because they were transferred to ACS:Law.⁹²⁹

ACS: Law provided that a total of 20,323 letters were sent out, and that out of that "total number of claims there were 1,457 alleged infringers who had agreed to pay costs or damages in full and 518 infringers who had agreed to pay costs and/or damages in part."⁹³⁰ That is a recovery rate of 10%.

ACS: Law aimed to proceed to litigation, but judgements in the case were denied by the Patent court.⁹³¹

Severity

Damages were calculated arbitrarily.⁹³² Davenport Lyons asked for 300 pounds in damages, but this quickly rose to 500 pounds and 600 pounds.⁹³³ Usually, the firm asked for an additional 25 as ISP administration costs.⁹³⁴ The total amount could be raised to 1,000 pounds if people did not pay immediately.⁹³⁵

ACS: Law asked for different amounts, depending on its client. Damages claims were usually higher for movies and games (between 400⁹³⁶ and 700⁹³⁷ pounds) than for music (between 350⁹³⁸ and 500⁹³⁹ pounds).

Few cases lead to an actually judicial verdict of damages. One of the major cases reached a court verdict of 16,000 pounds (6,000 pounds for damages, and 10,000 pounds in legal costs).⁹⁴⁰ In other cases, four suspected uploaders were ordered to pay 2,750 pounds. These cases were all default judgements as the defendants did not show up in court.⁹⁴¹

⁹²⁸ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶161.

⁹²⁹ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶124.

⁹³⁰ Solicitors Disciplinary Tribunal, Case No. 10726-2011, Crossley. ¶150.

⁹³¹ Paul Revoir, "Up to 25,000 British illegal downloaders sued for £300 as games developers turn to courts, *Daily Mail* (21 August 2008), <http://www.dailymail.co.uk/news/article-1046607/Up-25-000-British-illegal-downloaders-sued-300-games-developers-turn-courts.html>

⁹³² Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶111.

⁹³³ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶184.

⁹³⁴ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶168.

⁹³⁵ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶190.

⁹³⁶ Solicitors Disciplinary Tribunal, Case No. 10726-2011, Crossley. ¶148.

⁹³⁷ Solicitors Disciplinary Tribunal, Case No. 10726-2011, Crossley. ¶142.

⁹³⁸ Solicitors Disciplinary Tribunal, Case No. 10726-2011, Crossley. ¶148.

⁹³⁹ Solicitors Disciplinary Tribunal, Case No. 10726-2011, Crossley. ¶129.

⁹⁴⁰ Paul Revoir, "Up to 25,000 British illegal downloaders sued for £300 as games developers turn to courts, *Daily Mail* (21 August 2008), <http://www.dailymail.co.uk/news/article-1046607/Up-25-000-British-illegal-downloaders-sued-300-games-developers-turn-courts.html>

⁹⁴¹ "Game file-sharers told to pay £2,750," *Metro* (1 July 2008), <http://metro.co.uk/2008/07/01/game-file-sharers-told-to-pay-2-750-230423/>

Safeguards

Privacy

Whether or not this enforcement strategy interfered with privacy rights, depended on whether personal data was processed. This usually happens when infringement is found, and when enforcing parties have access to personal data.

Infringement is found at the top layer, by participating in the P2P network. Forensic agents identified IP addresses that are infringing. By participating, they would in some cases also have access to the catalogue of a user that is sharing content through P2P networks. However, by participating in the network, the user accepted this.

After taking the IP addresses to the court, the lawyers obtained a Norwich Pharmacal Order which would enable them to force ISPs to identify the users matching those IP addresses, and share those contacts with the law firms.

These personal data should be stored in a privacy respecting way. Hackers exposed all the personal details stored at ACS:Law after some attacks.⁹⁴² At the tribunal, the question arose as to whether the firm failed to take the appropriate technical and organizational measures against the accidental loss of personal data. If not for the firms' limited means they would have received a penalty of 200,000 pounds.⁹⁴³ On the other hand, they appealed this. They were the victim of a DDOS cyber attack by a large group and that no one could have responded well enough according to analysis.⁹⁴⁴

Impartial, competent and independent judge

These cases have been condemned for their lack of judicial review. The only review that happened was in first instance done by the law firms and rights holders that had a financial interest in a ruling in their favor.

Afterwards, the courts reviewed the applications for Norwich Pharmacal orders, but this was not the same type of review one would get in trial. In one of the few cases to actually make it to trial,⁹⁴⁵ Mr Justice Birss QC, patents county court judge, commented on an application for the discontinuance of 27 claims on the Norwich Pharmacal process:⁹⁴⁶ “.. A Norwich Pharmacal application is not and cannot be the place in which to try the cause of action.”⁹⁴⁷ The judge commented that a person had no way to defend themselves.⁹⁴⁸

The judge also said: “It is remarkable, therefore, that the underlying cause of action on which all these cases are based has not been tested at trial.”⁹⁴⁹ “Robust correspondence between lawyers and sophisticated parties is part of the legal process. However, letters which deal with issues of the complexity of the ones arising in this case need to be considered very carefully if they are addressed to ordinary members of the public.”⁹⁵⁰

⁹⁴² Josh Halliday, “Law firm could face £500,000 fine over data breach,” *The Guardian* (September 28, 2010), <http://www.theguardian.com/media/2010/sep/28/filesharing-acslaw>.

⁹⁴³ Solicitors Disciplinary Tribunal, Case No. 10726-2011, Crossley. ¶181-83.

⁹⁴⁴ Solicitors Disciplinary Tribunal, Case No. 10726-2011, Crossley. ¶184-88.

⁹⁴⁵ Media CAT Ltd v Adams & Ors [2011] EWPC 6 (08 February 2011).

⁹⁴⁶ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶163.

⁹⁴⁷ Media CAT Ltd v Adams & Ors [2011] EWPC 6 (08 February 2011). ¶14.

⁹⁴⁸ Media CAT Ltd v Adams & Ors [2011] EWPC 6 (08 February 2011). ¶14.

⁹⁴⁹ Media CAT Ltd v Adams & Ors [2011] EWPC 6 (08 February 2011). ¶15.

⁹⁵⁰ Media CAT Ltd v Adams & Ors [2011] EWPC 6 (08 February 2011). ¶17.

The judge himself damned the lack of judicial oversight. The only oversight in the process was when the judge determined whether a Norwich Pharmacal order should be granted. That required different standards of evidence, and did not go into the specifics of copyright. The test carried out in the granting the order was completely different that the test applied by a court to determine whether infringement had taken place.⁹⁵¹

No one would test legal theories applied, and no one could judge the quality of the monitoring software.⁹⁵²

Very few cases reached court, in ‘request for judgements.’ I had no reason to doubt the impartiality, competence or independence of those judges.

Presumption of innocence

The distribution of evidence was heavily tilted in favor of the law firms, not only procedurally, but also psychologically.

The letters were intended to scare people into quick settlements. This is why the price needed to be low. Miller suggested 500 pounds, because “it needs to be like an “expensive parking ticket” to maximize recovery and at the same time, be a sufficient sting to warn (most of) them not to do it again...” If recoveries were too low, they wanted to start suing.⁹⁵³

In those letters, Davenport Lyons asked for 500 pounds in compensation, plus the ISP administration costs of 25 pounds. Then it said: “Damages and costs are likely to be much greater than this sum. It is the sum that our client is prepared to accept (on this occasion only) by way of settlement to help defray its costs if you are prepared to give the undertaking sought and enclosed with this letter and settle the matter early by paying the compensation claimed in this letter.”⁹⁵⁴ The money claimed initially started at 300 pounds for the first letters, but quickly rose to 500 and 600 pounds.⁹⁵⁵

The letters then went on: “If it becomes necessary to issue proceedings against you, our client will be seeking as a minimum from you an interim payment of at least £1,000 and will request the Court to determine the level of total damages and costs which should be awarded against you and which are likely to be much higher.”⁹⁵⁶

In the letters, the law firms attached a document headed “notice on evidence.” It said: “we cannot, due to the number of people we have written to, enter into further detailed correspondence with you regarding our client’s claim. In the event that you wish to dispute the matter, you will have an opportunity of doing so in any court proceedings, if it becomes necessary to issue them against you.”⁹⁵⁷ This part also included a forensic analyst’s evidence which said: “Because of data protection law the ISP will normally require us to apply to the court for a so called Norwich Pharmacal (or disclosure) order. Full evidence of the nature of our claim against you is provided to the Court, which is then invited to order your ISP to disclose your contact details. This enables us to write to you. On the day set out in the Letter of Claim, such an order was made against your ISP, pursuant to which your ISP

⁹⁵¹ Media CAT Ltd v Adams & Ors [2011] EWPC 6 (08 February 2011). ¶16.

⁹⁵² Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶109.

⁹⁵³ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶41.

⁹⁵⁴ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶68.

⁹⁵⁵ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶84.

⁹⁵⁶ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶69.

⁹⁵⁷ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶72.

provided your name and address some weeks later and we were then able to write to you.”⁹⁵⁸

In the case before the disciplinary council, numerous witnesses testify to the intimidating character of the letters.⁹⁵⁹ One witness (who, as it later turned out, was wrongfully accused) stated in court that these letters are “extremely intimidating, especially in a document of the length of the one that we received first off.”⁹⁶⁰ Others said they were “intimidating threatening letters which are causing stress and anxiety.”⁹⁶¹

The granting of the order created the impression that a judge had looked into the matter and people were already guilty. An expert witness said that “it is easy for seasoned lawyers to underestimate the effect a letter of this kind could have on ordinary members of the public. This court’s office has had telephone calls from people in tears having received correspondence from ACS:Law on behalf of MediaCAT. Clearly a recipient of a letter like this needs to take urgent and specialist legal advice. Obviously many people do not and find it very difficult to do so. Some people will be tempted to pay regardless of whether they have actually done anything simply because of the desire to avoid embarrassment and publicity given that the allegation is about pornography.”⁹⁶² Some people thought it was a scam and went to the police.⁹⁶³

The wording of the letters suggested that the amounts would be much higher in court.⁹⁶⁴ This is also what the lawyers expected: Crossley recommended doing a minimum of 5 and up to 100 test cases per annum in proceedings. “This should have the effect of substantially increasing the recovery rate of payment in any phase and is therefore an important part of the process.”⁹⁶⁵ However, some of the “evidence” provided by the lawyers was based on claims not yet proven or decided by courts: the firm claimed there was a positive obligation on the IP holders to secure their Internet connection.⁹⁶⁶

The evidence collected in these cases was questionable: in the cases, expert witnesses discuss that people might have their Wi-Fi hijacked, or use a dynamic IP address.⁹⁶⁷ The IP address identified a premises or a router, not the computer or individual.⁹⁶⁸ To make matters worse, there could also have been an error rate for identification by the ISP. ISPs therefore sometimes manually check.⁹⁶⁹

In the Media CAT case as well, the judge commented that merely accusing someone of being part of a P2P swarm is insufficient evidence of infringement. “Proof that a person owns a photocopier does not prove they have committed acts of copyright infringement.” He quoted an expert witness, saying “trackers were not assiduous in keeping their lists up to date, that IP addresses get reallocated and that an IP address may end up on the tracker list even when a person starts downloading a file onto their home system but then stops immediately. No file is downloaded (or so little of the file as to be irrelevant) but the tracker

⁹⁵⁸ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶173.

⁹⁵⁹ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶93-94.

⁹⁶⁰ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶91.

⁹⁶¹ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶95.

⁹⁶² Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶106.

⁹⁶³ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶104.

⁹⁶⁴ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶99.

⁹⁶⁵ Solicitors Disciplinary Tribunal, Case No. 10726-2011, Crossley. ¶30.

⁹⁶⁶ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶75-81.

⁹⁶⁷ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶108.

⁹⁶⁸ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶113.

⁹⁶⁹ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶168.

system has logged the IP address as a node on the P2P network.” Although this did not mean the assertions of infringement were wrong per se, it did mean those were matters “to explore with proper evidence.”⁹⁷⁰

Notice, right to be heard (prior to conviction), defenses and appeal

Identified subscribers would receive a notice, but it would be vague and pages of legal and technical jargon.

There was hardly room for appeal: the firm’s employees were provided with an information pack around March 2009. “File-sharing Quality Procedures and Control” had a Q and A with things like: “we maintain that an Internet account holder is responsible for his Internet connection and therefore liable for any infringing activity occurring on it. In some cases you will find that the account holder is the parent of a child who has committed the act...”

The notices sent also said that any formal response from an individual had to be made in writing, particularly if they had any defense to put or criticisms to make of the evidence. Responses to users had to be approved by the file sharing partner, or the senior paralegal on a daily basis. These responses had specific answers for specific questions. For example, to the question “What if I don’t pay,” the answer would be given that then they might consider litigation and the damages and costs sought would substantially increase after that point.⁹⁷¹

From the tribunal case, it was clear that they did not properly deal with infringers who responded and tried to defend themselves against the claims and allegations.⁹⁷² Witnesses talked about “bully tactics on the phone.”⁹⁷³

The costs to defend against these claims could rise to 10,000 pounds, according to the House of Lords. This was why they called it legal blackmail.⁹⁷⁴

The few cases that did actually make it to court, were handled through default judgements, without a hearing, when defendants did not respond to the settlement requests.

Transparency

The process was opaque so there was hardly any transparency. In fact, some of the “evidence” provided by the lawyers was based on claims not yet proven or decided by courts: the firm claimed there was a positive obligation on the IP holders to secure their Internet connection.⁹⁷⁵

During the process, apparently (from witness testimony) Davenport said that all the documents sent to people could not be posted on websites or forums because they were copyright protected.⁹⁷⁶ This also made the process less transparent.

⁹⁷⁰ Media CAT Ltd v Adams & Ors [2011] EWPC 6 (08 February 2011). ¶17.

⁹⁷¹ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶62.

⁹⁷² Solicitors Disciplinary Tribunal, Case No. 10726-2011, Crossley. ¶91.24-91.25.

⁹⁷³ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶92.

⁹⁷⁴ Nate Anderson, “The “legal blackmail” business: inside a P2P settlement factory,” *Ars Technica* (September 29, 2010), <http://arstechnica.com/tech-policy/2010/09/amounts-to-blackmail-inside-a-p2p-settlement-letter-factory/>.

⁹⁷⁵ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶75-81

⁹⁷⁶ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶92

Proportionality

To assess proportionality, one has to look at whether sanctions were necessary, suitable and no unreasonable burden on other rights. One could argue that the sanctions were necessary to fight against infringement and to recover missed income, and the sanction would certainly be effective in the sense that it could earn the rights holders back some money. However, the fines were far larger than the money lost on file sharing. In the case revolving around MediaCAT, Mr. Justice Birss QC, the patents county court judge, condemned the process and said that the fine far exceeded the damages suffered by the individuals.⁹⁷⁷ They therefore would fail a proportionality test.

6.5 Impact on infringement levels

It does not look like this system was intended to be a deterrent. The numbers were too small to achieve this, and more likely aimed at revenue for the different partakers.

For example, the tribunal case mentions that the law firm and clients wanted to do a minimum of 5 and up to 100 test cases per annum in proceedings. "This should have the effect of substantially increasing the recovery rate of payment in any phase and is therefore an important part of the process."⁹⁷⁸

Even if it were aimed as a deterrent, it failed. In 2008, three million people in the UK downloaded films illegally. One in three 15-24 year olds used P2P networks.⁹⁷⁹ The IFPI claimed that in 2008, about 95% of all files shared were shared illegally.⁹⁸⁰ That number remained high, as Mediatique said that 25%-28% of people were sharing illegally in 2009.⁹⁸¹

After that, 2012 research by Musicmetrics showed that file sharing remained "mainstream" in the UK.⁹⁸² A report by Ofcom, the UK communications regulator, claimed that in 2012, 16% of all Internet users older than twelve infringed on copyrights online. 35% of them used P2P networks.⁹⁸³ The amount of Internet users was corrected to 18% later.⁹⁸⁴

Another study by Ofcom, between May 2012 and May 2013, revealed that 35% of all movies watched online were pirated. Interestingly enough, only 2% of file sharers made up

⁹⁷⁷ Media CAT Ltd v Adams & Ors [2011] EWPC 6 (08 February 2011).

⁹⁷⁸ Solicitors Disciplinary Tribunal, Case No. 10726-2011, Crossley. ¶130

⁹⁷⁹ International Federation of the Phonographic Industry, *Digital Music Report 2009* (IFPI 2009).

⁹⁸⁰ Rosie Swash, "Online piracy: 95% of music downloads are illegal," *The Guardian* (January 17, 2009), <http://www.theguardian.com/music/2009/jan/17/music-piracy>.

⁹⁸¹ "Online piracy – downloading the facts," *Mediatique* (May 6, 2009), <http://www.mediatique.co.uk/sitedata/Reports/piracy.pdf>.

⁹⁸² Lanre Bakare, "Illegal music filesharing is now mainstream," *The Guardian* (September 18, 2012), <http://www.theguardian.com/commentisfree/2012/sep/18/illegal-music-filesharing-mainstream-ed-sheeran>.

⁹⁸³ Mark Jackson, "Ofcom Claims 16 Percent of UK Internet Users Make Illegal Downloads," *ISPreview* (March 7, 2013), <http://www.ispreview.co.uk/index.php/2013/03/ofcom-study-claims-6-7-million-illegal-downloaders-in-the-uk.html>.

⁹⁸⁴ Mark Sweney, "Music, TV and film piracy rises among UK Internet users," *The Guardian* (May 28, 2013), <http://www.theguardian.com/media/2013/may/28/music-tv-film-piracy-uk-Internet>.

75% of all Internet piracy.⁹⁸⁵ BPI claimed that in 2012, 7 million UK people pirated content, of which 4 million used P2P networks to do so.⁹⁸⁶

6.6 The costs of the system

Costs played a big role in this procedure. They were distributed among rights holders, forensic agencies, law firms, and ISPs. The system was designed to save on costs though, but in the end failed to do so.

As mentioned, the paper advocating this approach, authored by Miller, claimed that economies of scale could be achieved, calling it a “cost effective method” because “most cases settle early on”, and “we do not believe a full trial will ever be necessary.”⁹⁸⁷ They also said that if recoveries would become too low, they wanted to start suing.⁹⁸⁸

Both firms charged set up costs for each client, of around 2500 pounds. ISPs did not object to the system, but sought recovery of their legal costs which was generally agreed to by the firm on behalf of their clients.⁹⁸⁹ One of the ISPs did however dispute the Norwich Pharmacal Order, which meant legal costs rose to 38,684.⁹⁹⁰

Miller and Gore sent out 6.113 letters. In the process they made a total recovery of 370,000 pounds, of which they kept approx. 150,000 pounds for themselves. Meanwhile, the firm wrote off, or appeared to have written off, under 250,000 pounds of chargeable time and entered into money sharing and conditional fee agreements.⁹⁹¹

But the process was not financially viable enough. Internal discussion in the firm led to the idea that “presumably 12,500 letters per year needed to go out for the business to be sustainable, otherwise they could not continue going on.”⁹⁹² In the end they gave up the work for financial reasons. Gore said: “we were losing money in carrying out this work and particularly in the current economic climate it was not financially viable.”⁹⁹³

For ACS Law: “(1) 20,323 letters were sent out; (2) The firm made a total recovery of £936,570.72 out of which the Respondent's firm received £341,078.92 and (3) Out of the total number of claims there were 1457 alleged infringers who had agreed to pay costs or damages in full and 518 infringers who had agreed to pay costs and/or damages in part.”⁹⁹⁴ For ACS: Law the firm made individual calculations for clients. For example, for game owner RP they decided that they needed to collect a minimum of 2500 unique IP addresses to be “effective.”⁹⁹⁵

⁹⁸⁵ “Online Piracy Rate in the UK in 2012-2013,” *Havoscope*, <http://www.havoscope.com/online-piracy-rate-in-the-uk-in-2012-2013/>. Last viewed on: Feb. 13, 2014.

⁹⁸⁶ Mark Jackson, “BPI Claims 7 Million UK People Use Illegal Internet Piracy Services,” *ISPreview* (February 7, 2013), <http://www.ispreview.co.uk/index.php/2013/02/bpi-claims-7-million-uk-people-use-illegal-Internet-piracy-services.html>.

⁹⁸⁷ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶12 - 15

⁹⁸⁸ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶41.

⁹⁸⁹ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶29

⁹⁹⁰ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶34

⁹⁹¹ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶55

⁹⁹² Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶165

⁹⁹³ Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore. ¶66

⁹⁹⁴ Solicitors Disciplinary Tribunal, Case No. 10726-2011, Crossley. ¶50

⁹⁹⁵ Solicitors Disciplinary Tribunal, Case No. 10726-2011, Crossley. ¶29

6.7 Conclusion

The case showed how law firms have targeted users directly in the UK. It consists of two phases (settlement requests and court cases) which have been evaluated as sub cases. The case showed how law firms in the UK collected IP addresses by participating in the P2P network. They then got a Norwich Pharmacal order from a local judge to identify the people connected to the IP addresses with help of the ISP, in order to sue them. The law firms aimed for settlements directly by sending letters asking for payment.

The law firms targeted tens of thousands of people with settlement requests, eventually reaching only less than ten default judgements in court. Regarding severity, the law firms asked for settlements between 300 and 700 pounds. The default judgements by court would lead to sums between 2,750 and 16,000 pounds.

The judge was only involved to grant the Norwich Pharmacal order to get contact details. This involvement was limited. The burden of proof therefore rested heavily on the accused. The letters were phrased in a way to push defendants to settle. Although users were sent a notice, this was already the settlement request. Technically there was a right to be heard or appeal, but that was made very unattractive. Accused parties had unequal access to defenses. Regarding transparency, there was little to none. The punishments were not proportional. In the default judgements, no hearing was held, however this is granted when defendants fail to respond to summons or in this case the settlement request.

There was little to no impact on file sharing. The case also showed that targeting end users on a large scale was expensive, but that grouping defendants and aiming for settlements saved costs. These outcomes will be highlighted again in the conclusion and compared with the outcomes of the other cases.

7. THE HADOPI GRADUATED RESPONSE PROCEDURE (FRANCE) IN 2011-2013

7.1 Introduction

In 2011, the French graduated response procedure became active. This procedure, named HADOPI after the administrative body coordinating it, created a three strikes system for copyright enforcement. Rights holders would hire tech companies to find infringement and report this to the authority. The authority would then send warnings to users connected to the infringing IP addresses. If infringement happened again, a new warning would be sent. After two warnings, the case could be forwarded to the prosecutor for a criminal trial which could result in an internet disconnection. For the evaluation of performance on the variables, the case is divided into 3 subcases, which are different phases in the procedure (warning 1, warning 2, court case).

This chapter will first provide the legal background to this procedure. In this section I also describe the legislative history, because it is relevant to the variables. For this, I used legal sources and academic literature. Some news articles have been used for the legislative history. After that, the chapter describes the procedure in practice. For this, I relied on legal sources, but also on official reports by the authority. I also included the perspective of practitioners. For this case study, I spoke to four respondents familiar with this strategy. I interviewed Sarah Jacquier, legal director of HADOPI, the organization in charge of this procedure. I had an email conversation with the ISP SFR, as ISPs implement this procedure partly. I also had an email conversation with L'Association de lutte contre la piraterie audiovisuelle (ALPA), the French antipiracy authority, and with Zimmermann from the Quadrature du Net, an NGO advocating digital user rights. I tried TMG, a technology company that spots copyright infringement for HADOPI, and the ISP Orange, but they refused to participate.

After that section, the chapter describes the different variables. For this, the sources above have been used, as well as academic studies on this procedure. The information was collected from January 2012 until March 2014. The study does not take into account any reports released in 2014. It does include an empirical study on the effects of the procedure on deterrence from May 2014.

7.2 Legal background

Numerous countries around the globe have implemented a graduated response procedure. Adoption has been controversial because of the heavy penalties at the end of the procedure. Users that infringe on copyrights may have their Internet access suspended. In Europe, the French took the lead in campaigning for the graduated response, with then President Nicolas Sarkozy calling it a crusade to “civilize” the Internet.⁹⁹⁶ In 2004, a report by the French High Council of Literary and Artistic Property recommended a system that would require

⁹⁹⁶ See: Milton U. Müller, “Activists Fear Sarkozy's Efforts to Tame Web,” *Spiegel Online International* (May 24, 2011), <http://www.spiegel.de/international/Europe/0,1518,764305,00.html>, through: Bridy, “Graduated Response American Style,” P.8

broadband providers to send warnings to users suspected of copyright infringement, which would be followed by a fine if the infringement continued.⁹⁹⁷

The new graduated response is in part the result of lobbying, in response to the European commission when consultation took place for the telecoms package in 2008.⁹⁹⁸ The MPAA for example asked the commission to encourage cooperation during the review of the telecoms package.⁹⁹⁹

In 2007, a commission created by president Sarkozy submitted a report that proposed the creation of an administrative body that would oversee a graduated response procedure. In 2008, legislation - 'Loi favorisant la diffusion et la protection de la création sur Internet' - created this administrative body.¹⁰⁰⁰ It is called 'Haute Autorité pour la Diffusion des Oeuvres et la Protection des Droits sur Internet' (HADOPI), which gave the law and procedure its nickname.¹⁰⁰¹ This authority handled the notification mechanism and the relation with access providers.¹⁰⁰² It had other goals besides graduated response (called 'the protection of human rights violations'). It also looks towards ways to stimulate legal offers, regulates technical protection measures and it does research.¹⁰⁰³

The HADOPI procedure is based on two laws. The first law, adopted on 13 May 2009, included provisions that would require the HADOPI body to impose a suspension or termination of Internet service to users after two warnings if their Internet connection had been used for infringement.¹⁰⁰⁴ Opponents challenged this law and consequently those provisions were struck down by the French Constitutional Council (the highest constitutional authority in France that checks whether new laws or statutes are compatible with the French constitution).

The Constitutional Council pointed out two deficiencies.¹⁰⁰⁵ First of all, the council argued that suspending an Internet connection affects human rights and therefore has to be done by a court instead of an administrative body. Second, they said introducing a negligence provision that blamed the infringement on the subscriber instead of the actual infringing user unless the subscriber proved the opposite violated the presumption of innocence.¹⁰⁰⁶

⁹⁹⁷ Bridy, "Graduated Response American Style," P.12

⁹⁹⁸ See for example: IFPI, Public Consultation on Creative Content Online in the Single Market – Submission of the "International Federation of the Phonographic Industry" (IFPI) in response to the Questionnaire of the European Commission regarding Policy/Regulatory Issues (Feb. 29 2008) P.13, http://ec.europa.eu/avpolicy/docs/other_actions/col_2008/ngo/ifpi_en.pdf

⁹⁹⁹ Motion Picture Association, Public Consultation on Creative Content Online in the Single Market – Submission of the "Motion Picture Association" (MPA) in response to the Questionnaire of the European Commission regarding Policy/Regulatory issues Feb. 29, 2008) P.2, available at http://ec.europa.eu/avpolicy/docs/other_actions/col_2008/comp/mpa_en.pdf

¹⁰⁰⁰ Bridy, "Graduated Response American Style," P.12

¹⁰⁰¹ Internet Society, Perspectives on Policy Responses to Online Copyright Infringement, an Evolving Policy Landscape," Internet Society website (Feb 20, 2011) P.26, <http://www.Internetsociety.org/perspectives-policy-responses-online-copyright-infringement-evolving-policy-landscape>

¹⁰⁰² Alain Strowel, "The 'Graduated Response' in France: Is It the Good Reply to Online Copyright Infringement." in: *Copyright Enforcement and the Internet*, ed. Stamatoudi (Kluwer Law International, The Netherlands, 2010). P. 147-148.

¹⁰⁰³ République Française, *Annex au projet de loi de finances pour 2013, Rapport sur les Autorités publiques indépendantes*, 71-94. P.71. Also in L331-13 of the Intellectual property code.

¹⁰⁰⁴ Strowel, "The 'Graduated Response in France," P. 148.

¹⁰⁰⁵ Decision 2009-580 DC of 10 June 2009, at: www.conseil-constitutionnel.fr

¹⁰⁰⁶ Strowel, "The 'Graduated Response' in France," P.154.

Because of the decision by the Constitutional Council, the revised law of 12 June 2009 only included warning mechanisms, but no stringent enforcement procedures. This led the French Parliament to adopt a second HADOPI Law that included an accelerated legal procedure and sanctions that were to be imposed by a criminal judge.¹⁰⁰⁷ The Constitutional Council on 22 October issued one adaption that divided the procedure in two stages: a warning stage that authorized HADOPI to examine claims of rights holders concerning alleged infringers and send out the warning letters, and second, a disconnection stage ordered only by court, but which gives the right to HADOPI to maintain a list of disconnected subscribers to prevent them from subscribing to another Internet service provider during the disconnection period.¹⁰⁰⁸

In the meantime the French telecoms law included a provision that forces ISPs to inform their subscribers of the consequences of copyright infringement.¹⁰⁰⁹ This was included in the contracts between ISPs and their subscribers.¹⁰¹⁰ The law underlined the pedagogical goals of the procedure, achieved through the warnings sent. In fact, HADOPI itself consistently referred to its work as being pedagogical instead of being enforcement.¹⁰¹¹

In the run-up to the French presidential elections, presidential prospect Francois Hollande promised to repeal the HADOPI law, if elected.¹⁰¹² After Hollande was elected, his new Culture Minister Aurélie Filippetti indicated that she was not impressed with the way HADOPI worked, and that cuts could be made. "In financial terms, 12 million Euros a year and 60 officers, it's an expensive way to send a million e-mails," the Minister said. "As part of budgetary efforts, I will ask that funding of HADOPI is greatly reduced."¹⁰¹³ The French government also commissioned Pierre Lescure, former CEO of Canal+ to report and reflect on the HADOPI system, and on cultural policy in general.

The report described (among other things) copyright exceptions, digital libraries and non commercial sharing. One of its key proposals was to revamp the graduated response system.¹⁰¹⁴ The report found that HADOPI had not accomplished enough of what it set out to do, because although P2P traffic decreased, traffic diverted to other infringing sources. This is why it recommended abolishing the commission and putting its responsibilities elsewhere, reducing the fine and getting rid of Internet termination as a possible remedy. It looked at other ways to combat piracy as well by, for example, going after large-scale piracy through

¹⁰⁰⁷ Strowel, "The 'Graduated Response' in France," P. 148-149.

¹⁰⁰⁸ Alexandra Giannopoulou (2012), "Copyright enforcement measures: the role of the ISPs and the respect of the principle of proportionality," *European Journal for Law and Technology*, Vol. 3. 1, (2012). <http://ejlt.org/article/viewArticle/122/204>

¹⁰⁰⁹ Monica Horten, "France puts copyright in contract," IPtegrity.com (August 30, 2011), <http://www.iptegrity.com/index.php/france/687-france-puts-copyright-in-isp-contract>

¹⁰¹⁰ L331-27 of the IPC.

¹⁰¹¹ République Française, *Annex au projet de loi de finances pour 2013, Rapport sur les Autorités publiques indépendantes*, 71-94. P.71.

¹⁰¹² Glyn Moody, "Leading French Presidential Candidate Would Repeal HADOPI But Keep Net Surveillance," *Techdirt* (October 26, 2011), <http://www.techdirt.com/articles/20111023/05483716480/leading-french-presidential-candidate-would-repeal-HADOPI-keep-net-surveillance.shtml>.

¹⁰¹³ Enigmax, "Three strikes anti-piracy budget "Too expensive to justify" says minister," *Torrentfreak* (August 3, 2012), <http://torrentfreak.com/three-strikes-anti-piracy-budget-too-expensive-to-justify-says-minister-120603/>.

¹⁰¹⁴ Anne-Catherine Lorrain, "Copyright policymaking and the digital public domain: a bitter-sweet wishful thinking from France," *Infojustice* (May 17, 2013), <http://infojustice.org/archives/29651>.

financial intermediaries.¹⁰¹⁵ Regarding the disconnection penalty the Internet policy minister said, “today, it’s not possible to cut off Internet access,” she said. “It’s something like cutting off water.”¹⁰¹⁶

The minister said she would adopt most of the recommendations of the Lescure report.¹⁰¹⁷ In July 2013 the law was revised again into what was later referred to as HADOPI-3. The French government issued a decree on July 8, 2013 (HADOPI-3) which abolished the suspension as a possible penalty for negligence on behalf of the subscriber, while retaining the maximum fine of 1500 Euros.¹⁰¹⁸ In a press release, the government revealed that the HADOPI authority would be abolished and its responsibilities located to the CSA (French audiovisual authority).¹⁰¹⁹

This news led to discussions in the media. Although some were quick to say the French government “dropped”¹⁰²⁰ the HADOPI law, that it was “gutted”¹⁰²¹ or “got the guillotine”,¹⁰²² most of the system remained intact. As Sarah Jacquier of HADOPI mentioned: “the Lescure report said that the mission should be maintained.” The change in the system was “just a question of money and merger,” and not about the criticism of what people consider a lack of freedom.¹⁰²³

¹⁰¹⁵ Pierre Lescure, *Mission « Acte II de l’exception culturelle » Contribution aux politiques culturelles à l’ère numérique*, Ministère de la Culture et de la Communication (May 2013) P.371 and P.379-381.,

www.culturecommunication.gouv.fr/var/culture/storage/culture_mag/rapport_lescure/index.htm#/1

¹⁰¹⁶ Eric Pfanner, “French Appear Ready to Soften Law on Media Piracy,” *The New York Times* (June 2, 2013), http://www.nytimes.com/2013/06/03/technology/03iht-piracy03.html?_r=0.

¹⁰¹⁷ “Lescure Report on Cultural Exception in France - The Way Forward?,” *The 1709 Blog* (May 20, 2013), <http://the1709blog.blogspot.nl/2013/05/lescure-report-on-cultural-exception-in.html>.

¹⁰¹⁸ Décret n° 2013-596 du 8 juillet 2013 supprimant la peine contraventionnelle complémentaire de suspension de l'accès à un service de communication au public en ligne et relatif aux modalités de transmission des informations prévue à l'article L. 331-21 du code de la propriété intellectuelle.

¹⁰¹⁹ “Lescure Report on Cultural Exception in France - The Way Forward?,” *The 1709 Blog* (May 20, 2013), <http://the1709blog.blogspot.nl/2013/05/lescure-report-on-cultural-exception-in.html>.

¹⁰²⁰ Siraj Datoo, “France drops controversial ‘Hadopi law’ after spending millions,” *the Guardian* (July 9, 2013), <http://www.theguardian.com/technology/2013/jul/09/france-hadopi-law-anti-piracy>

¹⁰²¹ Glynn Moody, “French Hadopi Scheme Gutted; Other Bad Ideas To Be Introduced Instead,” *Techdirt* (December 10, 2012), <http://www.techdirt.com/articles/20121209/07085621316/france-HADOPI-scheme-gutted-other-bad-ideas-to-be-introduced-instead.shtml>.

¹⁰²² Lars Brandle, “France’s ‘Three-Strikes’ Hadopi Law Gets the Guillotine,” *Billboardbiz* (July 10, 2013), <http://www.billboard.com/biz/articles/news/global/1569397/frances-three-strikes-HADOPI-law-gets-the-guillotine>.

¹⁰²³ Sarah Jacquier (Legal Director of HADOPI) interviewed by author, January 2014.

7.3 The procedure in practice

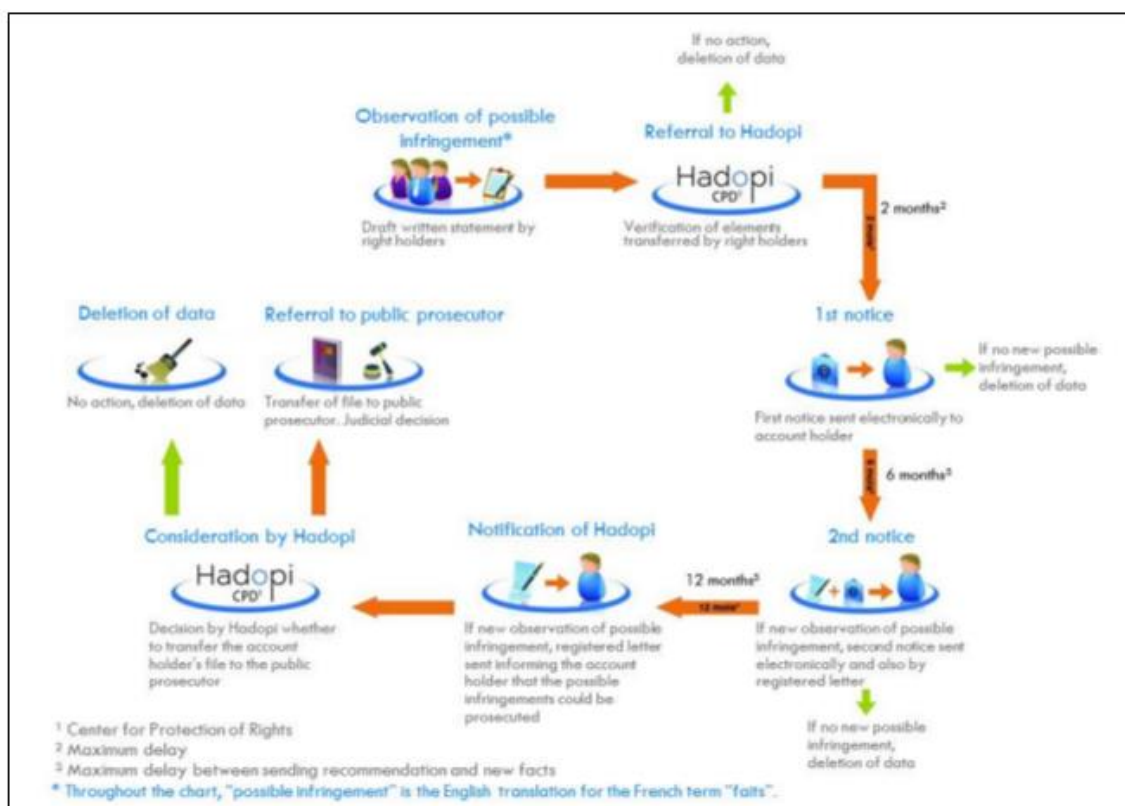


Figure 7.1: the HADOPI procedure schematically.¹⁰²⁴

The HADOPI authority consisted of two bodies: the Commission, and the Committee for the Protection of Rights.

The Commission was the governing body of the High Authority and had a college consisting of nine members who came from the Council of State, the Supreme Court, the Court of auditors, the Supreme Council of the Literary and Artistic Property, and 5 others proposed by the ministry, the national assembly and the senate.¹⁰²⁵ This commission dealt with all the tasks entrusted to it, except for those that were entrusted to the Committee for the Protection of Rights.

The committee on the protection of rights was an autonomous body which consisted of three members ('judges'), appointed for a term of six years, that come from the Council of State, the Supreme Court, and the Court of Auditors.¹⁰²⁶ This committee dealt with the graduated response procedure.

At the ISP level, the subscriber was made aware of the HADOPI procedure in the terms and conditions. They were required by law to so, as laid down in article L331-27 of the

¹⁰²⁴ Image source: HADOPI, "Réponse Graduée," accessed Apr. 5, 2012, <http://www.HADOPI.fr/usages-responsables/nouvelles-libertes-nouvelles-responsabilites/reponse-graduee.html>, translated by: Trisha Meyer, "Graduated response in France: The Clash of Copyright and the Internet," *Journal of Information Policy* 2 (2012): 107-127.

¹⁰²⁵ L331-16 IPC.

¹⁰²⁶ L331-17 IPC.

CPI. In an email to me, SFR confirmed that thad such a provision in section 7.3 of their conditions.¹⁰²⁷

The procedure based on the two HADOPI laws worked as follows:

- (1) Initiation: HADOPI did not collect personal data itself, but this was done by companies hired by rights holders. These were 'sworn agents' of rights holders groups and collecting societies, that had been accredited by the French Ministry of Culture. Those sworn agents identified IP addresses they claim were infringing on their copyrights. Article L. 331-24 CPI said sworn agents had to be appointed by lawfully constituted professional bodies, collective management societies, CNC (Centre National de la Cinématographie), or by the Public prosecutor. Article L. 331-21-1 CPI made sure that now also members of the commission for the protection of rights can detect punishable infringements.¹⁰²⁸ Individual rights holders could not bring facts to HADOPI, or ask for the IP address through which infringement has taken place.¹⁰²⁹ Detection requires the collection of personal data, and the agents therefore had to be authorized by the CNIL to collect the data.¹⁰³⁰

Trident Media Guard was the only known company acting as such a private investigator, and had been confirmed to monitor P2P file sharing networks. When such a company believed they found content that infringes on copyrights, they communicated the relevant information to HADOPI. These referrals included the date and time, the IP address, information on the relevant copyrighted material, and the name of the Internet Access Provider of the subscriber.¹⁰³¹

The HADOPI then reviewed these allegations for accuracy and whether copyright ownership could be confirmed. If this was the case, HADOPI requested the subscriber data from the access providers on the basis of the infringing IP addresses to identify the users.¹⁰³² The access provider had to communicate the necessary subscriber information (name, phone number, address, etc.) within eight days after having received the required technical information by HADOPI. If an access provider was not willing to cooperate it would risk a fine of 5000 Euros (L335-7). ISPs were expected to be able to identify 150,000 IP addresses per day. If they did not do so within 8 days, they risked a 1500 Euro fine per unidentified IP address per day.¹⁰³³

Only direct administrative agents of HADOPI (sworn in by its president) had access to the personal data. Data was supposed to be erased 2 months after it was provided to HADOPI, 14 months after the first warning, and 21 months after a second warning (except, of course, when a new warning is issued). When the infringement had been sent to the public prosecutor, data had to be removed from HADOPI's

¹⁰²⁷ Frédéric Dejonckheere (SFR) email to author, March 2014.

¹⁰²⁸ VL. Benabou, "The Chase: The French Insight into the 'Three Strikes' System." in: *Copyright Enforcement and the Internet*, ed. Stamatoudi (Kluwer Law International, The Netherlands, 2010). P. 173.

¹⁰²⁹ Benabou, "The Chase: The French Insight into the 'Three Strikes' System." P. 173.

¹⁰³⁰ Benabou, "The Chase: The French Insight into the 'Three Strikes' System." P. 174.

¹⁰³¹ "France," *Global Censorship Chokepoints*, <https://globalchokepoints.org/countries/france>, accessed on March 3, 2013.

¹⁰³² Strowel, "The 'Graduated Response' in France," P. 149.

¹⁰³³ Ernesto, "France starts reporting 'millions' of file-sharers," *Torrentfreak* (September 21, 2010), <http://torrentfreak.com/france-starts-reporting-millions-of-file-sharers-100921/>.

databases after one year or whenever a court decided not to issue a disconnection order (article 3, Décret n°2010-236).¹⁰³⁴

(2) Warning phase

(a) First warning: The Right Protection Committee of the HADOPI body could send an 'educational notification' through access providers to subscribers that their access to the Internet should not be used to make unlicensed copies of copyright protected content. (L331-25) This was a general monitoring obligation¹⁰³⁵ that also applied to subscribers offering access to third parties (like Universities offering Internet access to their students).

It mentioned that in the case of gross negligence (L 335-7-1 IPC) and in the case of copyright infringement through the Internet, penalties would follow (L 335-7 IPC).¹⁰³⁶

Such a notification contained the date and time of infringing acts, and the contact information of HADOPI, to allow the user to send observations or make a request for further information. Furthermore, the notification contained general information, on legal sources for online content and on the negative effects of piracy for creators and copyright industries.¹⁰³⁷ (L331-25)

(b) Second warning: If the HADOPI noticed that new infringing acts had been committed by the same Internet subscriber within 6 months of the first notification, HADOPI could send a second notification (electronically, or by mail), containing the same information.¹⁰³⁸ This notification could also contain an obligation for the subscriber to implement security measures.¹⁰³⁹ A list of security measures was established by the HADOPI body itself.¹⁰⁴⁰ R335-5 introduced by decree security tools that had to be installed. The notification did not contain information on the content itself. The subscriber could make observations to HADOPI or ask for clarification on the content of the works that triggered the warning (this information was originally not included in the warning) (L331-25).¹⁰⁴¹

(c) To identify repeated offenders, HADOPI held a list of IP addresses that had been identified as used for infringement (L. 331-37 CPI) and was authorized to create automatic data processing (ADP). The data conserved was only limited to the proof necessary for judicial proceedings: acts of procedure and information to the professional bodies and collective management societies, of the referral to the court, and of the notifications made by the HADOPI to the ISP when a sanction of suspension of Internet access was issued.¹⁰⁴²

¹⁰³⁴ "France," *Global Censorship Chokepoints*, <https://globalchokepoints.org/countries/france>, accessed on March 3, 2013.

¹⁰³⁵ Article L. 331-26 §1 of the IPC.

¹⁰³⁶ Benabou, "The Chase: The French Insight into the 'Three Strikes' System." P.173-174.

¹⁰³⁷ Strowel, "The 'Graduated Response' in France," P.149.

¹⁰³⁸ L. 331-26 § 2 IPC.

¹⁰³⁹ Article L. 331-26 § 2 IPC, and Strowel, "The 'Graduated Response' in France," P.149-150.

¹⁰⁴⁰ L. 331-32 IPC.

¹⁰⁴¹ Benabou, "The Chase: The French Insight into the 'Three Strikes' System." P.174.

¹⁰⁴² Benabou, "The Chase: The French Insight into the 'Three Strikes' System." P.174.

**PREMIER AVERTISSEMENT – HAUTE AUTORITÉ
POUR LA DIFFUSION DES ŒUVRES ET LA PROTECTION
DES DROITS SUR INTERNET (HADOPI)**

Dossier n° XXX XX XXX X XXX X
Date : jour mois année

Prénom NOM
XX voie XXXXX
CPSTAL VILLE
xxx.xxxxx@xxxx.xx



Madame, Monsieur,

Il a été constaté le mardi 26 mars 2013 à 10 heures 16 *, qu'une ou plusieurs œuvres ont été téléchargées ou partagées depuis votre accès à internet, en violation des droits d'auteur. Ces faits peuvent constituer une infraction pénale.

En tant que titulaire d'un abonnement à internet, vous êtes légalement responsable de l'utilisation qui en est faite. L'obligation de surveillance de cet accès est prévue par l'article L. 336-3 du code de la propriété intellectuelle.

Les faits constatés ont été commis avec le(s) logiciel(s)/protocole(s) XXX, depuis l'adresse IP XX.XXX.XX.XX, attribuée à votre connexion par votre fournisseur d'accès à internet XX.

Le téléchargement illégal, appelé couramment « piratage », prive les créateurs de leur rétribution et représente un danger pour l'économie du secteur culturel. Pour vous aider à identifier les sites internet proposant des contenus légaux et à préserver le développement du secteur culturel, vous pouvez découvrir l'ensemble des offres labellisées par l'Hadopi sur le site internet www.pur.fr.

Il vous est recommandé de prendre sans délai toutes mesures utiles pour éviter une nouvelle atteinte au droit d'auteur. A cette fin, vous pouvez consulter les fiches pratiques « usage et internet », disponibles sur le site internet de l'Hadopi : www.hadopi.fr/ressources/fiches-pratiques qui vous apporteront notamment des informations pour sécuriser votre ligne. Vous pouvez également vous rapprocher de votre fournisseur d'accès à internet.

Si, malgré les avertissements de l'Hadopi, votre accès à internet était à nouveau utilisé pour des mises en partage ou des téléchargements illégaux, vous pourriez, à l'issue de la procédure suivie devant l'Hadopi, être poursuivi(e) devant le tribunal de police pour contravention de négligence caractérisée. Vous risquez alors une amende d'un montant maximum de 1500 € et, le cas échéant, une suspension de votre accès à internet pour une durée maximale d'un mois (article R. 335-5 du code de la propriété intellectuelle). Retrouvez toute information utile sur www.hadopi.fr/acces-au-formulaire-reponse-graduee-jai-recu-un-mail.

Vous avez la possibilité de demander des précisions sur le contenu des œuvres qui ont été téléchargées ou offertes en partage et de formuler des observations, en contactant l'Hadopi :

Figure 7.2: a HADOPI warning.¹⁰⁴³

Interestingly enough, HADOPI had a special warning for “professionals” aimed to have them secure their Wi-Fi.¹⁰⁴⁴ These were hotels, restaurants, or other places with WI-FI hot spots.

(3) Repressive/corrective measures

(a) Suspension of Internet access

- (i) After the first two strikes, the HADOPI would open an investigation into the case on infringement, relying on the information provided in the first two phases and collecting further facts that may constitute an infringement. Whilst investigating, HADOPI could ask the alleged infringer to present observations, and HADOPI or the alleged infringer could further request a hearing (in which the alleged infringer may be assisted by legal counsel). If there had been a hearing, an official report would be released to the alleged infringer.
- (ii) After closing the investigation, HADOPI would present a summary report, which also contained a response by the access provider on whether or not closing off Internet access would be technically possible.

¹⁰⁴³ Image source: HADOPI, *Rapport Annuel 2013*, p.37

¹⁰⁴⁴ HADOPI, *Rapport Annuel 2013*, p.40-41

- (iii) HADOPI then forwarded this summary report to the attorney-general, who could decide whether or not criminal proceedings should commence. The attorney general could also decide that an additional investigation would be needed to establish whether an infringement occurred or whether the subscriber was negligent. This would for example mean that the computer of the subscriber would be searched. If the attorney general decided that there was sufficient proof of infringement, he would initiate either a simplified (before one criminal judge) or standard criminal procedure.
 - (iv) The criminal judge or criminal court could grant the various sanctions as provided by French copyright law. The judge or court could also impose Internet access suspension, ranging to one year, possibly accompanied by a prohibition for a user to subscribe with another access provider. In case of bundled subscriptions (also TV and phone access), this suspension only applied to Internet access. The subscriber had to continue paying access fees. A subscriber who had not directly committed infringing acts but had demonstrated negligence and had not implemented HADOPI security measures could be suspended for a maximum period of one month.¹⁰⁴⁵ For negligence, a subscriber could also be fined 1500 Euros. (L.335-7-1 CPI). If such a subscriber entered into another contract to access another public online communication service during the suspension period that subscriber could be liable to a max fine of 3,750 Euros. If an ISP did not comply with the suspension, it would liable for a fine of max 5000 Euros. In the event of copyright infringement (not negligence), the court could sanction a subscriber three years of imprisonment and a 300,000 Euro fine, and forbid Internet access for up to one year, with the prohibition to take another access contract.¹⁰⁴⁶
 - (v) When considering the suspension of access, the judge had to take into account the circumstances and seriousness of the violation, the circumstances of the infringer and the need to protect the freedom of expression.¹⁰⁴⁷ On the basis of these factors the judge could also decide on the duration of the suspension. If the decision by the judge was binding, the HADOPI would be informed of the supplementary penalty, and would notify the ISP to proceed and suspend access, no later than 15 days of the notice.¹⁰⁴⁸
- (b) The criminal judge in the simplified procedure could also rule on additional damages claimed by the copyright holder.¹⁰⁴⁹ In case of the standard criminal procedure, the Court imposed all the sanction, including civil damages.

In the newer, post July 2013 version, disconnection had been removed as a penalty.

¹⁰⁴⁵ L.335-7-1of the IPC.

¹⁰⁴⁶ Benabou, "The Chase: The French Insight into the 'Three Strikes' System." P.172.

¹⁰⁴⁷ Listed in Article L. 335-7-2 of the IPC.

¹⁰⁴⁸ Benabou, "The Chase: The French Insight into the 'Three Strikes' System." P.178.

¹⁰⁴⁹ Article 495-6-1, §2 of the Code on Criminal Procedure.

7.4 Scale, severity and procedural safeguards

In the report of the French independent authorities submitted to Parliament, it was said that HADOPI in its first 24 months had partly been focused on the implementation of graduated response, and that they expected more efficiency in the following periods. They referred to the first two years as the ‘implementation’ phase.¹⁰⁵⁰ This may have consequences for the way the HADOPI procedure performed on the relevant variables. As the system changed in July 2013, I have data until that date. Additional information had not been made public yet.

In this implementation period not everything ran smoothly. In May 2011, TMG suffered a security breach, which made the French government temporarily suspend the acquisition of new data from TMG. The breach was exposed when a French writer was able to get his hands on internal documents, including IP addresses, through the TMG servers. Eric Walter, then head of the HADOPI agency, decided to temporarily halt business with TMG.¹⁰⁵¹

Popular blogs further criticized the anti-piracy software used by TMG as being too open for abuse, which could have the consequence of privacy breaches.¹⁰⁵² I cannot verify those claims and TMG unfortunately refused to speak to me.

Scale

The HADOPI authority itself referred to its system as an “inverted pyramid.”¹⁰⁵³ One of the main ideas behind HADOPI was that the procedure could scale up enforcement. Rights holders had argued that lawsuits were ineffective because they were too limited in scope.¹⁰⁵⁴

In the first three weeks of its existence, HADOPI received 25,000 copyright infringement notices from rights holders per day¹⁰⁵⁵, which became 18 million notifications in the first 9 months of its existence.¹⁰⁵⁶ This means 18 million acts of infringement. By June 2011, HADOPI had made 1,023,079 requests to ISPs to identify subscribers, sent out 470,935 first warnings, and 20,598 second warnings.¹⁰⁵⁷

¹⁰⁵⁰ République Française, *Annex au projet de loi de finances pour 2013, Rapport sur les Autorités publiques indépendantes*, 71-94. P.73.

¹⁰⁵¹ “Le honeypot de TMG,” *Reflets.info* (May 13, 2011), <http://reflets.info/le-honeypot-de-tmg/> and: Nate Anderson, “France halts ‘three strikes’ IP-address collection after data leak,” *Wired* (May 17, 2011), <http://www.wired.com/threatlevel/2011/05/tmg/>

¹⁰⁵² Peter Bright, “French ‘three strikes’ anti-piracy software riddled with flaws,” *Ars Technica* (May 26, 2011), <http://arstechnica.com/tech-policy/2011/05/french-three-strikes-anti-piracy-software-riddled-with-flaws/> and: Cory Doctorow, “More incompetence revealed on the part of France’s ‘three-strikes’ copyright enforcer,” *Boingboing* (May 26, 2011), <http://boingboing.net/2011/05/26/more-incompetence-re.html>.

¹⁰⁵³ Sarah Jacquier (Legal Director of HADOPI) interviewed by author, January 2014.

¹⁰⁵⁴ Monica Horten, *The Copyright Enforcement Enigma, Internet Politics and the ‘Telecoms Package’*, (palgrave MacMillan, 2012), P. 81.

¹⁰⁵⁵ “Music Rights Holders Send 25,000 Copyright Notices in France Daily”, *Michael Geist* (Oct 25, 2010), <http://www.michaelgeist.ca/2010/10/hadopi-25k-notices/>

¹⁰⁵⁶ Loek Essers, “Fransen nemen half miljoen file sharers op de korrel,” *Webwereld* (July 14, 2011), <http://webwereld.nl/nieuws/107298/fransen-nemen-half-miljoen-filesnarers-op-de-korrel.html>, accessed on Oct 26, 2011.

¹⁰⁵⁷ HADOPI, “L’Essentiel du Rapport D’Activité. 2010 (Paris: HADOPI, 2011),” through Trisha Meyer, “Graduated response in France: The Clash of Copyright and the Internet,” *Journal of Information Policy* 2 (2012): 107-127

According to a parliamentary reply made by the Minister of Justice, the fruits of the 2009 statutes, after being active for three years, were then as follows: 1,150,000 first warnings, 100,000 second warnings and 340 files in third stage with 14 having been forwarded to the local prosecutors.

By the end of 2012, of the 14 cases being prosecuted at the local level: - 9 were still being investigated; - 1 was scheduled for court; - 1 had been filed without a trial; and - 3 gave rise to definitive judgments, broken down as follows: - 1 acquittal; - 1 conviction (fine of €150); and - 1 conviction (no sentence due to circumstances).¹⁰⁵⁸ This is also in the report on French independent authorities.¹⁰⁵⁹

For those cases that make it to the third stage few actually are referred to prosecution. According to Sarah Jacquier of the HADOPI authority this is because after the third stage an evaluation was made as to whether there is enough evidence to hand it over to the prosecutor. Some cases were put on hold where they wait for another infringement.¹⁰⁶⁰ This is the investigation referred to in the previous section. In some cases, individuals protest enough to escape trial. The New York Times reports that five individuals who reached the final stage were helped by an organization called SOS HADOPI and were cleared before going to court.¹⁰⁶¹

In 2013, the HADOPI authority increased the amount of notifications sent out, nearly doubling in the amount of warnings sent out per month, as compared to the previous years. By the end of July 2013, HADOPI had issued a total of 2,004,847 first notices and 201,288 second notices, and there had been 710 investigations, to see whether subscribers who had received three allegations should be referred to prosecutors (although it is not entirely clear whether this number covers only the completed ones, or then current investigations as well).¹⁰⁶²

According to HADOPI, in 9 out of 10 cases, the third phase is not referred to trial because of submissions by the subscriber, or because the infringement stopped after that.¹⁰⁶³ In June 2013, the total number of third strikes was 663, while the cases referred to court were 51.¹⁰⁶⁴ A number of those cases were decided and it was established that users had been negligent. They were sentenced to payments ranging from 50 to 600 Euros.¹⁰⁶⁵

In those last months, HADOPI issued its first disconnection penalty. The person involved was sentenced to a disconnection for 15 days, and had to pay €600 fine for sharing a couple of works.¹⁰⁶⁶ Interestingly enough, this sentence was issued right before the disconnection penalty was removed from the law. A French legal principle applies which says

¹⁰⁵⁸ FrenchKat, "HADOPI: Where Things Stand," *1709 Blog* (Dec 31, 2012), <http://the1709blog.blogspot.nl/2012/12/hadopi-where-things-stand.html>

¹⁰⁵⁹ République Française, *Annex au projet de loi de finances pour 2013, Rapport sur les Autorités publiques indépendantes*, 71-94. P.73.

¹⁰⁶⁰ Sarah Jacquier (Legal Director of HADOPI) interviewed by author, January 2014

¹⁰⁶¹ Eric Pfanner, "Copyright Cheats Face the Music in France," *The New York Times* (February 19, 2012), <http://www.nytimes.com/2012/02/20/technology/20iht-piracy20.html?pagewanted=all>.

¹⁰⁶² HADOPI, *Réponse graduée – Les chiffres clés* (Aug. 2013), http://www.HADOPI.fr/sites/default/files/page/pdf/Chiffresreponsegraduee_aout.pdf, P.1, 3, 5.

¹⁰⁶³ HADOPI, *Report Annuel 2013*, p. 9

¹⁰⁶⁴ HADOPI, *Report Annuel 2013*, p. 28

¹⁰⁶⁵ HADOPI, *Report Annuel 2013*, p. 35

¹⁰⁶⁶ Marc Rees, "Hadopi : 600 € d'amende et quinze jours de suspension pour un abonné," *Next Inpact* (June 12, 2013), <http://www.pcinpact.com/news/80487-HADOPI-600-d-amende-et-quinze-jours-suspension-pour-abonne.htm>.

new milder sentences for violations apply over older harsher ones, so authorities will waive this suspension.¹⁰⁶⁷

In 2014, the authority itself revealed that 9% of French Internet users had received a warning.¹⁰⁶⁸

Severity

Although the statutes originally allowed for heavy penalties (in fact, they allowed for ‘triple punishment’: Paying a fine, the removal of Internet access, and paying subscription costs), in reality, punishments have not been severe: there were few convictions for negligence, of which one had no punishment, and of which one was a fine of 150 Euros. There has been one sentenced disconnection, which has been suspended, because of the system change. Besides that, people have received warning letters, and their personal data has been stored for limited times for enforcement purposes. Interestingly enough, in the cases that went to trial, none of them involved proven infringement, but all were about negligence.¹⁰⁶⁹

Safeguards

Safeguards have been one of the main discussion points during the creation of the HADOPI law. In part, this is because graduated response was about avoiding the courts.¹⁰⁷⁰ The Constitutional Council struck down provisions from the first HADOPI law because they offered too little safeguards.

First of all, the Council was against the power of the authority itself to order suspension of Internet access. It explained that the freedom of expression also entails the right to access new information and services that provide new information.¹⁰⁷¹ It added that Internet access falls under this freedom because of the actual state of communication technologies, the broad development of the online public services and because of the importance of those services for the democratic life and the expression of ideas and opinions.¹⁰⁷² The Constitutional Council argued that these rights may be limited, certainly to safeguard intellectual property, but restrictions must be necessary and proportionate to the purpose they seek to achieve.

The constitutional council argued that therefore, no administrative council could order suspension, because the measure applies to the freedom to speak and communicate from home, because it could affect more people than the actual infringer (the subscriber, and all other people using the subscription), and because legislated like this, the power of the administrative authority would apply to the whole population.¹⁰⁷³

¹⁰⁶⁷ Marc Rees, “Hadopi : la peine de 15 jours de suspension à Internet ne sera pas appliquée,” *Next Impact* (September 5, 2013), <http://www.pcinpact.com/news/82170-HADOPI-peine-15-jours-suspension-a-Internet-ne-sera-pas-appliquee.htm>.

¹⁰⁶⁸ HADOPI, *Réponse graduée – Les chiffres clés* (July. 2014), http://HADOPI.fr/sites/default/files/page/pdf/20140716_Point_presse_CPD_Vdef3_0.pdf

¹⁰⁶⁹ Rebecca Giblin, "Evaluating Graduated Response," *Columbia Journal of Law & the Arts* 37 (2014): 147. P. 157-158.

¹⁰⁷⁰ Monica Horten, *The Copyright Enforcement Enigma, Internet Politics and the ‘Telecoms Package’*, (Palgrave MacMillan, 2012), P.3.

¹⁰⁷¹ in § 12 of the decision

¹⁰⁷² Strowel, "The ‘Graduated Response’ in France," P.154-155.

¹⁰⁷³ Strowel, "The ‘Graduated Response’ in France," P.156-157.

Interestingly enough, whilst this was happening the EU took a step back in the discussion on the graduated response procedure by saying that the requirement of a judicial decision is not mandatory anymore for suspension of access. However, graduated response measures did need to have procedural safeguards, such as effective judicial protection and due process. In particular, they needed a prior, fair and impartial procedure, ensuring the presumption of innocence and the right to be heard of the person or persons, and effective and timely judicial review.¹⁰⁷⁴

The constitutional council was also against the 'negligence' provision. It said that punishing a subscriber instead of the actual infringing user violates the presumption of innocence, because it makes subscribers liable for any copyright infringement, unless they prove the contrary.

As a reaction to this decision, the second HADOPI law determined that only a judge could rule on penalties as a result of infringement. But the negligence provision remains.

Privacy

To find infringement, graduated response systems require the surveillance of Internet traffic, and to find infringers they require ISPs to identify infringers. This raises privacy concerns. In fact, the European Data Protection Supervisor has said that this violates the EU charter of Fundamental Rights and EU Data Protection and Privacy Directives.¹⁰⁷⁵

There are many different ways in which surveillance can take place. Deep packet inspection (DPI) would be the most invasive, and likely to be a violation of privacy. However, as information on infringement was collected by 'sworn agents' like TMG, it is unlikely that ISPs used DPI to spot copyright infringement in the context of this procedure.

The surveillance done by third party agents like TMG is often referred to as "over the top" surveillance (because it operates at the application layer, and not at the level of physical infrastructure), because such agents monitor public P2P file sharing networks by joining them and keeping track of the IP addresses on those networks that share infringing files. To spot which files are infringing, those agents have giant catalogues of copyright protected content, supplied to them by rights holders.¹⁰⁷⁶ This method of surveillance is not as intrusive as DPI, and targets less people, although it is still a large group. Also, people that contribute to P2P networks that are publicly accessible can reasonably expect that their content or hard drive is less private.¹⁰⁷⁷

Another potential privacy risk is whether or not identities of users that allegedly shared copyright protected content are made public. The system fortunately has been designed in such a way that subscriber information is not handed over to rights holders. Having a list of repeat offenders could potentially threaten privacy. The French Data Privacy Law (Law on Informatics and the Protection of Freedoms of 6 January 1978) covers the collection and processing of IP addresses of users who are suspected of committing online infringement. Article 9 of this Law allowed only some legal entities that represent the rights owners to collect and process the data needed to identify infringers.

¹⁰⁷⁴ Benabou, "The Chase: The French Insight into the 'Three Strikes' System." P.177.

¹⁰⁷⁵ Frank La Rue, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression." *U.N. DOC. A/HRC/17/27* (2011). P.14.

¹⁰⁷⁶ Bridy, "Graduated Response American Style," P.30.

¹⁰⁷⁷ Bridy, "Graduated Response American Style," P.31.

The HADOPI law further provided that only sworn surveyors of collecting societies and of properly constituted professional bodies were allowed to make referrals to the Rights Protection Committee.¹⁰⁷⁸

Impartial, competent and independent judge

To what extent are we dealing with an impartial, competent and independent judge? The final phase of the HADOPI process certainly seems to provide this by including a criminal judge. Those judges are by law required to be impartial, competent, and independent.

With regards to the first and second phase, 'judgment' was handled by the rights protection committee of the high authority. The HADOPI itself is a neutral authority according to the law at the time. The High Authority used accredited agents, who will be the collecting societies and the organizations representing the rights-holder industries (SACEM, SNEP), and film and music producers, and the French Film council (Centre Nationale de Cinematographie).¹⁰⁷⁹ The rights protection committee was an autonomous body which consists of three members ('judges'), appointed for a term of six years, coming from the council of state, the Supreme Court, and the court of auditors (L331-17). This committee dealt with the graduated response procedure. That they are appointed for a longer period of time (although not for life), and that they have judicial backgrounds, also seems to suggest they are impartial, competent and independent.

Apart from that, the French Intellectual Property Code created provisions that were supposed to create more independence for the HADOPI employees. L331-18 provided that in the last three years, members could not have worked for an access provider, or an audio-visual communication enterprise.

Meanwhile, independence is not the same as impartiality. There is no reason to believe that members of the committee for the protection of rights have a financial, professional or personal relationship with the parties relevant to graduated response. One could wonder to what extent the authority is influenced by politics, as this was such a high point on Sarkozy's agenda.

Presumption of innocence

The presumption of innocence was affected in two ways: In the allegation phase, and through the negligence provision.

The first two allegation phases have been so large in scale that it seems impossible for the HADOPI employees to ascertain the accuracy of the allegations made by rights holders and their agents. In the report on independent authorities submitted to the French Parliament, it said that 6 FTE of the Protection of Rights Committee (of 13.5) send out the recommendations (119097 per FTE) in 2011. In the first three quarters of 2012 6 FTE (of 16.3 FTE) sent out the recommendations (each agent 132012 per FTE).¹⁰⁸⁰ That would mean that each agent would check infringements of more than one hundred thousand people per year. That is impossible. In fact, in a leaked report, the French Privacy Commissioner (CNIL)

¹⁰⁷⁸ Strowel, "The 'Graduated Response' in France," P. 152.

¹⁰⁷⁹ Monica Horten, "Briefing on France's Creation and Internet Law – DRAFT," *IPtegrity* (Nov 11, 2008), <http://www.iptegrity.com/pdf/Monica.Horten.creation.Internet.law.2.11.2008.pdf>

¹⁰⁸⁰ République Française, *Annex au projet de loi de finances pour 2013, Rapport sur les Autorités publiques indépendantes*, 71-94. P.82.

admitted that the high number of cases will create a situation where it is impossible to check the accusations made by rights holders for accuracy. So HADOPI will accept or deny the transmitted findings, without checking them. There is not even a sampling procedure used.¹⁰⁸¹

In an interview with Sarah Jacquier of HADOPI at the time, she mentioned that they did have criteria to check incoming complaints. They for example checked if the information sent in was from a sworn agent, and whether the date was correct. They did concede that they did not go into every isolated event, because there were opportunities for the end user to explain or to go into events.¹⁰⁸²

That is interesting, because the evidence in the HADOPI procedure was gathered by private investigators, who had a financial interest in the process.¹⁰⁸³ Also, the quality of the allegations was unclear. The system was designed to make it cheap for rights holders to issue allegations en masse. Some say that rights holders have a questionable reputation when it comes to finding infringement.¹⁰⁸⁴ But this also creates bad incentives. Normally, in civil proceedings, the costs are against the plaintiff if the claim does not succeed. This time, that is not the case.¹⁰⁸⁵

The French Constitutional Council originally criticized the negligence provision, which was still in the Intellectual property code. A person who had subscribed to online public communication services to have Internet access was under a duty to ensure that this access was not used for reproducing, showing, making available or communicating to the public works or property protected by copyright, or a related right, without the authorization of the copyright holders provided for in Books I and II when such authorization was required.¹⁰⁸⁶ This was different from the offence of infringing copyright.¹⁰⁸⁷

Originally, the intellectual property code contained a provision that said that subscribers themselves had to prove that infringement happened by a third party (presumption of guilt).¹⁰⁸⁸ This meant that the access holder did not have to do anything in particular, but it would be sufficient to acknowledge that infringement had taken place through someone's connection to trigger liability.¹⁰⁸⁹ The Constitutional Council criticized this provision, which was subsequently removed.¹⁰⁹⁰

However, the negligence provision itself is still there. One wonders how the burdens of proof have been distributed now. In the first case that has actually led to a conviction, the subscriber said that he was incapable of downloading infringing content, and that he knew his wife had done it, who confessed. However, by admitting that he knew she had done it,

¹⁰⁸¹ Guillaume Champeau, "HADOPI: la CNIL avait dénoncé l'absence de contrôle de TMG!" *Numerama* (September 20, 2010), <http://www.numerama.com/magazine/16826-hadopi-la-cnil-avait-denonce-l-absence-de-contrôle-de-tmg.html>

¹⁰⁸² Sarah Jacquier (Legal Director of HADOPI) interviewed by author, January 2014.

¹⁰⁸³ "France," *Global Censorship Chokepoints*, <https://globalchokepoints.org/countries/france>. Last viewed on March 3, 2013, and: L336-3 of the IPC.

¹⁰⁸⁴ Nicolas Suzor and Brian Fitzgerald. "The Legitimacy of Graduated Response Schemes in Copyright Law," *University of New South Wales Law Journal* 34 (2011): 1. P.17.

¹⁰⁸⁵ Suzor and Fitzgerald. "The Legitimacy of Graduated Response Schemes in Copyright Law," P.24.

¹⁰⁸⁶ L 336-3 of the IPC.

¹⁰⁸⁷ The Constitutional Council also mentions this. In 7.

¹⁰⁸⁸ L 331-38 of the IPC.

¹⁰⁸⁹ Benabou, "The Chase: The French Insight into the 'Three Strikes' System." P.170-171.

¹⁰⁹⁰ 18 of the constitutional council decision.

he ‘incriminated’ himself, and was found liable for not securing his connection.¹⁰⁹¹ That is not only strange, but one could argue that this violates a safeguard connected to the presumption of innocence, namely that punishment only applies to the offender.

There are additional problems connected to this: Negligence in this context has also been defined as “not having put in place security measures” or having “lacked diligence in putting in place these measures”—perhaps even something as simple as a weak wireless password. This created a new obligation to secure one's Internet connection, creating legal liability for individuals and businesses that open their wireless networks. This could also apply to universities, public places like bars and libraries.

But it requires some ‘tech’ knowledge to know how to secure a connection, and wireless connections were invaded often.¹⁰⁹² The problem is that this might have lead subscribers to use filtering systems offered by ISPs. Libraries or universities could take disproportionate measures to avoid liability, which could infringe on other human rights like privacy and free speech. And the costs of those solutions are for the subscriber. It is still unclear how the installation of these measures will affect the subscriber liability.¹⁰⁹³

On the other hand, removing the provision that subscribers had to prove their innocence made it easy for them to avoid liability, because they could simply claim their access has been fraudulently intruded by a third party.¹⁰⁹⁴ Or remain silent.¹⁰⁹⁵

In an interview, Sarah Jacquier of the HADOPI authority at the time said it was not about being liable for infringement, but about being liable for negligence. The user would have been warned many times that his or her connection has been used for illegal purposes, so it is “completely okay” to go after this person.¹⁰⁹⁶

Notice, right to be heard (prior to conviction), defenses and appeal

In the first phase of HADOPI, subscribers were not heard before they were warned. Those warnings contained something of a notice, although they notified users that their connection had been used for infringement. In the second phase, the subscriber could make observations to HADOPI or ask for clarification on the content of the works that triggered the warning (this information was originally not included for discretion).¹⁰⁹⁷

After the first two strikes the HADOPI would open an investigation into the case on infringement, relying on the information provided in the first two phases and collecting further facts that may constitute an infringement. Whilst investigating, HADOPI asked the alleged infringer to present observations, and HADOPI or the alleged infringer could further

¹⁰⁹¹ Glyn Moody, “First HADOPI Victim Convicted, Not For His Own Infringement, But Because His Wife Downloaded Songs,” *Techdirt* (September 13, 2012), <http://www.techdirt.com/articles/20120913/06550920370/first-HADOPI-victim-convicted-not-his-own-infringement-because-his-wife-downloaded-songs.shtml>

¹⁰⁹² Rainey Reitman, “Repealing French Three Strikes Law is the Next Step to Safeguarding Free Expression,” *Electronic Frontier Foundation* (August 8, 2012), <https://www.eff.org/deeplinks/2012/08/repeal-french-three-strikes-law>.

¹⁰⁹³ Benabou, “The Chase: The French Insight into the ‘Three Strikes’ System.” P. 172.

¹⁰⁹⁴ Benabou, “The Chase: The French Insight into the ‘Three Strikes’ System.” P.172.

¹⁰⁹⁵ Guillaume Champeau, “Devant l'Hadopi, le silence est la meilleure des defenses,” *Numerama* (December 16, 2011), <http://www.numerama.com/magazine/20964-devant-l-HADOPI-le-silence-est-la-meilleure-des-defenses.html>.

¹⁰⁹⁶ Sarah Jacquier (Legal Director of HADOPI) interviewed by author, January 2014.

¹⁰⁹⁷ Benabou, “The Chase: The French Insight into the ‘Three Strikes’ System.” P. 174, and L331-25 of the IPC.

request a hearing (in which the alleged infringer may be assisted by legal counsel). If there had been a hearing, an official report would be released to the alleged infringer.

A huge number of people responded to the warnings. The percentage of users that contacted HADOPI after receiving a warning was around 7,3% for 2011, and around 9,79% for 2012. In 2011 the committee received 52,387 letters/calls, in 2012 this number was 23,460. According to the report, most often these callers were interested in the details of the works concerned.¹⁰⁹⁸

HADOPI itself reported an upward trend of each phase: 6% of subscribers that received a first warning contacted HADOPI, 25% of subscribers that received a second warning contacted HADOPI, and 71% of subscribers of stage three contacted HADOPI. These percentages were based on 2011, and HADOPI claimed that most of these users wanted to secure their access to the Internet or to stop P2P network activity on their connection.¹⁰⁹⁹

One wonders to what extent the committee was able to process all these requests. In 2011, 7,5 FTE were working on them, which equals 6984 requests per FTE. The amount of people working on them increased in 2012, with 10,3 FTE dealing with those appeals in the first three quarters of 2012. However, this still equals 4392 requests per FTE.¹¹⁰⁰ When individuals asked to be heard, they had the right to a counsel of choice.¹¹⁰¹

The special and simplified proceedings created by the second HADOPI law are comparable to those applicable to speed tickets,¹¹⁰² and intended to deliver swift justice. It excluded a due hearing of the defendant, who had 45 days to contest the decision by a motion to vacate and bring the case before the judge for a regular trial.¹¹⁰³ Some writers suggested that the idea is that the fast track court cases would give a judge five minutes, and 45 minutes in total.¹¹⁰⁴

In terms of procedural rights, both criminal procedures offered that (and there are more) the decision must be well reasoned, subject to appeal (45 days) and that the order would be stayed pending appeal.¹¹⁰⁵

Transparency

The HADOPI law was the outcome of public debate, both in parliament and in the press. As it concerned a public body, its implementation has been relatively transparent as well. At <http://www.HADOPI.fr/>, the authority published research done by the authority itself, regular press releases, and reports on its functioning. Apart from that, the French government required annual reports that go into its results and finances. It did not publish reports on how it applied copyright rules in particular, which made the first and second

¹⁰⁹⁸ République Française, *Annex au projet de loi de finances pour 2013, Rapport sur les Autorités publiques indépendantes*, 71-94. P.81-82.

¹⁰⁹⁹ HADOPI, *HADOPI: 1.1/2 year after the launch* (2012) P.3, available at: http://www.HADOPI.fr/sites/default/files/page/pdf/note17_en.pdf

¹¹⁰⁰ République Française, *Annex au projet de loi de finances pour 2013, Rapport sur les Autorités publiques indépendantes*, 71-94. P.82.

¹¹⁰¹ L331-21 of the IPC.

¹¹⁰² Benabou, "The Chase: The French Insight into the 'Three Strikes' System." P.177.

¹¹⁰³ Benabou, "The Chase: The French Insight into the 'Three Strikes' System." P.178.

¹¹⁰⁴ Janko Roettgers, "Three strikes: Five minutes per court decision," *P2P Blog* (Jan 7, 2009), <http://www.p2p-blog.com/item-1101.html>

¹¹⁰⁵ Strowel, "The 'Graduated Response' in France," P.150-151.

phase less transparent. On the other hand, it would have been impossible to publish millions of sanctions, and could create data protection problems.

With regards to the transparency of its outcomes: The decisions made by judges in the criminal procedures had to be well reasoned.¹¹⁰⁶ This allowed citizens to know how the law and the new negligence provisions are applied.

Proportionality

One of the major concerns at HADOPI's inception concerned the proportionality of the measure. To assess whether measures are proportional, it is important to look at whether the measures are necessary to achieve the stated goal, suitable, and whether they do not put too much of a burden on individual rights.

So was this measure necessary? The stated goals of HADOPI were education and deterrence. Certainly, there are other ways to achieve this. However, the necessity in this case came from empirical evidence that demonstrated that previous enforcement measures were unable to sufficiently curb P2P file sharing.

Was this suitable? It seemed to work to an extent (see more on this in the next section as well). The evidence provided by the declining scale in warnings sent out in each step of the process suggested that as an educational/deterrent measure it is effective. As Sarah Jacquier from HADOPI put it: "maybe because we don't find the people, or maybe because they go to streaming, but also maybe because they got the point." She said that the small number of cases handed over to the prosecutor is an indication of how the education worked.¹¹⁰⁷

Was there a large burden on individual rights? The threat of disconnection was the cause of much controversy, and according to Sarah Jacquier the main point of criticism.¹¹⁰⁸ But the final sentence had not been awarded (with the exception of one suspended sentence). The other sentences, small monetary fines, did not seem to be an excessive burden on the rights of individuals, and comparable with parking tickets. The maximum fine of 1500 Euros for severe negligence would be a heavy penalty, but it had not been issued yet.

7.5 Impact on infringement levels

The authority itself claimed that the graduated response procedure had proven successful during its 'implementation phase.' They said there was a clear "downward trend in illegal P2P downloads"¹¹⁰⁹

They cited some research reports on the effects, with the side note that although some "marginal effects" remain difficult to determine exactly, the different methodologies used for the different conclusions all pointed towards the same thing: They reflect a "shared tendency to move away from this form of illegal downloading since the graduated response procedure was introduced."¹¹¹⁰

¹¹⁰⁶ Strowel, "The 'Graduated Response' in France," P.150-151.

¹¹⁰⁷ Sarah Jacquier (Legal Director of HADOPI) interviewed by author, January 2014.

¹¹⁰⁸ Sarah Jacquier (Legal Director of HADOPI) interviewed by author, January 2014

¹¹⁰⁹ HADOPI, *HADOPI: 1.1/2 year after the launch* (2012) P.1, available at:

http://www.HADOPI.fr/sites/default/files/page/pdf/note17_en.pdf

¹¹¹⁰ HADOPI, *HADOPI: 1.1/2 year after the launch* (2012) P.2.

They revealed that 95% of users that have received a first warning have not received a second warning.¹¹¹¹ 90-98% of users that received a second warning did not receive a third warning. 97-99% of users that received a third warning did have contact with the system afterwards. HADOPI expects this number to go up.¹¹¹²

Apart from the decrease of notified people, HADOPI cited a number of studies that measured P2P usage (figure 7.3, 7.4, 7.5, 7.6, 7.7. All images are from the HADOPI report).¹¹¹³

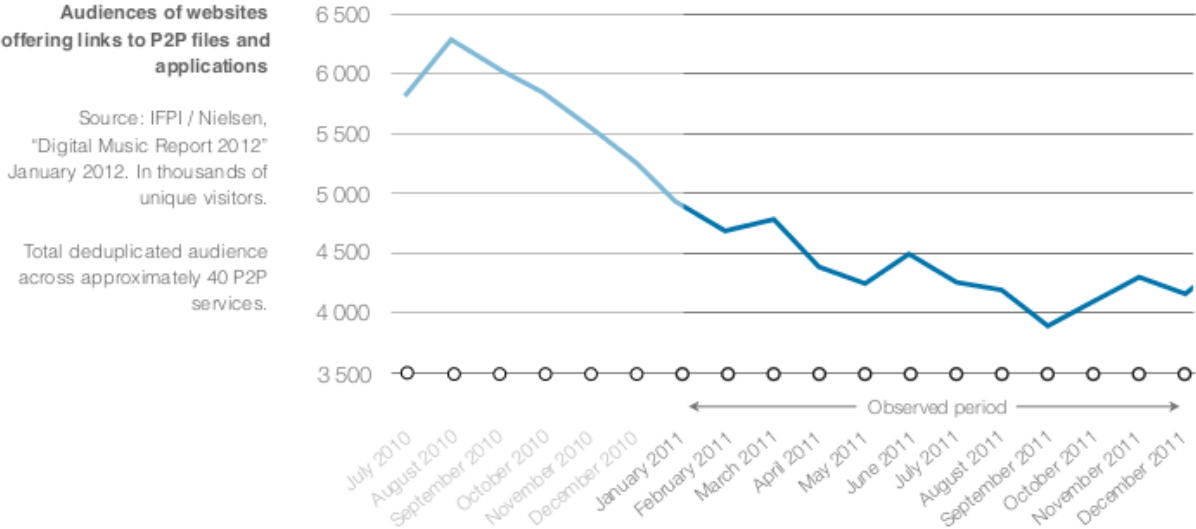


Figure 7.3: Nielsen study on audiences of P2P websites.

¹¹¹¹ République Française, *Annex au projet de loi de finances pour 2013, Rapport sur les Autorités publiques indépendantes*, 71-94. P.73.

¹¹¹² République Française, *Annex au projet de loi de finances pour 2013, Rapport sur les Autorités publiques indépendantes*, 71-94. P.80.

¹¹¹³ HADOPI, *HADOPI: 1.1/2 year after the launch* (2012) P.4-6.

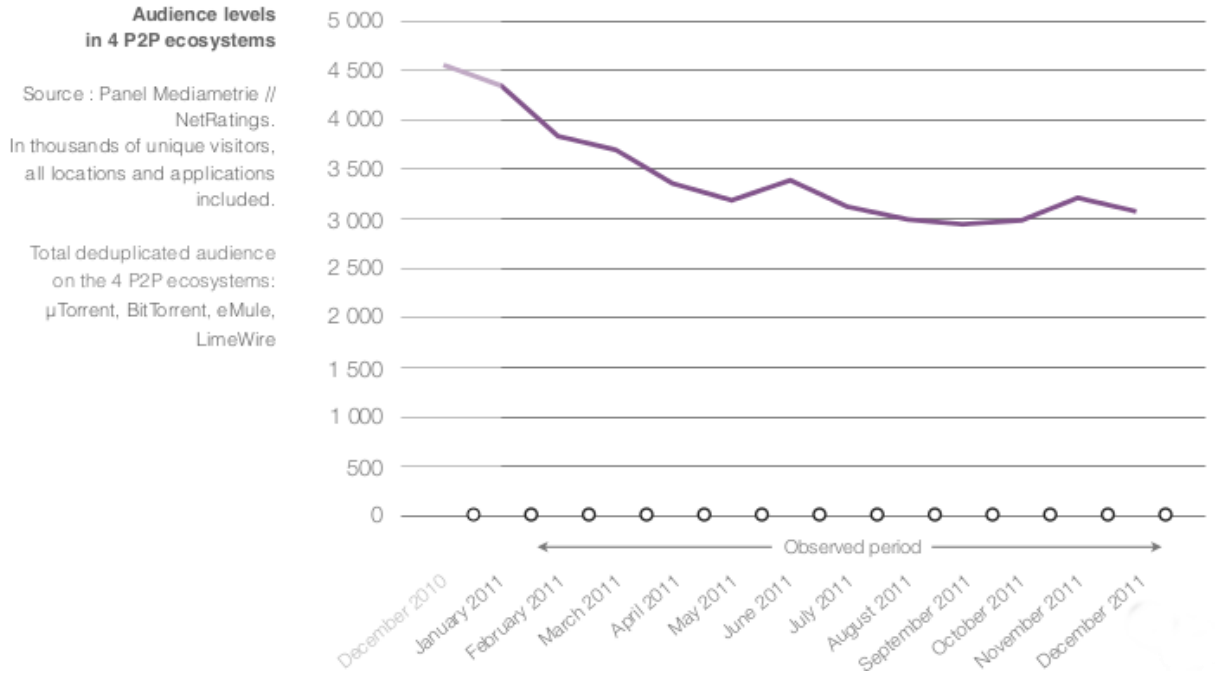


Figure 7.4: Médiamètrie//NetRatings study on audience levels in 4 P2P ecosystems.

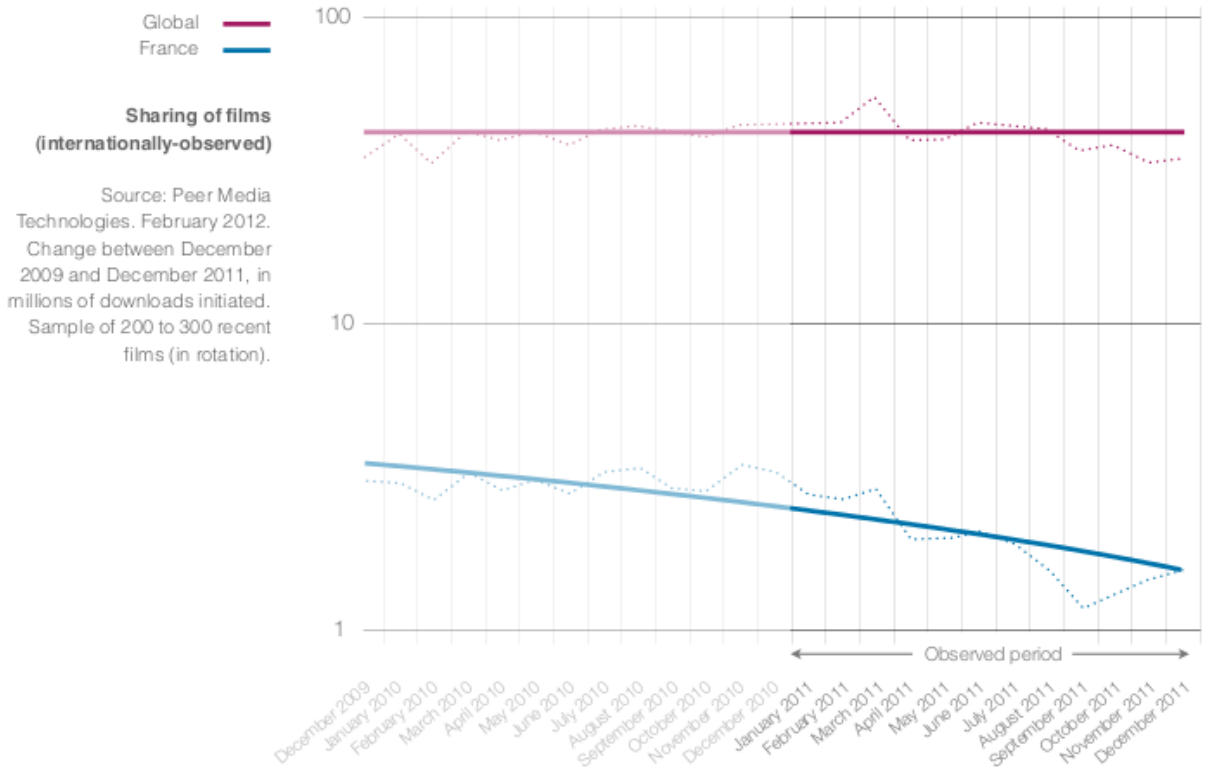


Figure 7.5: Peer Media Technologies study on sharing of films.

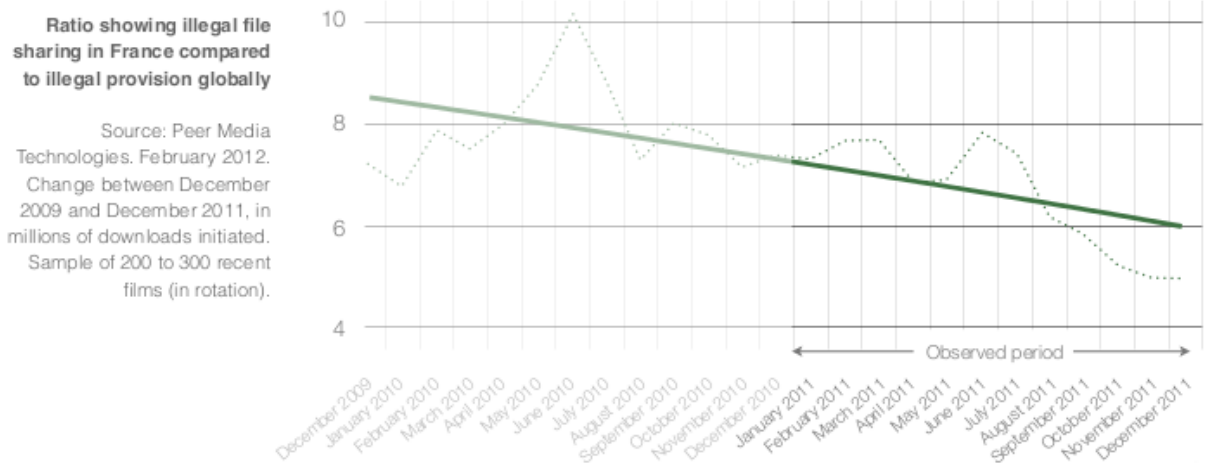


Figure 7.6: Peer Media Technologies study on illegal file sharing in France compared to the rest of the world.

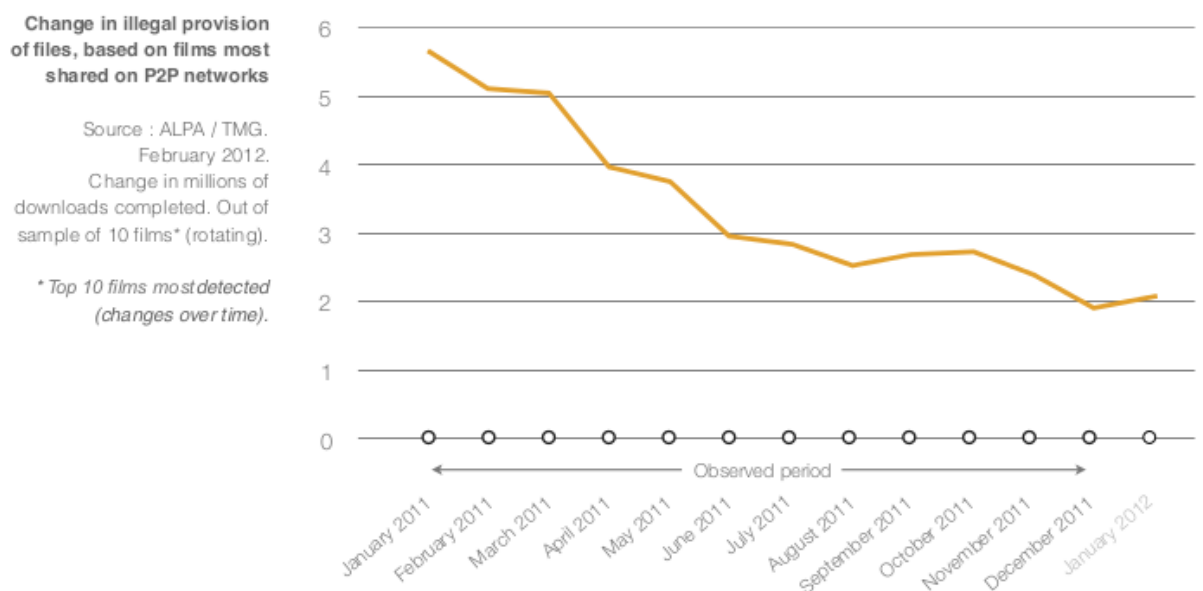


Figure 7.7: ALPA study on number of files shared on P2P networks.

With regard to the Nielsen study (a drop of 17%), Giblin pointed out that the study referred to the IFPI Digital Music Report 2012. However, that report actually claimed that the number of P2P file sharers dropped by 26 per cent.¹¹¹⁴ In its report for 2013, this number was back at 17%, but because in both cases no methodology was provided, it cannot be determined whether this is true.¹¹¹⁵

With regard to the second figure (a 29% reduction), by Médiamétrie/NetRatings, Giblin pointed out that this report or its methodology were not publicly available and could therefore not be verified. She did mention that both Médiamétrie/NetRatings and Nielsen used measuring software that can only be applied to users when they agree to have the software installed and their behavior tracked. Changes in behavior of users who know their behavior is being tracked are unlikely to be representative of the general population.¹¹¹⁶

¹¹¹⁴ Giblin, "Evaluating Graduated Response," P.181.

¹¹¹⁵ Giblin, "Evaluating Graduated Response," P.181.

¹¹¹⁶ Giblin, "Evaluating Graduated Response," P.181.

For the third study, Giblin pointed out that Peer Media Technologies was an anti-piracy company who was also unwilling to share its methodology, like ALPA, author of the fourth study. ALPA is the French MPAA, and had an interest in the outcome of this study, according to Giblin.¹¹¹⁷

The French website Numerama also pointed out that most of the HADOPI data was funded by rights holders, like the IFPI and ALPA (the French anti-piracy organization). This could also make those numbers less trustworthy. According to the website, this also explained why there was such a big discrepancy between them (a 17% decline of people using P2P versus a 66% decline).¹¹¹⁸

HADOPI further mentioned that surveys revealed that 1 out of 3 people in France said that HADOPI gave them a reason to consume cultural works through legal channels, and that 71% of all P2P users said that they would stop downloading illegal content if they received a warning by HADOPI.¹¹¹⁹

In its report HADOPI also cited a study by Mediametrie/NetRatings that file hosting and streaming had not had more visitors as a result of HADOPI.¹¹²⁰ HADOPI itself claimed there was “no indication” that there had been a massive transfer to other forms of file sharing.¹¹²¹

Another study done by the American Wessely college and the Carnegie Mellon University revealed that graduated response had led to a 22.5% increase in Apple’s iTunes song sales and a 25% increase in Apple’s iTunes album sales between 2009 and 2011, compared to countries without a graduated response procedure, like the UK, Italy, Spain, Germany and Belgium. They further supported their conclusions by looking at genres that were more popular on torrent sites (so genres that experienced high piracy levels). On torrent sites Hip hop music was more popular than classical music, and after the graduated response procedure was enacted, the sales of hip hop music on iTunes grew more rapidly. The authors claimed that this supported their view that graduated response had been an effective way to stimulate legal content. They also said this generated 14.8 million Euros for the French economy.¹¹²²

¹¹¹⁷ Giblin, "Evaluating Graduated Response," P.181-182.

¹¹¹⁸ Monica Horten, "Hadopi – has it massaged the numbers," *IPtegrity* (March 31, 2012), http://www.iptegrity.com/index.php/france/755-HADOPI-has-it-massaged-the-numbers_ and: Guillaume Champeau, "Hadopi affirme que le P2P est en baisse. Vraiment?," *Numerama* (March 27, 2012), <http://www.numerama.com/magazine/22146-HADOPI-affirme-que-le-p2p-est-en-baisse-vraiment.html>.

¹¹¹⁹ HADOPI, *HADOPI: 1.1/2 year after the launch* (2012) P.6.

¹¹²⁰ HADOPI, *HADOPI: 1.1/2 year after the launch* (2012) P.7.

¹¹²¹ HADOPI, *HADOPI: 1.1/2 year after the launch* (2012).

¹¹²² Brett Danaher, et al., "The effect of graduated response anti-piracy laws on music sales: evidence from an event study in France," *The Journal of Industrial Economics* 62.3 (2014): 541-553.

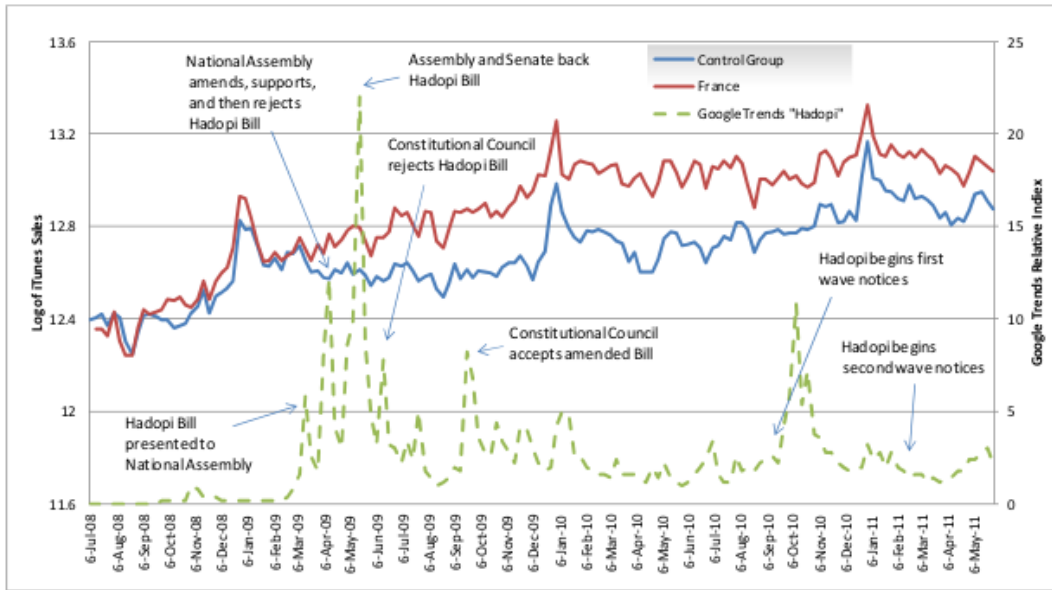


Figure 7.8: iTunes Single Track Unit Sales Trends (4 majors combines), France vs. Control. ¹¹²³

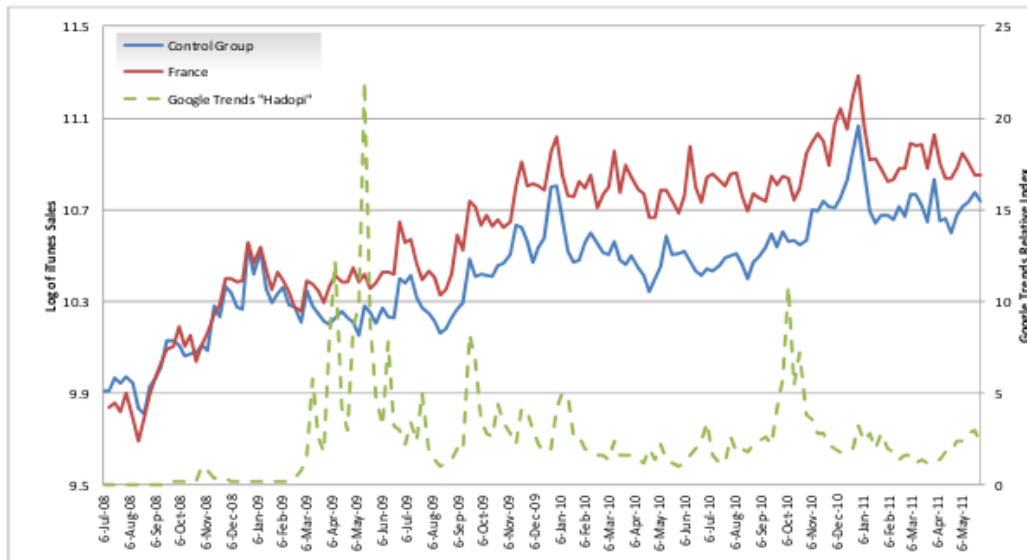


Figure 7.9: iTunes Single Track Unit Sales Trends (4 majors combines), France vs. Control. ¹¹²⁴

However, the French newspaper *le Monde* debunked this by using another Google trends search term. They looked at iPhone trends to see whether or not these trends could better explain the increased iTunes sales. They said that the peaks in sales better corresponded with other events: the launch of new iPhone models and the Christmas seasons. They also said that the effect was better visible because France had a lower starting base (the market in the UK for iTunes sales is much bigger, for example). The increase in specific genres was not, according to them, about which genres had more pirated content, but about young

¹¹²³ Image source: Danaher, et al., "The effect of graduated response anti-piracy laws on music sales."

¹¹²⁴ Image source: Danaher, et al., "The effect of graduated response anti-piracy laws on music sales."

people who were more generally inclined to use digital services and not listening to classical music.¹¹²⁵

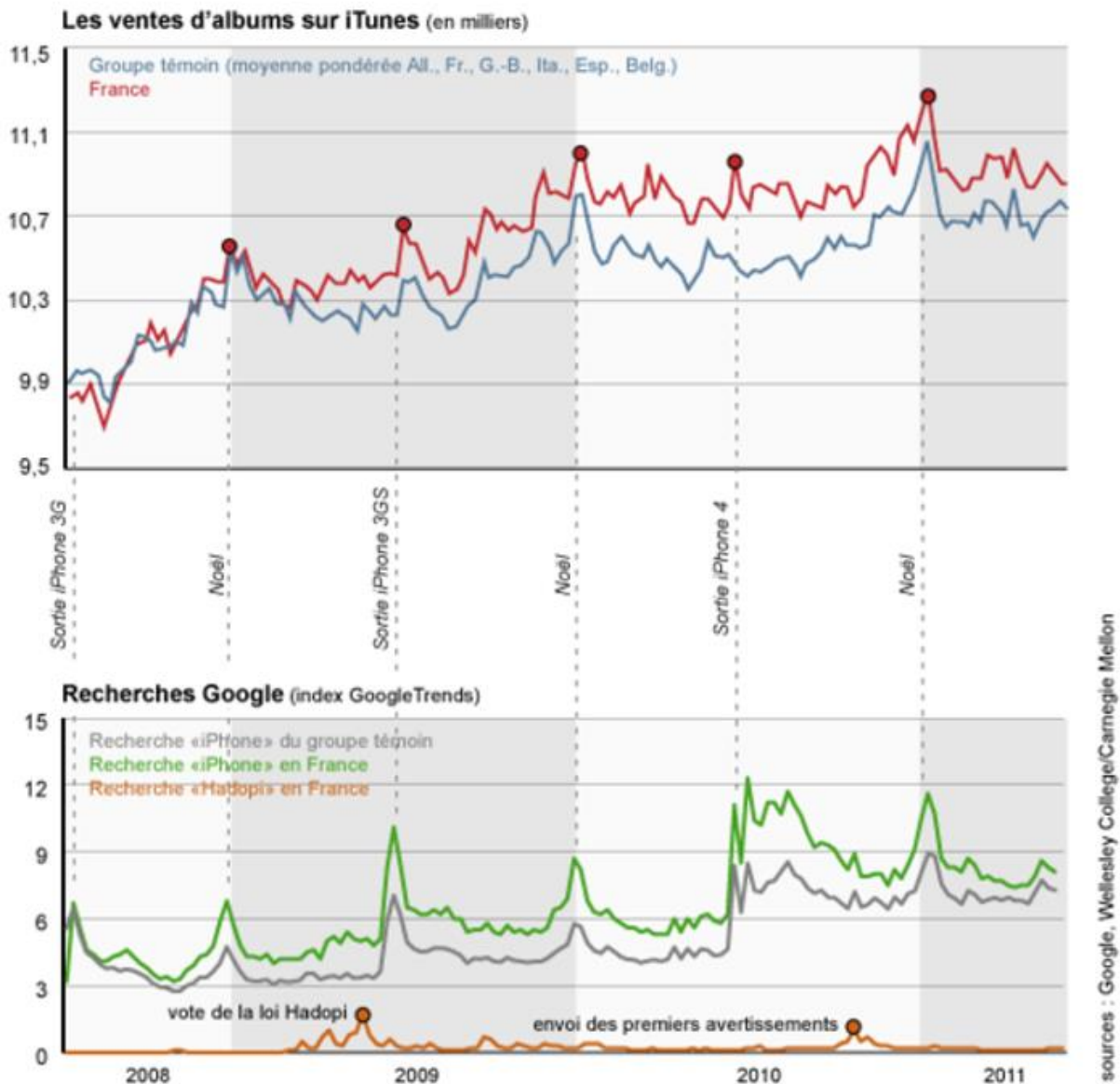


Figure 7.10: Le Monde study on iTunes sales compared to Google search trends.¹¹²⁶

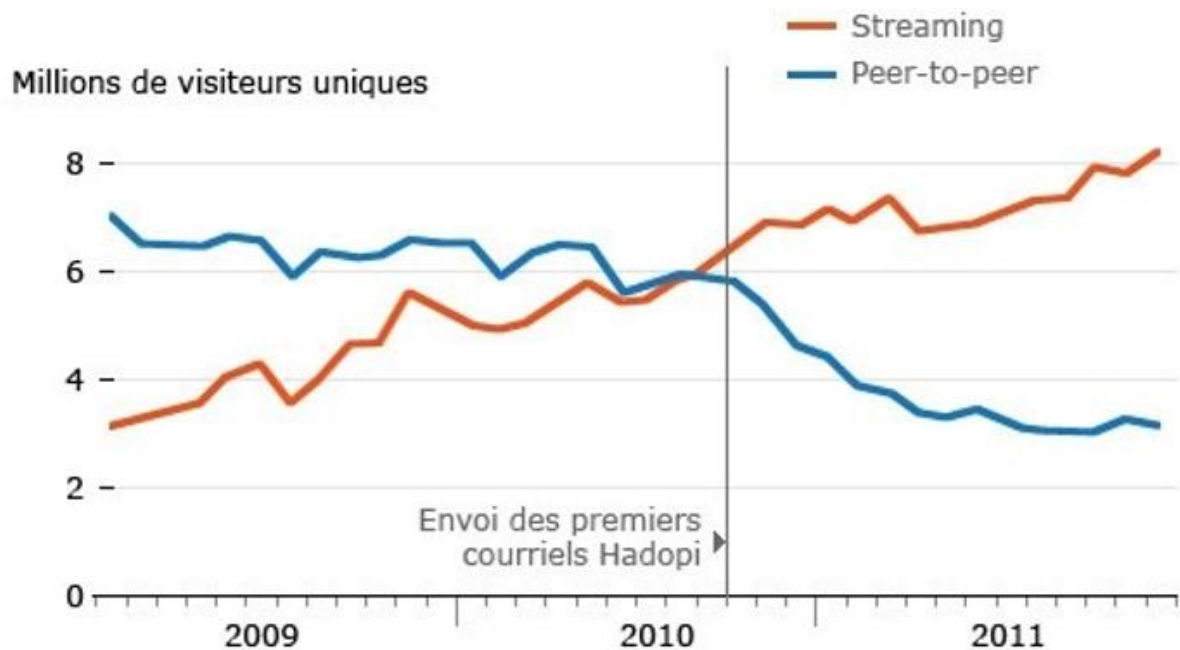
Torrentfreak looked into the research and claimed that the data seemed to be revealing something, but that the iTunes sales were already rising before the first warnings were sent out. Also, in the research, the researchers themselves claimed that after warnings were sent out the effect of that was close to zero.¹¹²⁷ The researchers said that consumers were more likely to have reacted to the media attention instead of the actual law. Torrentfreak also

¹¹²⁵ Damian Leloup and Jérémie Baruch, "Hadopi, source de la croissance d'iTunes?," *Le Monde* (January 1, 2012), http://www.lemonde.fr/technologies/article/2012/01/24/HADOPI-source-de-la-croissance-d-itunes_1633919_651865.html

¹¹²⁶ Image source: Damian Leloup and Jérémie Baruch, "Hadopi, source de la croissance d'iTunes?," *Le Monde* (January 1, 2012), http://www.lemonde.fr/technologies/article/2012/01/24/HADOPI-source-de-la-croissance-d-itunes_1633919_651865.html

¹¹²⁷ Page 16 of the report.

claimed that interest for sites like the Pirate bay remained the same, and suggested that the “buzz around Spotify” in the control group countries might have accounted for the difference in iTunes sales.¹¹²⁸



source : Panel Médiamétrie // NetRating
 (19 sites de streaming et de téléchargement direct
 face à 4 principaux services de peer-to-peer)

LE FIGARO.fr

Figure 7.11: Le Figaro study on streaming audiences compared to peer-to-peer.¹¹²⁹

An analysis done by Le Figaro (French Newspaper) showed that streaming traffic increased. IPtegrity said that this was confirmed “anecdotally” by a representative from France Telecom.¹¹³⁰ The operator said that the overall infringing traffic is still growing, but that P2P was a smaller percentage of that. France Telecom also experienced more encrypted traffic on its networks.¹¹³¹

Another point of criticism would be that the iTunes research looked only at music. The legal markets for video and books were still in development, so it was unclear what the

¹¹²⁸ Ernesto, “Anti-piracy warnings have no effect on iTunes sales,” *Torrentfreak* (January 24, 2012), <http://torrentfreak.com/anti-piracy-no-effect-on-itunes-sales-120124/>

¹¹²⁹ Image source: Benjamin Ferran, “Le bilan contrasté de l'action de l'Hadopi,” *le Figaro* (March 28, 2012), <http://www.lefigaro.fr/secteur/high-tech/2012/03/27/01007-20120327ARTFIG00670-le-bilan-contrastee-de-l-action-de-l-hadopi.php>

¹¹³⁰ Benjamin Ferran, “Le bilan contrasté de l'action de l'Hadopi,” *le Figaro* (March 28, 2012), <http://www.lefigaro.fr/secteur/high-tech/2012/03/27/01007-20120327ARTFIG00670-le-bilan-contrastee-de-l-action-de-l-hadopi.php>

¹¹³¹ Monica Horten, “Hadopi – has it massaged the numbers,” *IPtegrity* (March 31, 2012), <http://www.iptegrity.com/index.php/france/755-HADOPI-has-it-massaged-the-numbers>

effects were at that end.¹¹³² France was still one of the countries with the largest growing market share for BitTorrent.¹¹³³

In terms of ending infringement, other points of criticism on the effects of this procedure came from an interesting side: law enforcement agencies. During discussions on the Digital Economy Act and a possible graduated response procedure in the UK, British law enforcement agencies came out against the law, because they feared it would lead to more encryption, and make monitoring criminal behavior more difficult.¹¹³⁴ During the debates on the HADOPI, US intelligence agencies like the NSA supposedly did the same, expressing their concern that this might stimulate more encryption.¹¹³⁵

This is in line with what the Internet society predicted as a possible reaction to graduated response procedures. Users might shift to less traceable methods of access to content, or use encryption. Also, people might use other unsecured wireless networks. Another possibility would be that people would choose more closed private networks, or online anonymity solutions. One thing that was clear, when someone was blocked from the Internet, that access point could not be used anymore for infringement.¹¹³⁶

In 2013, critics argued that because the number that eventually reached the prosecutor was so low, and the costs so high, HADOPI had failed. However, according to HADOPI itself, those two did not have anything to do with each other. There was a gap between the first warning and the stage at the judge, and there can be many reasons for it, "but maybe they got the point." That so little cases reached the prosecutor could mean the 'education' part of HADOPI worked, according to HADOPI.¹¹³⁷

Giblin said that fewer notices on each strike could be accounted for by different reasons: there was a time lag between the first and second notices, which according to HADOPI's figures was five months. This could mean that users kept infringing for that period, and only received one second notice.¹¹³⁸ Also, HADOPI had certain time limitations, which could mean that every time a period expired, users received a new first notice again.¹¹³⁹ Furthermore, the number of allegations seemed to be much higher than the number of notices issued.¹¹⁴⁰

In 2013, more numbers came out. First of all, Kim Dotcom, the owner of what used to be Cyber locker Megaupload, launched a new service called Mega, and he claimed that France was the number 1 membership country. In a tweet he claimed France surpasses

¹¹³² Nathalie Falot, "Hadopi three years later: 1.15 million notices result in two convictions," *Future of Copyright* (December 31, 2012), <http://www.futureofcopyright.com/home/blog-post/2012/12/31/HADOPI-three-years-later-115-million-notices-result-in-two-convictions.html>.

¹¹³³ Billboard Staff, "Legimate Streaming Services Cut Down on Piracy, Report Suggests," *Billboardbiz* (October 3, 2012), <http://www.billboard.biz/bbbiz/industry/digital-and-mobile/bittorrent-share-shrinks-in-countries-that-1007966012.story>.

¹¹³⁴ Mike Masnick, "UK Law Enforcement Tells UK Gov't: Please Don't Kick File Sharers Offline," *Techdirt* (October 27, 2009), <http://www.techdirt.com/articles/20091027/0254326689.shtml>.

¹¹³⁵ Jared Moya, "NSA 'Yelled' at France Over 'Three-Strikes' Legislation," *ZeroPaid* (October 6, 2010), <http://www.zeropaid.com/news/90967/nsa-yelled-at-france-over-three-strikes-legislation/>.

¹¹³⁶ Internet Society, Perspectives on Policy Responses to Online Copyright Infringement, an Evolving Policy Landscape," Internet Society website (Feb 20, 2011) P.43-45, <http://www.Internetsociety.org/perspectives-policy-responses-online-copyright-infringement-evolving-policy-landscape>

¹¹³⁷ Sarah Jacquier (Legal Director of HADOPI) interviewed by author, January 2014.

¹¹³⁸ Giblin, "Evaluating Graduated Response," P.183.

¹¹³⁹ Giblin, "Evaluating Graduated Response," P.184.

¹¹⁴⁰ Giblin, "Evaluating Graduated Response," P.184.

Spain, Belgium, the US and Germany. This could indicate that French people were switching to other ways to share material.¹¹⁴¹

However, SNEP (Syndicat National de l'édition Phonographique) said that the number of visits to illegal music sites by French Internet users had continued to grow between the introduction of HADOPI and January 2013 by 7 percent to 10.7 million.¹¹⁴²

According to the IFPI, even until 2013, P2P file sharing had been dropping in France. They said that between the introduction of the law in 2010, and February 2013, unlicensed P2P file-sharing fell by 22 per cent.¹¹⁴³

However, this could also be attributed to a global declining trend in P2P file sharing. From 2011 to 2012, in the US, P2P music sharing fell by 17% in the U.S., long before its graduated response system started there.¹¹⁴⁴

Apart from the effects on infringement, some have looked at whether this stimulated the market for entertainment. The HADOPI report suggested that legal online market grew as a result of its activities.

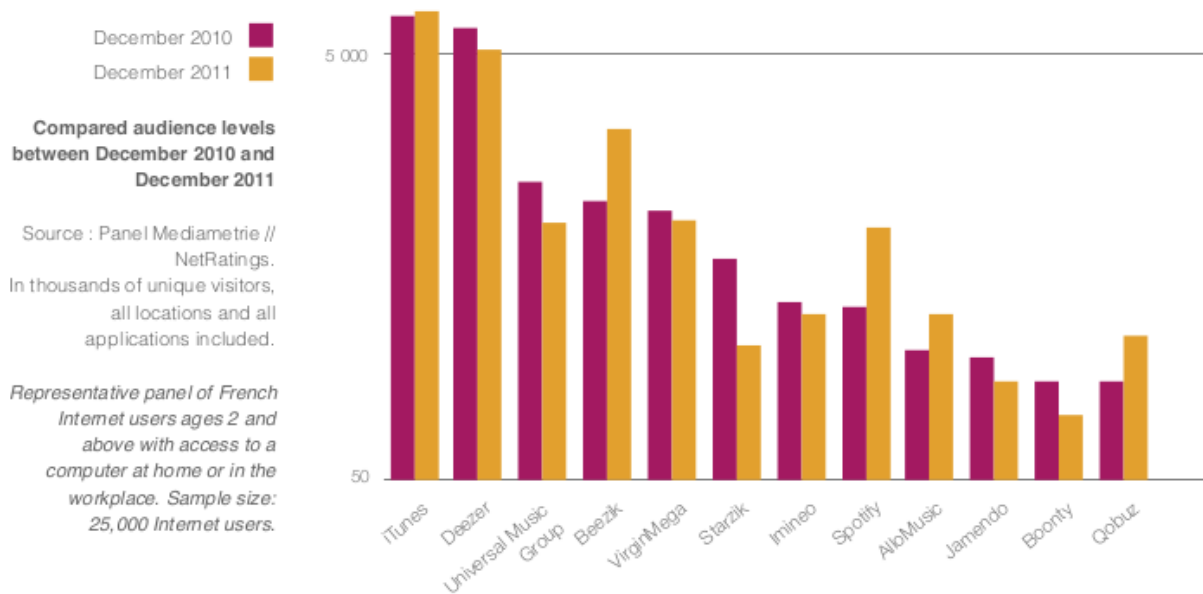


Figure 7.12: Médiametrie // NetRatings audience measurement in December 2010 and December 2011.¹¹⁴⁵

This also demonstrated the iTunes growth. However, looking at the data, the growth was not that big, and the places where it was big, Breezik and Spotify, were free services.

¹¹⁴¹ "Kim Dotcom," *Kim Dotcom Twitter* (March 28, 2015),

<https://twitter.com/KimDotcom/status/302739882323890176>, and: Julien L., "La France avec son Hadopi, 1er fournisseur de clients pour Mega," *Numerama* (February 16, 2013), <http://www.numerama.com/magazine/25117-la-france-avec-son-HADOPI-1er-fournisseur-de-clients-pour-mega.html>.

¹¹⁴² Eric Pfanner, "French Appear Ready to Soften Law on Media Piracy," *The New York Times* (June 2, 2013), http://www.nytimes.com/2013/06/03/technology/03iht-piracy03.html?_r=0.

¹¹⁴³ Ernesto, "Do "strikes" programs help to reduce piracy?," *Torrentfreak* (April 26, 2013), <https://torrentfreak.com/do-strikes-programs-help-to-reduce-piracy-130426/>.

¹¹⁴⁴ Lee Graham, "The NPD Group: Music File Sharing Declined Significantly in 2012," *NPD Group* (February 26, 2012), <https://www.npd.com/wps/portal/npd/us/news/press-releases/the-mpd-group-music-file-sharing-declined-significantly-in-2012/>.

¹¹⁴⁵ Image source: HADOPI, *HADOPI: 1.1/2 year after the launch* (2012) P.4-6.

Some commentators, like Torrentfreak, pointed out that in the HADOPI reports the one thing missing was the state of the entertainment industry in general, instead of just online.¹¹⁴⁶ Interestingly enough, the music industry still experienced a drop in revenues by 3.9% in 2011, although the digital market grew by 25%.¹¹⁴⁷ The video market dropped by 2.7%.¹¹⁴⁸

Regardless of the HADOPI procedure, other entertainment areas seemed to grow steadily. In the 'Sky is rising' report by the CCIA and floor64, they showed that live music revenues had gone up since 2007, and television revenues, game industry revenues, and the amount of books published since had grown steadily, without demonstrating a significant change in growth pattern during HADOPI's introduction or implementation.¹¹⁴⁹

Music sales however, continued to drop. SNEP (Syndicat National de l'édition Phonographique) produced its quarter results for the first period of 2013, and the wholesale market for recorded music dropped by 6,7%. In 2012, sales fell by 4,4%. Physical sales fell by 7,3%, and also digital sales went down, by 5,2%.

According to SNEP, this digital decline was attributable to circumstances (a label deal expired, and a YouTube agreement with rights group SACEM was suspended), and would otherwise have been stable (there had been a 12% growth in 2012).

Interestingly enough, France did not seem to perform better in the digital field than other countries that did not have a graduated response procedure. The digital content market in France remained stable around 29%, while the worldwide average remained at 35%.¹¹⁵⁰

According to Numerama, France was seeing a greater reduction in general sales than surrounding countries that had no graduated response scheme (Germany (- 4.6%), Italy (- 1.8%), the Netherlands (- 4.7%) and Great Britain (- 5.6%)).¹¹⁵¹

Finally, some authors pointed out there was a lot of variation in cited figures, which is relevant. Those numbers described decreases that range from 17 to 66 percent.¹¹⁵²

Another economic study suggested that the graduated response procedure did not affect the initial decision to engage in illegal file sharing, but that it may have reduced the intensity of file sharing by those who pirated. The study also suggested that people better informed about the law and piracy alternatives proceeded to pirate but through other channels.¹¹⁵³

¹¹⁴⁶ Ernesto, "French 'three strikes' law slashes piracy, but fails to boost sales," *Torrentfreak* (March 30, 2012), <http://torrentfreak.com/french-three-strikes-law-slashes-piracy-but-fails-to-boost-sales-120330/>.

¹¹⁴⁷ "French online music worth EUR 110 mln in 2011 – study," *Telecompaper* (January 31, 2012), <http://www.telecompaper.com/news/french-online-music-worth-eur-110-mln-in-2011-study--852719>.

¹¹⁴⁸ "France's 2011 physical media sales down 9%; VOD shot up 50%," *DVD and beyond* (February 13, 2012), <http://www.dvd-intelligence.com/display-article.php?article=1676>.

¹¹⁴⁹ Michael Masnick and Michael Ho, *The Sky is Rising, a detailed look at the state of the entertainment industry*, (Jan 2012), <https://www.techdirt.com/skyisrising/>

¹¹⁵⁰ Through the SNEP website: <http://www.actu.snepmusique.com/snep/>

¹¹⁵¹ Guillaume Champeau, "Hadopi : le vrai bilan négatif de la riposte graduée," *Numerama* (May 9, 2013), <http://www.numerama.com/magazine/25919-HADOPI-le-vrai-bilan-negatif-de-la-riposte-graduee.html>.

¹¹⁵² Geiger, "Challenges for the Enforcement of Copyright in the Online World," P.7.

¹¹⁵³ Michael Arnold et al. "Graduated response policy and the behavior of digital pirates: Evidence from the french three-strike (hadopi) law." Available at SSRN 2380522 (2014).

7.6 The costs of the system

When people cited the HADOPI procedure as a relatively cheap way to enforce copyrights, they meant cheap for rights holders.¹¹⁵⁴ The HADOPI system had costs itself that could be divided between the different parties: rights holders, the authority (the state), and access providers (third parties).

Rights holders required systems and in some cases agents that monitored Internet traffic to detect infringement, and notified the authority.¹¹⁵⁵ ISPs in turn needed systems to identify the subscribers and to send the infringement notices. It is unclear how much this exactly cost.¹¹⁵⁶ There were also judicial and administrative costs.¹¹⁵⁷

It is unclear what the costs were for rights holders to have TMG monitor the network. TMG unfortunately refused to speak to me. ALPA refused to comment on those costs, as they were a private contract.¹¹⁵⁸

HADOPI itself had 50 people working there and a specific budget which was gradually lowered (2011: 11,4 million Euros, 2012: 10,3 million Euros, 2013: 8 million Euros).¹¹⁵⁹ Those costs came from the state, which means the tax payers. The number of people working at HADOPI remained stable.¹¹⁶⁰ It seems the budget was slightly higher than planned, as the 2013 report talked about 10,5 million Euros.¹¹⁶¹

The costs for ISPs might have been higher, although it is not exactly clear what burden notice processing and sending was for ISPs. Those ISPs were not compensated by HADOPI, and according to HADOPI were “not happy” about this.¹¹⁶² At HADOPI’s inception they asked for compensation.¹¹⁶³ French website Numérama said it would cost around 8.5 Euros per IP lookup.¹¹⁶⁴ That could mean that more than 8 million was spend by ISPs alone. Those costs could have gone to the subscribers again. In fact, the French ISP ‘Free’ had

¹¹⁵⁴ Strowel, “The ‘Graduated Response’ in France,” P. 153.

¹¹⁵⁵ New Zealand Federation Against Copyright Theft, “Copyright (Infringing File Sharing) Regulations – Fee Review,” *Ministry for Economic Development* (2012) P.2, www.med.govt.nz/business/intellectual-property/pdf-docs-library/copyright/notice-process/illegal-peer-to-peer-file-sharing-submissions-on-fee-review-discussion/nzfact.pdf

¹¹⁵⁶ Internet Society, Perspectives on Policy Responses to Online Copyright Infringement, an Evolving Policy Landscape,” Internet Society website (Feb 20, 2011) P.23, <http://www.Internetsociety.org/perspectives-policy-responses-online-copyright-infringement-evolving-policy-landscape>

¹¹⁵⁷ Internet Society, Perspectives on Policy Responses to Online Copyright Infringement, an Evolving Policy Landscape,” Internet Society website (Feb 20, 2011) P.47, <http://www.Internetsociety.org/perspectives-policy-responses-online-copyright-infringement-evolving-policy-landscape>

¹¹⁵⁸ Frederic Delacroix (SFR) email to author, February 2014.

¹¹⁵⁹ République Française, *Annex au projet de loi de finances pour 2013, Rapport sur les Autorités publiques indépendantes*, 71-94.

¹¹⁶⁰ HADOPI, *Report Annuel 2013*, P.78.

¹¹⁶¹ HADOPI, *Report Annuel 2013*, P.85.

¹¹⁶² Sarah Jacquier (Legal Director of HADOPI) interviewed by author, January 2014.

¹¹⁶³ “French ISPs demand compensation for Hadopi cooperation,” *Telecompaper* (August 12, 2010), <http://www.telecompaper.com/news/french-isps-demand-compensation-for-HADOPI-cooperation--750964>.

¹¹⁶⁴ Guillaume Champeau, “Hadopi : le gouvernement refuse de payer la note,” *Numerama* (August 12, 2010), <http://www.numerama.com/magazine/16492-HADOPI-le-gouvernement-refuse-de-payer-la-note.html> and: Drew Wilson, “French Government and ISPs Negotiating Who Foots Approx. \$64 Million USD a Year HADOPI Bill,” *ZeroPaid* (August 12, 2010), <http://www.zeropaid.com/news/90268/french-government-and-isps-negotiating-who-foots-approx-64-million-usd-a-year-HADOPI-bill/>.

already increased its rates and blamed this increase on the HADOPI law.¹¹⁶⁵ ISPs also risked a fine if they do not identify IP addresses fast enough. They were expected to identify 150,000 a day, which was interesting because a US judge ruled that an ISP only had to identify 28 IP addresses per month, because of the immense workload connected to identification.¹¹⁶⁶

SFR, a large ISP, told me in an email that: “operators consider historically that the contribution to the graduated response is by nature alien to the main business of the operators. The service provided by operators to the benefit of HADOPI varies with the operator specific internal organization, its network infrastructure, its information systems, etc. These parameters vary for each operator and same goes for the resulting costs. So there is not a common market price at all as implied by Numérama.”¹¹⁶⁷

In the UK, during discussions on the graduated response procedure, ISPs claimed the costs would be high.¹¹⁶⁸ ISP BT claimed that it could cost 1 million pounds a day, which would add 24 pounds to each phone bill.¹¹⁶⁹ A UK government report claimed that it would cost even more than that (500 million pounds instead of 365 million pounds).¹¹⁷⁰ BPI countered these claims by commissioning a report from ‘Sweet Consulting’, which claimed that measures to identify, and notify copyright infringers would cost 13.85 million pounds in the first year, 9 million pounds in the second year and 3.45 million pounds in the third year. A report by the Creative coalition suggested 8.5 million pounds.¹¹⁷¹ In New Zealand, ISPs argued that the costs would be between 30 and 37 per notice.¹¹⁷²

During the debates on HADOPI, some estimated the total costs at around 50 million Euros.¹¹⁷³

Another potential cost that could be taken into account is that subscribers could be forced to pay by installing means to secure their connections.

These costs were an important factor. The Lescure report mentioned this too: “the focus of public funds on the prevention of P2P downloading is the result of a bad prioritization and an inadequate allocation of resources” and concluded “that it does not appear desirable to maintain an independent administrative authority whose activity is limited to combating illegal downloading. This would contribute neither to the lawfulness of

¹¹⁶⁵ Drew Wilson, “HADOPI Blamed for ISP Rate Hikes in France,” *ZeroPaid* (January 1, 2011), http://www.zeropaid.com/news/91800/HADOPI-blamed-for-isp-rate-hikes-in-france/?utm_source=twitterfeed&utm_medium=twitter.

¹¹⁶⁶ Ernesto, “France starts reporting ‘millions’ of file-sharers,” *Torrentfreak* (September 21, 2010), <http://torrentfreak.com/france-starts-reporting-millions-of-file-sharers-100921/>.

¹¹⁶⁷ Frédéric Dejonckheere (SFR) email to author, March 2014.

¹¹⁶⁸ Mike Masnick, “BPI Insists UK ISPs Overstating The Cost Of Three Strikes; So Will BPI Pay The Difference If Wrong?,” *Techdirt* (January 21, 2010), <http://www.techdirt.com/articles/20100120/1937547848.shtml>.

¹¹⁶⁹ Clinton Manning, “Internet piracy policing could add £24 to every phone bill,” *Mirror* (February 3, 2012), <http://www.mirror.co.uk/money/city-news/Internet-piracy-policing-could-add-420183>.

¹¹⁷⁰ Mike Masnick, “UK Government Report Shows That Digital Economy Bill Will Cost More Than Highest ‘Piracy’ Estimates, Drive 40,000 Offline,” *Techdirt* (December 28, 2009), <http://www.techdirt.com/articles/20091228/0335197514.shtml>.

¹¹⁷¹ Mark Sweney, “Illegal downloads: music industry to carry cost of catching pirates”, *the Guardian* (Sept 14, 2010), <http://www.theguardian.com/technology/2010/sep/14/illegal-downloads-music-industry>

¹¹⁷² Juha Saarinen, “Kiwis put a price on copyright notices: \$23,” *ITnews* (September 29, 2010), <http://www.itnews.com.au/News/233676,kiwis-put-a-price-on-copyright-notices-23.aspx>.

¹¹⁷³ Drew Wilson, “French Government and ISPs Negotiating Who Foots Approx. \$64 Million USD a Year HADOPI Bill,” *ZeroPaid* (August 12, 2010), <http://www.zeropaid.com/news/90268/french-government-and-isps-negotiating-who-foots-approx-64-million-usd-a-year-HADOPI-bill>.

the provision, nor to the coherence of state activity, nor to the saving of public funds.”¹¹⁷⁴
This was especially pressing as the system only marginally benefits authors, according to some.¹¹⁷⁵

7.7 Conclusion

With the help of tech firms, allegedly infringing users were identified to HADOPI, a public authority that aimed to stop infringement. The procedure consisted of three phases which have been evaluated as subcases. The HADOPI authority sent warning letters to those infringing users, with the help of ISPs. After two warning letters, it launched an investigation, which could be forwarded to the attorney general, who could initiate a criminal trial, which could lead to internet disconnection or a fine.

Millions of people received a first warning (subcase 1). Hundreds of thousands a second one (subcase 2). Only 51 people went to trial after the third phase (subcase 3). Regarding severity, warnings were sent, and the resulting penalty after the third phase was supposed to be disconnection. However, the final penalties have been fines between 50 and 600 Euros.

Regarding privacy, infringement was only found through over the top surveillance: by joining P2P networks. Although there was a rights protection committee that administered the warning phase, accusations were hardly checked for accuracy. Users were further found to be infringing by negligence, which also undermined the presumption of innocence. In the eventual trial, there was an impartial, competent and independent judge. The warning was a first notice but it already had consequences. There was a right to be heard and appeal after this notice, but it was unclear how well these defenses were evaluated by the rights protection committee, considering their sheer number. Transparency happened through public reports, although it is unclear how HADOPI applied the law. Regarding proportionality, the disconnection penalty was eventually removed in favor of smaller fines.

There has been debate on its impact on file sharing. Some have argued that it is effective. Although the amount of notices declined in the later phases, some argued that this was due to external circumstances. Also, file sharing through other channels rose. The case showed that the procedure was expensive, with tax payers and ISPs carrying costs, but cheaper for rights holders. These outcomes will be highlighted again in the conclusion and compared with the outcomes of the other cases.

¹¹⁷⁴ Pierre Lescure, *Mission « Acte II de l'exception culturelle » Contribution aux politiques culturelles à l'ère numérique*, Ministère de la Culture et de la Communication (May 2013) P.33,

www.culturecommunication.gouv.fr/var/culture/storage/culture_mag/rapport_lescurer/index.htm#/1

¹¹⁷⁵ Geiger, “Challenges for the Enforcement of Copyright in the Online World,” P.10.

8. THE EIRCOM GRADUATED RESPONSE PROCEDURE (IRELAND) IN 2010-2013

8.1 Introduction

In June 2010, Irish internet provider Eircom launched a graduated response procedure. This created a multiple strikes system for copyright enforcement. Rights holders would find infringement and report this to Eircom. Eircom would then send warnings to users connected to the infringing IP addresses. If infringement happened again, a new warning would be sent. After two warnings, the internet connection of the infringing user could be suspended for 7 days. After that, another infringement could lead to a longer suspension of up to 12 months. For the evaluation of performance on the variables, the case has been divided into 4 subcases, which are different phases in the procedure (warning 1, warning 2, 7-day suspension and 12-month suspension).

This chapter will first provide the legal background to this procedure. In this section I also describe the legislative history, because it is relevant to the variables. For this, I used legal sources and academic literature, but mostly case law. Some news articles have been used for the legislative history. After that, the chapter describes the procedure in practice. For this, I relied on legal sources, but also on official statements by Eircom. I also included the perspective of practitioners. For this case study, I interviewed the Irish Recorded Music Association (IRMA). I tried interviewing the Irish Data Protection Officer, but as they were involved in a court case directly relating to the subject, they decided not to participate. I also approached the ISP Eircom, but they did not want to go into specifics, and I had contact with Digital Rights Ireland. I also spoke to UPC, another ISP, at the time under pressure for not similarly implementing a graduated response procedure.

In addition to the interviews, I included news articles, academic research and reports by NGOs on the graduated response procedure. The Irish journalist Mark Tighe has put a lot of information on his blog.¹¹⁷⁶ He reported on a meeting in December 2011, where Willie Kavanagh, the chief executive of EMI Ireland, met with minister Sherlock to give details on how the graduated response has worked so far. There was a memo of this meeting.¹¹⁷⁷ Tighe also mentioned a meeting preceding the legislative adjustment, on 14 September 2011, at the telecommunications & Internet federation (TIF).¹¹⁷⁸ Present at that meeting were Minister Sherlock, Pat Galvin (Eircom, but also TIF), Gary Healy (Eircom), Kate O'Sullivan (UPC), Ian Barry (3), Michael Maher (VF), Emer Condon (TIF), Brian McCabe and Florence Kelly (DJEI). Information for this case study has been collected from January 2012 until January 2014.

¹¹⁷⁶ Mark Tighe, "Eircoms 3 strikes scheme," *The blog of an Irish Journalist* (March 2012), <http://irishjournalist.blogspot.nl/2012/03/eircoms-3-strikes-scheme.html>

¹¹⁷⁷ "Note of Minister Sherlock's meeting with the Irish Recorded Music Association on Monday 5th December 2011," available on Scribd: <http://www.scribd.com/doc/83984745/EMI-Briefing-001>

¹¹⁷⁸ Mark Tighe, "Eircoms 3 strikes scheme."

8.2 Legal background

With 2.6 million users in 2010,¹¹⁷⁹ former state owned monopolist Eircom was the largest telecommunications operator in the Irish Republic. Its main competitors were UPC Ireland, Vodafone Ireland, Imagine Communications, and Magnet Networks and Smart Telecom. At the time, Eircom had implemented a privately administered graduated response procedure, following developments that started in 2005.

In that year, the Irish High Court decided a case filed by the entertainment industries (EMI – Ireland, Sony Music, Universal, Warner) against Eircom and BT Communications Ireland. It said that ISPs must disclose subscriber data in copyright infringement cases.¹¹⁸⁰

The judge first considered the principle that even if a person does not facilitate a “wrongdoing,” that does not take away a duty to assist a person who has been wronged by giving full information and disclosing the identity of the wrongdoers. This is called a Norwich Pharmacal Order. “They require disclosure of identity and other information held by a third party concerning an alleged wrongdoer to the wronged person.” However, the court also repeated the principle that these orders should be confined to cases where clear proof of wrongdoing exists, and to cases in which names and identities are sought, instead of the factual information concerning the commission of the wrong. This applies especially to cases where discovery is sought instead of proceedings started. The court also cited a Canadian federal court of appeal decision in which it is said that “this technology (FK: the Internet) must not be allowed to obliterate those personal property rights which society has deemed important. Although privacy concerns must also be considered, it seems to me that they must yield to public concerns for the protection of intellectual property rights in situations where infringement threatens to erode those rights.” But the judge also said that “caution must be exercised by the courts in ordering such disclosure to make sure that privacy rights are invaded in the most minimal way.”

In the case, the plaintiffs sought the names and addresses of 17 of the subscribers of the defendants. The judge considered the evidence put forward by the parties valid and said that the record industries could make clear what IP addresses had been infringing, and why they needed the help of ISPs to determine which subscribers fit those IP addresses. The court said: “I am satisfied that whether the right to confidentiality arises by statute or by contract or at common law, it cannot be relied on by a wrongdoer or a person against whom there is evidence of wrongdoing to protect his or her identity. The right to privacy or confidentiality of identity must give way where there is prima facie evidence of wrongdoing. There is such evidence here.”

The judge therefore decided that this information could be given to the plaintiffs, but could not be made public, and could only be used to seek redress for copyright infringement.¹¹⁸¹

EMI, Sony, Universal, and Warner sued Eircom again in 2008, asking to get the operator to block access to the Pirate Bay website. The judge considered it proven that the Pirate Bay was dedicated to infringement, and that this situation undermined the intellectual property rights assigned to the plaintiffs, calling the unrestrained copying over the Internet allowed by the Pirate Bay “theft.”

¹¹⁷⁹ John Collins, “Three strikes rule aims to knock out music sharing,” *Irish Times* (June 4, 2010), and: Bridy, “Graduated Response American Style,” P. 24.

¹¹⁸⁰ EMI Records (Ireland) Ltd & Ors v. Eircom Ltd & Anor [2005] IEHC 233 (8 July 2005)

¹¹⁸¹ EMI Records (Ireland) Ltd & Ors v. Eircom Ltd & Anor [2005] IEHC 233 (8 July 2005)

The judge did consider Eircom an “innocent transmitter of infringing material” as named in s.40(4) of the copyright and related acts of 2000. This article read: “(4) Without prejudice to subsection (3), where a person who provides facilities referred to in that subsection is notified by the owner of the copyright in the work concerned that those facilities are being used to infringe the copyright in that work and that person fails to remove that infringing material as soon as practicable thereafter that person shall also be liable for the infringement.”

The judge added: “I interpret that, at the moment, as saying that the pipe or channel (i.e. the electronic pipe or channel in this case) down which the copyright infringing material is going can be the subject of injunctive relief under s. 40(4). This section is derived according to the long title of the 2000 Act as amended in 2007 from the relevant EU Directive, and is to be interpreted in conformity with it. In its original form, that Directive is Council Directive 2001/29 EC of the 22nd May, 2001, on the harmonization of certain aspects of copyright and related rights in the information society with recitals to which I have regard and the relevant article reads (...) 3. Member States shall ensure that right holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.”

The judge said that although Eircom was ‘innocent’, it was a party whose facilities were being used so that their publicly available channels for the transmission of material over the Internet (electronic pipes) were used for infringement, and therefore could be made subject of an injunctive order.

As a final decision, the judge did not award damages, but ordered Eircom to “block or otherwise disable access by its Internet subscribers to the website - thePirateBay.org and related domain names, as set out in the schedule, to IP addresses and URLs, as set out in the schedule, together with such other domain names, IP addresses and URLs as may reasonably be notified as related domain names by the plaintiffs to the defendant from time to time.”

But the record companies wanted ISPs to take more responsibility. “We wanted the ISPs to sort out the problem. Between 2005 and 2008, every national group wanted to do individual lawsuits, they were painful, totally worthless, and a waste of time and resources, and they didn’t sit well with average consumers.”¹¹⁸²

Therefore, on 21 April 2008, four major record companies claimed that Eircom should bear some responsibility for copyright infringement. IFPI sued as well. On 28th January 2009, IRMA settled with Eircom, but under the condition that Eircom would implement a graduated response scheme. The data protection commissioner feared that this procedure would violate the privacy of Eircom’s users, and went to court with a number of complaints. As a result, this scheme was evaluated by the High Court to see whether it was compatible with data protection laws (data protection acts 1988 and 2003).¹¹⁸³

In short, the judge ruled that it seemed unlikely that personal data would be at risk here, that the protection of copyright was a legitimate aim to pursue, and that the procedure was a civil law one (as opposed to criminal law) and did not require a hearing. The judge therefore considered the protocol lawful.

Interestingly enough, when the Irish music federation tried to sue other ISPs to get them to implement a similar scheme, the Irish High Court held that it lacked the power to

¹¹⁸² Dick Doyle (IRMA) interviewed by author, November 2013.

¹¹⁸³ EMI Records v. Eircom Ltd., [2010] IEHC 108, ¶ 1 (H. Ct.) (Ir.) and: “Ireland Cracks Down on Internet Piracy,” *Independent* (May 29, 2010), <http://www.independent.co.uk/news/media/ireland-cracks-down-on-Internet-piracy-1986733.html>

force such a scheme upon other ISPs (based on the separation of powers), because it lacked a legal provision to do so (although the court considered it “merited on the facts”).¹¹⁸⁴

UPC was first approached (market share of about 15%).¹¹⁸⁵ From the court case, it seems that the judge would have gladly ordered UPC to implement a similar scheme as Eircom. In the court case, the judge expressed his discontent with UPC’s attitude. It quoted conversations (emails) from which it concluded that even though UPC had provisions that show they could stop illegal activity, it did nothing. The court ignored the points claimed by UPC that detection and termination of illegal activity would be costly in light of the earlier evidence above. In fact, the judge said the systems were already there, but simply never used.¹¹⁸⁶

However, the court underlined how important the separation of powers was, especially the respect for the rule of law. It therefore looked to the precise scope of the legislative framework as set out by the copyright act and how EU law might be used to interpret national law.¹¹⁸⁷

It accepted that UPC was a mere conduit, and that the Notice and takedown rules did not apply.¹¹⁸⁸ However, recital 45 of the E-commerce directive allowed for injunctions: “The limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it.”

Unfortunately for the recording industries, the Irish copyright act only referred to removal.¹¹⁸⁹ The EU directive did leave the door open for injunctive relief against parties exempted, but the state had to enforce this.¹¹⁹⁰ The court then went into measures in other states to end piracy. All seemed to share a court ordered disconnection.¹¹⁹¹

The court said that because Ireland lacked such a provision “to prevent infringement by subscribers” it was not complying with EU law (in particular, with article 8(3) of EU Directive 2001/29/EC, which requires injunctive relief to be available against an intermediary to prevent infringement.)

Soon after, Eircom issued a press release stating that it would still continue to perform the scheme as agreed to in the settlement agreement.¹¹⁹²

¹¹⁸⁴ EMI Records (Ireland) Ltd & Ors –v- UPC Communications Ireland Ltd (2010) IEHC 377 (10 november 2010). ¶138

¹¹⁸⁵ EMI Records (Ireland) Ltd & Ors –v- UPC Communications Ireland Ltd (2010) IEHC 377 (10 november 2010). ¶3

¹¹⁸⁶ EMI Records (Ireland) Ltd & Ors –v- UPC Communications Ireland Ltd (2010) IEHC 377 (10 november 2010). ¶50-57

¹¹⁸⁷ EMI Records (Ireland) Ltd & Ors –v- UPC Communications Ireland Ltd (2010) IEHC 377 (10 november 2010). ¶85

¹¹⁸⁸ EMI Records (Ireland) Ltd & Ors –v- UPC Communications Ireland Ltd (2010) IEHC 377 (10 november 2010). ¶97-100

¹¹⁸⁹ EMI Records (Ireland) Ltd & Ors –v- UPC Communications Ireland Ltd (2010) IEHC 377 (10 november 2010). ¶109-110

¹¹⁹⁰ EMI Records (Ireland) Ltd & Ors –v- UPC Communications Ireland Ltd (2010) IEHC 377 (10 november 2010). ¶111-116

¹¹⁹¹ EMI Records (Ireland) Ltd & Ors –v- UPC Communications Ireland Ltd (2010) IEHC 377 (10 november 2010). ¶119-130

¹¹⁹² "Eircom Statement on Illegal File Sharing," *Press release on Eircom website* (Dec 8, 2010), [http://pressroom.eircom.net/press_releases/article/eircom Statement on Illegal File Sharing/](http://pressroom.eircom.net/press_releases/article/eircom%20Statement%20on%20Illegal%20File%20Sharing/)

Afterwards, the Irish government introduced amendments to the copyright and related rights act 2000, to fully implement article 8(3) of the EU directive. Eventually, on 29 February 2012, this statutory instrument (S.I. No. 59 of 2012) was passed into law.¹¹⁹³ This allowed rights holders to file injunctions to service providers. When I spoke to them, an IRMA spokesman said that they were “in a process that may result in litigation against other ISPs.”¹¹⁹⁴

At the end of 2011, the Commissioner took action again, and performed a six-month investigation of consumer complaints after an incident in which 390 subscribers were wrongly identified as infringers. According to Eircom this was the result of a “minor technical issue.”¹¹⁹⁵

Following this investigation, the Irish Data Protection Commissioner directed Eircom to stop its graduated response procedure, citing violations of data protection rules. In an enforcement notice following this investigation, the Commissioner accused Eircom of: facilitating Internet traffic surveillance of users without their consent, improperly retaining and using data linking subscriber identities to IP addresses, and failing to ensure the accuracy of that data.¹¹⁹⁶ The record companies party to the settlement immediately filed for judicial review.¹¹⁹⁷

The problem in the case before the High Court was the following: On Sunday 28 March 2010 all clocks went forward 1 hour at 1:00 for summer time, on Sunday 31 October 2010 all clocks in Ireland and Europe went back one hour at 2.00 hours for winter time. Eircom ignored the winter time change which caused problems.¹¹⁹⁸

In the case, the Court recognized that it should exercise some restraint when evaluating the decision by a competent body.¹¹⁹⁹ However, it immediately noted that most of the issues raised by the Data protection commissioner were already tackled in the earlier case on the settlement, and that the “mere fact” that the clocks were mistakenly not adjusted, did not make it “fair or legally right” to make them cease operation. In other words, the Court thought the DPC notice did not contain enough reasons¹²⁰⁰ and declared it invalid.¹²⁰¹

A complicating issue was the question to what extent the record companies could file for judicial review in this case, since this was about a decision filed against Eircom by the data protection officer. The judge thought it was legal for record companies to ask for judicial review. They were interested parties, as it affected their economic interests in a substantial way.¹²⁰²

¹¹⁹³ "Statutory Instruments, S.I. No. 59 of 2012," *Irish Statute Book*, <http://www.irishstatutebook.ie/pdf/2012/en.si.2012.0059.pdf>

¹¹⁹⁴ Dick Doyle (IRMA) interviewed by author, November 2013.

¹¹⁹⁵ Mary Carolan, “Four Music Firms Dispute Data Chief’s Notice to Eircom,” *Irish Times* (March 1, 2012). P. 4. see also *EMI Records v. Data Protection Commissioner*, [2012] IEHC 264, ¶¶ 1.0, 1.3 (explaining that Eircom changed the clocks in its network to reflect daylight savings time two months late, thereby causing a mismatch between dynamically assigned IP addresses and subscriber accounts, which led to the delivery of erroneous notices of infringement), and: Bridy, “Graduated Response American Style,” P.26.

¹¹⁹⁶ Bridy, “Graduated Response American Style,” P.26

¹¹⁹⁷ *EMI Records (Ireland Ltd v Data Protection Commissioner)* (2012) IEHC 264.

¹¹⁹⁸ *EMI Records (Ireland Ltd v Data Protection Commissioner)* (2012) IEHC 264, ¶1.0

¹¹⁹⁹ *EMI Records (Ireland Ltd v Data Protection Commissioner)* (2012) IEHC 264, ¶5.0-5.2

¹²⁰⁰ *EMI Records (Ireland Ltd v Data Protection Commissioner)* (2012) IEHC 264, ¶11.1-11.4

¹²⁰¹ *EMI Records (Ireland Ltd v Data Protection Commissioner)* (2012) IEHC 264, ¶14.0-14.1

¹²⁰² *EMI Records (Ireland Ltd v Data Protection Commissioner)* (2012) IEHC 264, ¶12.0-12.4

The data protection commissioner appealed, but the Supreme Court upheld the ruling of the high court, ruling Eircom's settlement in accordance with Data Protection laws.¹²⁰³ When Eircom issued the statement that it would continue its graduated response system, it also launched the MusicHub service, which offered legal downloads and streaming.¹²⁰⁴ However, IRMA revealed that MusicHub stopped as it could not compete with other legal distribution channels like iTunes.¹²⁰⁵

The legal basis for the Graduated response lies in the court cases discussed above and in a contractual arrangement among private parties.¹²⁰⁶ It was the result of a settlement, before the Irish court could judge on the matter. This is relevant, because there are no copyright laws mandating this system. When IRMA tried to force another Irish ISP, UPC, to implement a graduated response regime,¹²⁰⁷ the Court refused to order UPC to implement a similar one, saying that it was a matter of contract. Even though this was based on contract, it had similar workings as public law because it applied to so many users.¹²⁰⁸

8.3 The procedure in practice

Although the protocol was confidential,¹²⁰⁹ much about the process could be distilled from the court case in which the High Court reviewed the settlement protocol, and by statements made by different players involved.

On Eircom's website a 'FAQ' made clear that one of the purposes was to educate:

- "informing customers of the issues;
- providing assistance to customers on how to prevent illegal music downloading & sharing;
- helping customers identify legitimate music services."¹²¹⁰

Subscribers agreed to this system through their subscriber contract. In the agreement, clause 5.6 said that the customer had to agree not to use the Internet access to infringe the proprietary rights of any software, clause 5.10 says that the customer had to agree with the acceptable usage policy posted on www.eircom.net, and 5.5 said that "Customers may not use the facility to create, host or transmit material which infringes the intellectual property rights including, but not limited to, the copyright of another person or organization."¹²¹¹ Clause 7.1 said that the agreement could be suspended or terminated by Eircom for breach of its terms.¹²¹²

¹²⁰³ William Fry, "3 strikes - Supreme Court rejects Data Protection Commissioner's appeal, *Lexology* (July 24, 2013), <http://www.lexology.com/library/detail.aspx?g=33062c2f-205a-471a-a8ef-ef0cae5e7c0d>

¹²⁰⁴ Music Ally, "Eircom launches MusicHub service and reveals graduated response policy," *Musically* (Dec 9, 2010), <http://musically.com/2010/12/09/eircom-launches-musichub-service-and-reveals-graduated-response-policy/>

¹²⁰⁵ Dick Doyle (IRMA) interviewed by author, November 2013.

¹²⁰⁶ EMI Records v. Eircom Ltd., [2010] IEHC 108, ¶ 1 (H. Ct.) (Ir.); and: "Ireland Cracks Down on Internet Piracy," *The Independent* (May 29, 2010), <http://www.independent.co.uk/news/media/ireland-cracks-down-on-internet-piracy-1986733.html>.

¹²⁰⁷ EMI Records v. UPC Communications, [2010] IEHC 377 (H. Ct.) (Ir.).

¹²⁰⁸ John Collins, "Three strikes rule aims to knock out music sharing," *Irish Times* (June 4, 2010), and: Bridy, "Graduated Response American Style," P.24.

¹²⁰⁹ "Eircom Statement on Illegal File Sharing," *Press release on Eircom website*.

¹²¹⁰ "Legal Music, Frequently Asked Questions," *Eircom website*, <http://www.eircom.net/notification/legalmusic/faqs/> Last viewed on March 3, 2013.

¹²¹¹ EMI Records v. Eircom Ltd., [2010] IEHC 108, ¶ 14.

¹²¹² EMI Records v. Eircom Ltd., [2010] IEHC 108, ¶ 15.

The recording industry was responsible for making infringement allegations. They used an independent technology company called DtecNet as a private detective to monitor P2P networks.¹²¹³ They would then communicate the infringement allocations to IRMA.

IRMA would then provide Eircom with notifications “which will contain among other details, the IP address identified as engaging in illegal music file sharing in breach of copyright along with evidence of the infringement. The IP addresses have been captured in accordance with relevant laws and processed on IRMA's behalf via a third party.”¹²¹⁴ The communication by IRMA to Eircom that there had been infringement would be subject to requirements: “details of the copyright holder (which could be, for example, a particular songwriter); that a breach of copyright has occurred; details of the relevant album or song or video; the IP address that has been detected in infringing copyright; and other details that show proper investigation, namely, the relevant software used and the digital fingerprint of the copyright material used.”¹²¹⁵

After the first infringement, subscribers would be notified with their bill that infringement was detected by IRMA, in connection with a particular copyright protected work at such and such a time linked to their IP address.¹²¹⁶ Eircom would then tell the subscriber that such acts were illegal and in breach of the terms and conditions of broadband service, and Eircom would provide information as to how the customer could avoid repeating the infringement.¹²¹⁷

After the second infringement Eircom would send a formal letter with stronger words. This could only happen when 14 days have passed since infringement 1.¹²¹⁸ This letter would also state that further infringement would result in disconnection.¹²¹⁹

If another notification was received after 14 days, Eircom would review the evidence. This was done by humans (but first two levels were automatic). After evaluation, a termination notice was sent giving 14 days before cut-off. A customer could make representations to Eircom, over the telephone or through the Internet. Eircom would review these claims (under paragraph 2.8 of the protocol), which could call for exceptions, or that the infringement had not taken place at all¹²²⁰ (however, this last step was not mentioned on Eircom’s website, or anywhere else).¹²²¹ Eircom would then proceed to withdraw the customer's broadband service for a period of 7 days.¹²²²

The customer would also be informed that should they continue to engage in file sharing of music in breach of copyright and a further notification of infringement was

¹²¹³ John Collins, “Eircom to cut broadband over illegal downloads,” *Irish Times*, (May 24, 2010) <http://www.irishtimes.com/newspaper/frontpage/2010/0524/1224271013389.html>

¹²¹⁴ “Eircom Statement on Illegal File Sharing,” *Press release on Eircom website*, and Bridy, “Graduated Response American Style,” P.24, and: *EMI Records v. Eircom Ltd.*, [2010] IEHC 108, ¶ 9

¹²¹⁵ *EMI Records v. Eircom Ltd.*, [2010] IEHC 108, ¶ 11

¹²¹⁶ *EMI Records v. Eircom Ltd.*, [2010] IEHC 108, ¶ 13

¹²¹⁷ “Eircom Statement on Illegal File Sharing,” *Press release on Eircom website*, and Bridy, “Graduated Response American Style,” P. 24.

¹²¹⁸ *EMI Records v. Eircom Ltd.*, [2010] IEHC 108, ¶ 13

¹²¹⁹ “Eircom Statement on Illegal File Sharing,” *Press release on Eircom website*, and Bridy, “Graduated Response American Style,” P. 24, and: *EMI Records v. Eircom Ltd.*, [2010] IEHC 108, ¶ 13

¹²²⁰ *EMI Records v. Eircom Ltd.*, [2010] IEHC 108, ¶ 13

¹²²¹ Rebecca Giblin, “Evaluating Graduated Response,” *Columbia Journal of Law & the Arts* 37 (2014): 147.

¹²²² “Eircom Statement on Illegal File Sharing,” *Press release on Eircom website*, and Bridy, “Graduated Response American Style,” P.24.

received, the customer's broadband service would be disconnected for a 12 month period."^{1223 1224}

During suspension, subscription fees were waived.¹²²⁵ This disconnection did not apply to television or telephone service that the subscriber got over his or her Internet facility.¹²²⁶ The ultimate sanction came with exceptions for people depending on broadband Internet access for medical services and others for their livelihood. Companies in which infringement took place might only be subject to an admonition.¹²²⁷

For my research, I got the perspectives of practitioners through interviews. DtecNet refused to comment on the relation they had with specific clients, but in an interview gave general statements on their workings: they were networks of computers all over the world that examined content. They identified and validated when content was infringing by looking at signatures, and in some cases by human validation (like in the case of high profile content or in a high profile environment). The process involved "lots of technical crawling and combing of data."¹²²⁸

DtecNet said that they are not in a position to judge the intent, or where/how infringement occurred, so they "pass that off to some of the organizations that are better suited at that." They found and identified content as likely infringement.¹²²⁹

IRMA operated entirely outside of the process of disconnection. They did build evidence against IP addresses and stored all this evidence, in case Eircom needed it.¹²³⁰ In some cases, subscribers contacted IRMA directly, but according to them, they were referred to Eircom immediately.¹²³¹

8.4 Scale, severity and procedural safeguards

Scale

The procedure had a test period that started in June 2010, and became permanent in October of that same year.¹²³²

In December 2011, so after approximately one year, Eircom had issued 29,000 notices to its subscribers.¹²³³ 100 subscribers received a 7 day suspension, 12 subscribers received a longer suspension.¹²³⁴

¹²²³ "Eircom Statement on Illegal File Sharing," *Press release on Eircom website*, and Bridy, "Graduated Response American Style," P.24.

¹²²⁴ Bridy, "Graduated Response American Style," P.24.

¹²²⁵ "Legal Music, Frequently Asked Questions," *Eircom website*, <http://www.eircom.net/notification/legalmusic/faqs/> Last viewed on March 3, 2013.

¹²²⁶ EMI Records v. Eircom Ltd., [2010] IEHC 108, ¶ 9

¹²²⁷ EMI Records v. Eircom Ltd., [2010] IEHC 108, ¶ 11

¹²²⁸ Fred Felman (DtecNet) interviewed by author, November 2013.

¹²²⁹ Fred Felman (DtecNet) interviewed by author, November 2013.

¹²³⁰ Dick Doyle (IRMA) interviewed by author, January 2014.

¹²³¹ Dick Doyle (IRMA) interviewed by author, January 2014.

¹²³² "Eircom Statement on Illegal File Sharing," *Press release on Eircom website*, and Bridy, "Graduated Response American Style," P.24, and: International Federation of the Phonographic Industry, *Digital Music Report 2011* (IFPI 2011). (defining graduated response), and Bridy, "Graduated Response American Style," P.24.

¹²³³ Mark Tighe, "Eircom Cut Off 100 Illegal Downloaders," *Sunday Times* (March 4, 2012), <http://www.thesundaytimes.co.uk/sto/news/ireland/article988221.ece>, and: Bridy, "Graduated Response American Style," P.25.

¹²³⁴ Tighe, "Eircom Cut Off 100 Illegal Downloaders," and: Bridy, "Graduated Response American Style," P.25.

In my interviews with practitioners, IRMA itself said they notified about 5000 infringements every month, and that, as of July 2013, 152,000 had been found, relating to about 6,000 accounts.¹²³⁵

They considered the system effective. In a period spanning two years, they said that of all the people receiving first 'strikes', only 10% received second letters, and 0,01% received a third letter.¹²³⁶

I could not verify these numbers, apart from the information that was brought forward in the media.¹²³⁷ It confirmed that for each phase, the number of people contacted has dropped dramatically. Although I did not have exact numbers, based on the information above it meant that for the subcase level, the first two subcases scaled up to thousands of subscribers, while the third phase reached hundreds and the last phase less.

Severity

Unlike HADOPI, which allowed for triple punishment (paying a fine + disconnection + still paying subscription costs), the graduated response procedure by Eircom was less severe. The first two phases (subcase 1 and 2) consisted of warnings, while disconnection in phase 3 (subcase 3) could be 7 days, and only after another infringement occurred be extended to a 12 month period (subcase 4). Contrary to what happened in France, subscription fees were waived during suspension periods.¹²³⁸

Also, disconnection came with exceptions for people depending on broadband Internet access for medical services and others for their livelihood. Companies in which infringement took place would only be subject to admonishment.

On the seriousness of the disconnection sanction, the judge said that "most people only have to walk to their local town centre to gain access for around €1.50 an hour."¹²³⁹

Safeguards

Whether this procedure allowed its users any safeguards is a serious question. Human rights organizations not limited to Ireland protested the way the procedure had been set up. Digital Rights Ireland called the process "unreliable, secret, undemocratic, disproportionate, and affecting innocent third parties."¹²⁴⁰ The Electronic Frontier Foundation called it one of the global chokepoints.¹²⁴¹ Apart from that, the procedure had been under careful scrutiny of the Data Protection Officer twice for allegedly infringing on privacy rights. Unfortunately, the exact workings of the procedure will remain a mystery for now, as this was privately administered, and Eircom refused to comment on this. However, from the court cases and other material, much can be made out on how well it performed on safeguards.

One general statement that Bridy made on this is that subscribers supposedly "click through" and accept waivers of procedural rights through standardized terms of service,

¹²³⁵ Dick Doyle (IRMA) interviewed by author, January 2014.

¹²³⁶ Dick Doyle (IRMA) interviewed by author, November 2013.

¹²³⁷ Tighe, "Eircom Cut Off 100 Illegal Downloaders," and: Bridy, "Graduated Response American Style," P.25.

¹²³⁸ Dick Doyle (IRMA) interviewed by author, January 2014.

¹²³⁹ EMI Records v. Eircom Ltd., [2010] IEHC 108, ¶ 9

¹²⁴⁰ "Three unproven accusations and you're out - why the Eircom/IRMA deal is bad for Internet users," *Digital Rights Ireland* (Jan 29, 2009), <http://www.digitalrights.ie/three-unproven-allegations-and-youre-out/>

¹²⁴¹ "Internet Intermediary Liability in Ireland," *Global Censorship Chokepoints*,

<https://globalchokepoints.org/Internet-intermediary-liability-ireland>, last viewed on March 3, 2013.

which were legally enforceable (even when they could not choose another provider). Bridy discussed the validity of such terms of service, mentioning their fine print and whether this was ethical.¹²⁴²

The notice by the data protection officer said that the Eircom settlement and protocol violated data protection legislation in a number of fields.¹²⁴³ It mostly concentrated on the legitimacy of unauthorized surveillance, the safety of storage, a lack of notice of storage, an improper procedure to determine whether stored data was accurately portraying infringers, and whether this was proportional.¹²⁴⁴ Even though the court evaluated these claims, and ruled that the process was legitimate, these points will be addressed in the parts below, and supplemented with my own perspectives and my interviews.

Privacy

Whether or not this enforcement strategy interfered with privacy rights, depended on whether personal data was processed. This usually happens when infringement is found, and when enforcing parties have access to personal data.

We know that surveillance was done by DtecNet, but they refused to go into the relations they had with their clients. It is unlikely that DtecNet used deep packet inspection (DPI) on the Eircom network. Eircom would not have needed to hire DtecNet if they wanted to use DPI. It is therefore likely that, just like in the case of HADOPI, infringement was found through “over the top” surveillance (at the application layer, and not at the level of physical infrastructure). DtecNet monitored public P2P file sharing networks by joining them and keeping track of the IP addresses on those networks that shared infringing files. To spot which files were infringing, those agents had giant catalogues of copyright protected content supplied to them by rights holders.¹²⁴⁵ Remarks by the court support that this method of detection was used, as they said that copyright protection was a legitimate ground for record companies to participate in swarms.¹²⁴⁶

This method of surveillance is not as intrusive as DPI, and targets fewer people, although it is still a large group. Also, people that contribute to P2P networks that are publicly accessible can reasonably expect that their content or hard drive is less private.¹²⁴⁷ In fact, the judge in the Eircom case said that engaging in criminal activity on P2P networks means you surrender you privacy rights. “I find it impossible to recognize as a matter of constitutional law, that the protection of the entitlement to be left in the sphere of private communications could ever extend to conversations, emails, letters, phone calls or any other communication designed to further a criminal enterprise.”¹²⁴⁸

The Irish Data Protection Officer argued in Court that detection as used by Eircom

¹²⁴² Bridy, "Graduated Response American Style," P.25.

¹²⁴³ EMI Records (Ireland Ltd v Data Protection Commissioner (2012) IEHC 264, ¶14.0

¹²⁴⁴ EMI Records (Ireland Ltd v Data Protection Commissioner (2012) IEHC 264, ¶14.0

¹²⁴⁵ Bridy, "Graduated Response American Style," P.30, and: "Procédures HADOPI," La Loi Hadopi, <http://www.la-loi-hadopi.fr/procedure-HADOPI/14-controle-HADOPI.html> last viewed on Jan 3, 2014.

¹²⁴⁶ EMI Records (Ireland Ltd v Data Protection Commissioner (2012) IEHC 264, ¶17.0-7.6

¹²⁴⁷ Bridy, "Graduated Response American Style," P. 31.

¹²⁴⁸ EMI Records (Ireland) Ltd & Ors –v- UPC Communications Ireland Ltd (2010) IEHC 377 (10 november 2010). 66-70

could be likened to entering a house without a search warrant, or universities opening a student locker or searching their mobile phones. However, the court agreed with Eircom that it was more like someone coming up to a trader selling illegal DVDs on the street.¹²⁴⁹

After detection, privacy could be in jeopardy by what happens with those identified as alleged infringers. The notifying parties or the parties detecting infringement would only know that a particular IP address had been involved in downloading. They would not know any further personal details.¹²⁵⁰

It is also unlikely that IRMA bodies would use IP addresses in any other way to notify them through Eircom, according to the judge evaluating the Eircom settlement. There was no real interest in personally identifying subscribers. Theoretically they could have used the Norwich Pharmacal order, but it seems they left this “expensive and futile pursuit” in favor of this settlement.¹²⁵¹ After sanctioning, privacy concerns are taken care of as well. The court mentioned that people cut off from access would not be part of some register.¹²⁵²

In general, the court in the UPC case said this was about the enforcement of a private contract without any further record keeping.¹²⁵³

In the interviews, IRMA confirms the picture painted in the court cases: “we put notifications together in standard format and forward them to Eircom with the IP address of the infringer. Then they go behind a Chinese wall.” IRMA is then “not allowed in process, we are no longer involved.” Eircom further handled the contact with the customer, including writing letters to them.¹²⁵⁴ Only Eircom had access to names connected to IP addresses. So IRMA never knew who an account holder was.¹²⁵⁵

Behind certain IP addresses, IRMA did build dossiers with evidence. This was done in case Eircom needed it.¹²⁵⁶ IRMA also mentioned that some people responded to received warning by contacting them, but they immediately referred them back to Eircom.¹²⁵⁷

IRMA adds that there were exceptions to disconnection for people depending on broadband Internet access for medical services and others for their livelihood and in some cases companies, to safeguard the privacy, Eircom would only communicate with IRMA: “this IP address does not fall within the terms of the protocol.”¹²⁵⁸

Apart from building the dossiers, IRMA claims to have no further interest in pursuing the name and addresses of infringers. He says that between 2005 and 2008 every national group wanted to do individual lawsuits. “They were painful, totally worthless, a waste of time and resources, and didn’t sit well with average consumers.”¹²⁵⁹

¹²⁴⁹ EMI Records (Ireland Ltd v Data Protection Commissioner (2012) IEHC 264, ¶7.0-7.6

¹²⁵⁰ EMI Records v. Eircom Ltd., [2010] IEHC 108, ¶ 12

¹²⁵¹ EMI Records v. Eircom Ltd., [2010] IEHC 108, ¶ 24-25

¹²⁵² EMI Records (Ireland) Ltd & Ors –v- UPC Communications Ireland Ltd (2010) IEHC 377 (10 november 2010). ¶72

¹²⁵³ EMI Records (Ireland) Ltd & Ors –v- UPC Communications Ireland Ltd (2010) IEHC 377 (10 november 2010). ¶66-70

¹²⁵⁴ Dick Doyle (IRMA) interviewed by author, November 2013.

¹²⁵⁵ Dick Doyle (IRMA) interviewed by author, January 2014.

¹²⁵⁶ Dick Doyle (IRMA) interviewed by author, January 2014.

¹²⁵⁷ Dick Doyle (IRMA) interviewed by author, January 2014.

¹²⁵⁸ Dick Doyle (IRMA) interviewed by author, January 2014.

¹²⁵⁹ Dick Doyle (IRMA) interviewed by author, November 2013.

Impartial, competent and independent judge

One of the most striking criticisms of this privately administered graduated response regime was that because of its private nature judicial review was excluded from the process.¹²⁶⁰ The role of adjudication and sentencing was taken up by Eircom itself. Unfortunately, Eircom officials were unwilling to go into the details of the implementation and refused to submit to an interview on this. This question can therefore only be partially answered, and only by speculating on the incentives of the parties involved.

The incentives seemed to push towards less impartiality. After all, this mechanism was created on the basis of a deal struck between rights holders and the ISP. So there was a relationship between 'judge' and complainant that could potentially affect the impartiality of the judgment. Because of automation, first phase warnings were assumed to be correct. On the other hand, Eircom would lose customers if they disconnected them without good reason, so it was not necessarily in their interest to be 'wrong' about accusations.

With regards to competence, little can be said about the employees that worked at Eircom, apart from the obvious fact that they lacked the judicial training a judge has.

Presumption of innocence

The presumption of innocence was affected by the way the first phases of the system were designed, and by the way the burden of proof was distributed in later phases.

The first two phases were large in scale and therefore automated. This means that those allegations were not checked for accuracy. That effectively stripped the presumption of innocence for subscribers in those phases. Just like in the case of HADOPI, evidence was gathered by private agents with a financial interest in the process, the quality of the allegations was also unclear, and the system was designed to facilitate more allegations and to make that process easy. There were no costs against the plaintiff if the claim did not succeed, so the burden was on the subscribers of Eircom.¹²⁶¹

If infringement happened after those first two phases, Eircom employees would become involved. They reviewed the evidence of a third notification. It was unclear how they did this, and on what copyright grounds. For example, as the enforcement targeted 'subscribers' this could mean that even though other people could have used that connection to infringe, the subscriber would be liable. Just like in the case of HADOPI, negligence was punished, and people would have to prove their innocence. Even worse, they had to do this within 14 days if they did not want their Internet cut-off. This is another heavy shift in favor of the complaining party, who had nothing to lose on notices sent out erroneously.

Notice, right to be heard (prior to conviction), defenses and appeal

The Telecommunications and Internet Federation in Ireland had argued that Eircom did not allow for enough protection or redress for end-users in its graduated response

¹²⁶⁰ Mark Tighe, "Eircom Cut Off 100 Illegal Downloaders," *Sunday Times* (March 4, 2012), <http://www.thesundaytimes.co.uk/sto/news/ireland/article988221.ece>, and Bridy, "Graduated Response American Style," P.25.

¹²⁶¹ Nicolas Suzor and Brian Fitzgerald. "The Legitimacy of Graduated Response Schemes in Copyright Law," *University of New South Wales Law Journal* 34 (2011): 1. P.24.

procedure.¹²⁶² This also surfaced in the court case on the protocol. The judge was asked whether it would be lawful to disconnect accounts if that account was not subject to investigation by an “authorized body, and without a court decision or fair and impartial hearing.”¹²⁶³ The judge responded that such an investigation or hearing would not be necessary since there were no accusations of an offence or criminal behavior. Parties were instead dealing with civil copyright liability, according to the judge.¹²⁶⁴

Regarding notice, subscribers were notified in the first two phases of the procedure that their accounts had been used for infringement. In the third phase they were also notified that their accounts would be suspended in two weeks if they did not submit any representations to Eircom. Because conviction had essentially been established, there would only be a right to be heard after conviction.

Eircom would then allow customers to make representations, over the telephone or over the Internet, on why they should not be disconnected. Eircom would look at these claims (under paragraph 2.8 of the protocol), which could say an exception is applicable, or that there had been no infringement at all. On the website it said: “Eircom has a dedicated team to assist customers with any queries in relation to notifications. In case the customer feels that they have been incorrectly identified or were not responsible for the illegal downloading then they can advise Eircom of this at the time of notification. Eircom will consider all customer appeals on a case by case basis.”¹²⁶⁵

If Eircom was not convinced, disconnection would take place. There was no way to appeal this decision at Eircom, or at another authority outside of the ISP.

Transparency

A large point of criticism of Eircom’s graduated response concerned its secretive nature. This lack of transparency was worrisome, because even though it concerned a private agreement, its application had nearly the same effect as a public law because it applied to millions of users. Also, broadband penetration could mean that some users would be limited to only Eircom in certain parts of Ireland.

Its design was based on a protocol that was the outcome of private deliberations between the music industry and Eircom itself. Those deliberations remained secret, and have not allowed for any public debate or engagement whatsoever. The protocol itself remained secret as well.

This also made its implementation secretive. Although the court case on the protocol and Eircom's website shed some light on how the procedure is implemented, much still remains unclear. For example: how rules are applied, how much redress for subscribers is allowed, on what exceptions subscribers can base themselves to avoid disconnection, etc.

The outcomes were also kept secret. The only reason people found out about the number of people sanctioned is because some notes of a meeting were leaked to the press. Apart from that, concrete numbers on sanctions, disconnections, and warnings remained unknown.

¹²⁶² "Memo of meeting between Irish telecoms and Minister Sean Sherlock re SI on copyright injunctions," available on *Scribd* at: <http://www.scribd.com/doc/83984690/tif-briefing2-001>, last viewed on Jan 4, 2014.

¹²⁶³ *EMI Records v. Eircom Ltd.*, [2010] IEHC 108, ¶ 16

¹²⁶⁴ *EMI Records v. Eircom Ltd.*, [2010] IEHC 108, ¶ 41

¹²⁶⁵ "Legal Music, Frequently Asked Questions," *Eircom website*, <http://www.eircom.net/notification/legalmusic/faqs/> Last viewed on March 3, 2013.

Proportionality

One of the major concerns with every graduated response procedure is its proportionality. To assess whether measures in this case were proportional, it was important to look at whether the measures were necessary to achieve the stated goal, suitable, and whether they did not put too much of a burden on individual rights.

So was this measure necessary? On Eircom's website a 'FAQ' makes clear that one of the purposes is to educate:

- " Informing customers of the issues,
- providing assistance to customers on how to prevent illegal music downloading and sharing,
- helping customers identify legitimate music services."¹²⁶⁶

Another goal was deterrence. There were more ways to achieve this, but previous measures had proved to be insufficient to curb P2P file sharing.

Was this suitable? Looking at the limited information available on the decreasing number of people targeted in each phase of the procedure, it would appear that the procedure had some deterrent effect. However, this information comes from leaked reports and my interviews. IRMA called it "very effective"¹²⁶⁷ (and therefore suitable) which they argued by numbers they themselves supplied. The amount of notices sent to subscribers decreased with every phase in the process. In a period spanning two years, they said that of all the people receiving first 'strikes', only 10% received second letters, and 0,01% received a third letter.¹²⁶⁸

Was there a large burden on individual rights? The threat of disconnection was the cause of much controversy. It seemed a very heavy penalty for copyright infringement, considering the role internet played in our society. Meanwhile, the first disconnection only lasted 7 days, while it could be extended to 12 months. Regarding privacy, the Court told the Irish Data Protection Officer that subscribers that infringe on the rights of others leave the private sphere, and that interference was therefore justified.¹²⁶⁹

8.5 Impact on infringement levels

After its implementation, things remained quiet on the effect of Eircom's graduated response procedure on infringement. IRMA itself did not provide any data to support this, even though they claimed that the procedure worked in their case against UPC. To get UPC to implement a graduated response procedure as well, evidence supplied in the court included that in response to the Norwich Pharmacal orders, most people were embarrassed that they or their family had downloaded illegally, the people who had committed the act, admitted it, and others disapproved when they learned a family member had done it. Other evidence they provided consisted of a survey which said that 7 out of 10 people would stop

¹²⁶⁶ "Legal Music, Frequently Asked Questions," *Eircom website*, <http://www.eircom.net/notification/legalmusic/faqs/> Last viewed on March 3, 2013.

¹²⁶⁷ Dick Doyle (IRMA) interviewed by author, November 2013.

¹²⁶⁸ Dick Doyle (IRMA) interviewed by author, November 2013.

¹²⁶⁹ EMI Records (Ireland) Ltd & Ors –v- UPC Communications Ireland Ltd (2010) IEHC 377 (10 november 2010). ¶166-70

copyright infringement if they received warnings. There was also evidence from the university of Florida showed that only 1% would go to the final level of the procedure.¹²⁷⁰

It was unfortunate that there was no real evidence that went into infringement levels on Eircom's services after its implementation. The decreasing number of notifications sent in each phase suggested that there was some deterrent effect where it concerned the use of P2P software to infringe, but that did not say anything about the use of other means of infringement, and whether they had flocked to proxies. In the court case against UPC, some claimed that evading detection was relatively easy to do through proxies and through encryption.¹²⁷¹

Apart from the numbers and the research suggested by IRMA, there was no evidence that this graduated response procedure had reduced infringement.¹²⁷²

8.6 The costs of the system

Although the Telecommunications and Internet Federation (TIF) argued that it was expensive to implement,¹²⁷³ graduated response procedures were generally seen as a cheaper way for rights holders to enforce copyrights.¹²⁷⁴ The system had costs itself that were divided among the different parties: rights holders and Eircom. In the court cases, the judge also mentioned that there were no cheap alternatives to detection. For example, there was evidence before the court that the proceedings through Norwich Pharmacal orders, used in Ireland in only three cases, to identify 17, 49, and 23 names, cost 680,000 Euros to pay solicitors and barristers on all sides. In return settlements were effected, but they only returned 80,000 Euros.¹²⁷⁵

Rights holders needed to create systems of notification and had to hire private companies to detect infringement.¹²⁷⁶ DtecNet refused to discuss the individual relations it had with its clients, so these costs remained unknown.¹²⁷⁷

In the interviews, IRMA confirmed that there was still a heavy burden on rights holders: "It costs us money. We have to employ investigators." Also, they needed a "computer room to make notices," and in "case the case goes forward, you build evidence. It does cost us."¹²⁷⁸ However, they also said that the alternative, individual lawsuits, were a waste of resources.¹²⁷⁹

¹²⁷⁰ EMI Records (Ireland) Ltd & Ors –v- UPC Communications Ireland Ltd (2010) IEHC 377 (10 november 2010). ¶171

¹²⁷¹ EMI Records (Ireland) Ltd & Ors –v- UPC Communications Ireland Ltd (2010) IEHC 377 (10 november 2010). ¶134-37

¹²⁷² Rebecca Giblin, "Evaluating Graduated Response," *Columbia Journal of Law & the Arts* 37 (2014): 147.

¹²⁷³ "Memo of meeting between Irish telecoms and Minister Sean Sherlock re SI on copyright injunctions," available on *Scribd* at: <http://www.scribd.com/doc/83984690/tif-briefing2-001>, last viewed on jan 4, 2014.

¹²⁷⁴ Alain Strowel, "The 'Graduated Response' in France: Is It the Good Reply to Online Copyright Infringement." in: *Copyright Enforcement and the Internet*, ed. Stamatoudi (Kluwer Law International, The Netherlands, 2010). P.153.

¹²⁷⁵ EMI Records (Ireland) Ltd & Ors –v- UPC Communications Ireland Ltd (2010) IEHC 377 (10 november 2010). ¶158-65

¹²⁷⁶ New Zealand Federation Against Copyright Theft, "Copyright (Infringing File Sharing) Regulations – Fee Review," *Ministry for Economic Development* (2012) P.2, www.med.govt.nz/business/intellectual-property/pdf-docs-library/copyright/notice-process/illegal-peer-to-peer-file-sharing-submissions-on-fee-review-discussion/nzfact.pdf

¹²⁷⁷ Fred Felman (DtecNet) interviewed by author, November 2013.

¹²⁷⁸ Dick Doyle (IRMA) interviewed by author, November 2013.

¹²⁷⁹ Dick Doyle (IRMA) interviewed by author, November 2013.

Eircom in turn needed a system to identify the subscribers and to send the infringement notices. It was unclear how much this exactly cost.¹²⁸⁰ In the previous chapter (the HADOPI case), I have documented different estimates by different parties, ranging into the millions. However, most of those numbers were provided by ISPs themselves.¹²⁸¹

However, in the case against UPC, the judge refused the points put forward by UPC that detection and termination of illegal activity would be costly. According to the judge, the systems were already there, but simply never used.¹²⁸² This is also what Eircom brought forward in that case: the technology is already in place for things like child pornography, and could simply be adapted to fit copyright.¹²⁸³

Another cost could be the result of market force. As this was a privately administered system by one ISP, subscribers could flock to other ISPs that had more lenient terms of service. The High Court said this as well: “it [i]s likely to be deeply unfair that only Eircom with about 40% of the market share... should bear the burden of this settlement, thus activating the winds of market forces to drive customers towards Eircom’s competitors.”¹²⁸⁴ This is why IRMA tried suing UPC, and in an my interview said that they were involved in a process that would result in litigation against other ISPs.¹²⁸⁵ In February 2014, IRMA had begun a process against UPC again that could result in a graduated response procedure there as well. “In an affidavit for the companies Evidence of 7,757 infringements of copyright in a sample 250 sound recordings over the month of November 2013 was provided to UPC, plus details of the infringing subscribers’ IP addresses.”¹²⁸⁶

The market force could not just scare people away from Eircom, but also towards ISPs that did not have similar mechanisms in place. The judge in the case against UPC claimed that ISPs also increase their profits by being a “market place of illegal downloads.”¹²⁸⁷

Although these statements were brought forward, it is unsure what the practical effect was on competition. The Electronic Frontier Foundation (EFF) quotes¹²⁸⁸ an Irish blog that said Eircom was losing 1000 subscribers a month, whilst competitor UPC increased the number of phone subscribers by 60% in 2010.¹²⁸⁹ I cannot, however, verify these claims.

In an interview with UPC, they said it was difficult to say whether this was true. UPC claimed to serve different clients, because they had a higher broadband speed, and served

¹²⁸⁰ Internet Society, Perspectives on Policy Responses to Online Copyright Infringement, an Evolving Policy Landscape,” Internet Society website (Feb 20, 2011) P.23, <http://www.Internetsociety.org/perspectives-policy-responses-online-copyright-infringement-evolving-policy-landscape>

¹²⁸¹ See previous chapter.

¹²⁸² EMI Records (Ireland) Ltd & Ors –v- UPC Communications Ireland Ltd (2010) IEHC 377 (10 november 2010). ¶150-57

¹²⁸³ “Memo of meeting between Irish telecoms and Minister Sean Sherlock re SI on copyright injunctions,” available on Scribd at: <http://www.scribd.com/doc/83984690/tif-briefing2-001>, last viewed on jan 4, 2014.

¹²⁸⁴ EMI Records v. Eircom [2010] IEHC 108, ¶10

¹²⁸⁵ Dick Doyle (IRMA) interviewed by author, November 2013.

¹²⁸⁶ Mary Carolan, “Legal action to stop UPC users downloading illegally,” *The Irish Times* (February 10, 2014), <http://www.irishtimes.com/news/crime-and-law/courts/legal-action-to-stop-upc-users-downloading-illegally-1.1686474>.

¹²⁸⁷ EMI Records (Ireland) Ltd & Ors –v- UPC Communications Ireland Ltd (2010) IEHC 377 (10 november 2010). ¶120

¹²⁸⁸ “Internet Intermediary Liability in Ireland,” *Global Censorship Chokepoints*, <https://globalchokepoints.org/Internet-intermediary-liability-ireland>. Last viewed on March 3, 2013.

¹²⁸⁹ Alan Toner, “Ireland: Three Strikes and Fair Use,” *kNOw Future Inc.* (March 3, 2011), <http://knowfuture.wordpress.com/2011/03/03/ireland-three-strikes-and-fair-use/>.

different bundles (combined with phone for example) which could have interested subscribers as well. They mentioned they did not want to implement a graduated response procedure, because they thought the government, the legislator, or the court should direct ISPs to fight copyright infringement. “UPC does not as a policy position believe it is appropriate for a private company to take a position on this and to bilaterally engage with commercial parties.”¹²⁹⁰

8.7 Conclusion

The Eircom graduated response procedure was a procedure initiated by rights holders and administered by internet provider Eircom. Tech firms hired by rights holders detected infringement and sent a notice to Eircom who then warned the accused. After three warnings, internet was disconnected for 7 days, which could be extended if the behavior continued. The case therefore consists of 4 subcases (warning 1, warning 2, 7-day cut-off and 12 month cut-off).

Regarding severity and scale, thousands of people received a first and second warning (subcase 1 and 2). Hundreds of subscribers received a 7 day suspension (subcase 3), less than a hundred subscribers received a longer suspension (subcase 4).

Regarding privacy, infringement was only found through over the top surveillance: by joining P2P networks. It was a privately administered sanctioning procedure, so there appeared to be no judge and it was unclear how accusations were checked or how the system is further applied. For the first two phases, the procedure was automated. The warning was a first notice but it already had consequences. There was a right to be heard and appeal. However, it was unknown how well these defenses were evaluated by the Eircom employees. There was no transparency. The disconnection penalty was considered disproportional by multiple parties.

There was debate on the impact on file sharing this had. Although the amount of notices declined in the later phases, it was unclear if this was due to the procedure. The procedure appeared to be expensive, but the costs were distributed to Eircom and its customers. These outcomes will be highlighted again in the conclusion and compared with the outcomes of the other cases.

¹²⁹⁰ Kate O Sullivan (UPC Ireland) interviewed by author, June 2013.

9. NOTICE AND TAKEDOWN AT GOOGLE SEARCH AND YOUTUBE IN 2011-2013

9.1 Introduction

Google implemented a notice and takedown procedure at two of its largest websites: its search engine and YouTube. For both, they implemented a notice and takedown system, that allowed rights holders to report allegedly infringing search results (Google search) or audio-visual content (YouTube), in order for Google to take that content down. To accommodate rights holders with large catalogues, Google created large-scale programs for both: the trusted copyright removal program and ContentID. This case describes how Google applied notice and takedown and the two large scale systems at its two largest websites at the time. For the evaluation of performance on the variables, the case has been divided into 4 subcases, which are the way Google designed large-scale automated takedowns and smaller scale takedowns at those sites (so the subcases are Google search takedowns, the Trusted Copyright Removal Program, YouTube takedowns and ContentID).

The first section on the legal background will first briefly describe Google and Youtube, before going into the legal obligations for ISPs like Google in the USA. For this I relied on information on Google's services, news articles and legal sources. The following section details the procedure in practice. For this, I supplemented the information cited above with an official report released by Google on its enforcement, and I conducted an interview with Fred von Lohmann, legal director for copyright at Google. To get the perspective of enforcers who work with Google, I spoke to Brein, the Recording Industry Association of America (RIAA), Attributor Guardian, and DTECNET. I tried to contact the copyright enforcement group and Guardaley. Both refused. The Movie Picture Association (MPA) also refused to speak to me. After this section, I will describe how the case performs on the variables. I spoke to the Electronic Frontier Foundation for the consumer/digital rights perspective. In addition to the interviews, I included academic research and reports by NGOs on notice and takedown. The information was collected from January 2012 until the end of 2013.

9.2 Legal background

Google search (DMCA and TCRP)

In 1998, Larry Page and Sergey Brin developed a new search engine they would come to call Google.¹²⁹¹ What made Google unique was its use of PageRank, a search technique that did not rely on how many times a search term was mentioned on pages, but also on the relationships among websites. In particular, it determined the relevance of a website by the number of pages, and the importance of those pages, that linked back to the original site.¹²⁹²

Its mission statement has been "to organize the world's information and make it universally accessible and useful."¹²⁹³ While search started as Google's core business, the company quickly expanded to include more services such as email, document editing, cloud storage, social networking, and more.

¹²⁹¹ "Company," *Google website*, <http://www.google.com/about/company/>

¹²⁹² "Products," *Google website*, <http://www.google.com/about/company/products/>

¹²⁹³ "Company," *Google website*, <http://www.google.com/about/company/>

Google search processed over one billion search requests each day.¹²⁹⁴ At the time of my research, it was also the most visited website in the world¹²⁹⁵ and the most popular search engine.¹²⁹⁶ Google Zeitgeist showed how the world searched.¹²⁹⁷ Google Trends showed which searches were the most popular.¹²⁹⁸

Being such a large search engine, Google could be used to search for infringing content. The content industry has often reacted furiously and has pressured Google to adopt measures to prevent users from finding protected and infringing materials, calling Google a “gateway to pirated content.”¹²⁹⁹

Google implemented a notice and takedown system that facilitated rights holders to notify Google of infringing content, so Google could remove it from their search results. For copyright holders with a good, proven track record, Google created the Trusted Copyright Removal Program (TCRP) that allowed trusted complainants to submit takedown requests in a higher volume.¹³⁰⁰ They published these requests in their transparency report.¹³⁰¹

YouTube (DMCA and Content ID)

YouTube was founded in 2005, and allowed billions of people to upload, share, watch and comment on original content, mostly videos.¹³⁰² Meanwhile, it allowed advertisers to advertise their products and could generate income for people uploading content. It has even been possible to rent movies on YouTube.¹³⁰³ In October 2006, Google bought the company for 1,65 billion dollars. The company would serve as a subsidiary of Google.

Providing a place for user generated content that is popular or obscure, YouTube fulfilled an important cultural function. Many official channels used YouTube to bring out messages including political content and interviews. In 2008, YouTube received the Peabody award for “promoting the free exchange of ideas, expressed in video formats, around the world (...) Its selection continues the tradition of the Peabody Award, a tradition committed to a free press, to free speech and to the use of electronic media as a form of public service for all citizens.”¹³⁰⁴

In terms of statistics, at the time of this research, every minute, 60 hours of video was uploaded to YouTube (one hour per second). The website had more than 800 million unique visitors every month and more than 3 billion hours of content was watched on YouTube. YouTube was

¹²⁹⁴ Eric Kuhn, “Google unveils top political searches of 2009,” *CNN* (December 18, 2009), <http://politicalticker.blogs.cnn.com/2009/12/18/google-unveils-top-political-searches-of-2009/>.

¹²⁹⁵ “The top 500 sites on the web”, <http://www.alexa.com/topsites>

¹²⁹⁶ Wendy Boswell, “Google Search Statistics,” *About Tech*, <http://websearch.about.com/od/focusongoogle/f/Google-Search-Statistics.htm> last viewed on april 16, 2014.

¹²⁹⁷ “Zeitgeist 2010: How the World Searched,” *Google Zeitgeist* (2011), <http://www.google.com/intl/en/press/zeitgeist2010/more-data.html>

¹²⁹⁸ “Google Trends,” *Google website*, <http://www.google.com/trends/?geo>

¹²⁹⁹ Ted Johnson, “Showbiz Lobby Puts Capitol Hill Pressure on Google to Take Action on Piracy,” *Variety* (September 18, 2013), <http://variety.com/2013/digital/news/google-pressured-by-hollywood-to-do-more-to-fight-piracy-1200616306/>.

¹³⁰⁰ Fred von Lohmann, “Report: How Google Fights Piracy,” *Google Public Policy Blog* (September 10, 2013). <http://googlepublicpolicy.blogspot.nl/2013/09/report-how-google-fights-piracy.html> and Google, *How Google Fights Piracy*, (Google Report, September 2013). See: <https://docs.google.com/a/google.com/file/d/0BwxyRPFduTN2dVFqYml5UeUeUE/edit?pli=1>

¹³⁰¹ “Copyright removal requests,” *Google Transparency Report*, <https://www.google.com/transparencyreport/removals/copyright/>

¹³⁰² “About Youtube,” *Youtube website*, http://www.youtube.com/t/about_youtube

¹³⁰³ “About Youtube,” *Youtube website*, http://www.youtube.com/t/about_youtube

¹³⁰⁴ See: “List of Peabody Award Winners” on Wikipedia.org, [https://en.wikipedia.org/wiki/List_of_Peabody_Award_winners_\(2000%E2%80%932009\)#2008](https://en.wikipedia.org/wiki/List_of_Peabody_Award_winners_(2000%E2%80%932009)#2008)

located in 39 countries, and 70 percent of all traffic came from outside of the US.¹³⁰⁵ It was the third most visited website in the world (after Google (1) and Facebook (2)).¹³⁰⁶

At YouTube, registered users could upload an unlimited number of videos, while unregistered users could watch videos. People could create their own YouTube accounts through which they could access special content or upload their own.¹³⁰⁷ YouTube users could watch, search, and easily locate millions of fast streaming videos online, upload quickly and simply, and tag videos in almost any format, as well as share videos with anyone in the world. Users could also search, join, and create video groups with people of similar interests, subscribe to member videos, save favorites, make playlists, embed videos on blogs or websites, and make videos private or public.¹³⁰⁸

There were different types of content on YouTube, ranging from original creations (home videos, original short movies and music), transformative derivatives (mashups or remixed or original content, altered in some way to make something new and creative), copied or ripped content (clips of original content which has been reproduced).¹³⁰⁹ This content could be added by either public or private parties.

Users were not allowed to upload just any content, however. In its community guidelines, YouTube stressed that, among other things, it was important for users to respect the copyrights of others.¹³¹⁰ Failing to stick to the community guidelines, could result in a warning for a user, or a ban from making new accounts.¹³¹¹

Their anti-piracy system was not perfect, and as a result, a number of lawsuits had taken place against YouTube. Viacom sued the website for 1 billion dollars, claiming that YouTube did not respect its copyrights and that it had to do more to protect those rights. Viacom spoke about 160,000 unauthorized clips that had been viewed more than 1.5 billion times.¹³¹² So far, in the Viacom case at the time of this research no final decision had been reached. Meanwhile, Mediaset sued the website for 500 million dollars, claiming that YouTube showed 4643 videos and clips without permission.¹³¹³

Since October 2007 it used "Content ID" technology to help with the management of copyrights.¹³¹⁴ This self-regulatory measure was intended to limit the amount of infringing content on its service and to limit its possible exposure to lawsuits.

Furthermore, YouTube generated income with more than 3 billion videos through advertisement.¹³¹⁵ 10,000 parties partnered with YouTube (for example through Content ID).

Legal obligations for ISPs

Both ISPs are under legal obligations by US copyright law. US copyright law is part of federal law and authorized by the Copyright Clause of the US Constitution. Article I, Section 8, Clause 8 states that Congress shall have the power "To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."

¹³⁰⁵ "Press statistics," *Youtube.com*, http://www.youtube.com/t/press_statistics

¹³⁰⁶ "The top 500 sites on the web", <http://www.alexa.com/topsites>

¹³⁰⁷ "About essentials" *Youtube.com*, http://www.youtube.com/t/about_essentials

¹³⁰⁸ Damien O'Brien and Professor Brian Fitzgerald, "Digital copyright law in a Youtube world," *Internet Law Bulletin* 9.6 & 7 (2006): 71-74. P.1.

¹³⁰⁹ O'Brien and Fitzgerald, "Digital copyright law in a Youtube world," P.2.

¹³¹⁰ "Community guidelines," *Youtube.com*, http://www.youtube.com/t/community_guidelines

¹³¹¹ "Community guidelines," *Youtube.com*, http://www.youtube.com/t/community_guidelines

¹³¹² "Viacom will sue YouTube for \$1bn," *BBC News* (March 13, 2007), <http://news.bbc.co.uk/2/hi/business/6446193.stm>.

¹³¹³ "UPDATE: Mediaset Files EUR500 Million Suit Vs Google's YouTube," *CNN Money* (July 30, 2008), http://money.cnn.com/news/newsfeeds/articles/dif500/200807301025DOWJONESDIONLINE000654_FORTUNE5.htm.

¹³¹⁴ "Press timeline," *Youtube.com*, http://www.youtube.com/t/press_timeline

¹³¹⁵ "Press statistics," *Youtube.com*, http://www.youtube.com/t/press_statistics

The copyright act of 1976 regulated US copyright law, found mostly in title 17 of the United States Code (USC), and had been amended by fifteen anti-piracy laws at the time,¹³¹⁶ mostly expanding copyright protection, increasing infringement penalties, and creating new enforcement provisions. One of the most important amendments was the Digital Millennium Copyright Act (DMCA) of 1998, which implemented the WIPO copyright directives and added new Internet protection for copyright. It created the safe harbor provisions and anti-circumvention laws for technological protection measures.¹³¹⁷

Part of the DMCA was the Online Copyright Infringement Liability Limitation Act (OCILLA).¹³¹⁸ This created section 512 of the US copyright law, which provided provisions on liability for material online. It contained safe harbor provisions and provisions that aimed to include ISPs in enforcement. ISPs would not be liable for copyright infringement if they transmitted, routed, or provided connections for material through their system or controlled/operated network, or for transient storage of that material, if (1) another person initiated or directed the transmission, (2) the transmission, routing, etc. was carried out through an automated technical process, (3) the ISP did not select the recipients, (4) copies of the material made by the ISPs were not maintained by or accessible to others, (5) the content of the transmission was not modified in the network.

ISPs would not be liable for copyright infringement during system caching (temporary storage). Again, this was subject to conditions. One of those conditions was that if the sender of the material made the information that was cached available online without consent of the copyright holder, the ISP would remove it or disable access to it, after receiving a notification by the copyright holder. But this applied only if the material had been removed from the original site before this or if a court had ordered this removal, and if the party that sent the notification included in that notification a statement that the material had been removed from the original site.

The provision provided that ISPs would not be liable for information residing on systems or networks at direction of users, if they did not have knowledge that the material or the activity by the user was infringing, were not aware of facts or circumstances from which infringing activity was apparent, and, after having obtained such knowledge or awareness immediately removed or disabled access to the material. They were also not liable for information if they did not receive financial benefit attributable to the infringing activity (if they have the right and ability to control that activity), and removed the infringement immediately after having received a notification (which is subject to requirements described later on). It also prescribed that these limitations for liability applied only when the ISPs had designated an agent to receive notifications of claimed infringement, and made this ability to receive notifications available through its service or on their website, and by providing the US copyright office with the relevant information.

For information location tools, like directories, indexes, references, pointers or hyperlinks, that linked to infringing material, an ISP would not be liable under the same conditions as for information residing on their systems or networks at the direction of users.

When non-profit educational institutions would act as an ISP, infringement by faculty members or graduate students who were employees performing a teaching or research function would not be attributable to those institutions if the material was not recommended for instruction for a course taught, and the institution had not received more than 2 notifications.

¹³¹⁶ Amendments: 1982: Piracy and Counterfeiting Amendments Act, 1984: Record Rental Amendment of 1984, 1990: Copyright Remedy Clarification Act, 1990: Computer Software Rental Amendments Act, 1992: Audio Home Recording Act, 1994: Uruguay Round Agreements Act, 1995: The Digital Performance Right in Sound Recordings Act, 1996: Anticounterfeiting Consumer Protection Act of 1996, 1997: No Electronic Theft (NET) Act, 1998: Sonny Bono Copyright Term Extension Act, 1998: Digital Millennium Copyright Act (DMCA), 1999: Digital Theft Deterrence and Copyright Damages Improvement Act of 1999, 2004: Intellectual Property Protection and Courts Amendments Act, 2005: Family Entertainment and Copyright Act, 2008: Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act.

¹³¹⁷ 17 USC section 1201 and further.

¹³¹⁸ Online copyright infringement liability act (2006), pub. L. No. 105-304, 112 Stat. 2877 (codified at 17 U.S.C. § 512 (2006))

On the requirements of a notification the law said that it had to be a written notification, provided to the designated agent of the ISP and that it had to include a physical or electronic signature of the person authorized to act on behalf of the owner of the copyrighted work, the copyrighted work (or multiple ones) claimed to have been infringed, identification of the material that was supposedly infringing, information sufficient to contact the complaining party, a statement that the complaining party had good faith to believe that the material used was not authorized by the copyright owner, and a statement that the information in the notification was accurate, and that the complaining party was authorized to act on behalf of the copyright owner.

The law also stated that ISPs were not liable for taking down material in good faith, but had to notify the subscriber that they had taken down the material, and had to inform the notifier of the first notice when they received a counter-notification that they would reinstate the original material within 10 to 14 business days. The original notifier could counter the counter notice by going to court. A counter notification itself had to contain the physical or electronic signature of the subscriber, had to identify the material and its original location, and had to include a statement in which he or she explained that the removal was a mistake, and their name, address, and telephone number, and a statement wherein the subscriber consented to jurisdiction of the federal district court.

Notifiers and counter notifiers would be liable for misrepresentations, for damages, costs and attorney's fees.

Copyright owners and their representatives could request the clerk on any US district court to issue subpoenas to ISPs for the identification of infringers. The request had to contain a notification (the same as is necessary for notice and takedown), a proposed subpoena, and a sworn declaration that the only purpose for the subpoena was to identify infringers and that the information would only be used to protect copyrights and related rights. To the issuing of subpoenas the Federal Rules of Civil Procedure applied.

The section also prescribed that ISPs would have a policy that provided for the termination of subscribers and account holders of the ISP system or network after repeated infringement (otherwise those ISPs would not have safe harbor). ISPs also had to accommodate, and refrain from interfering with, standard technical measures which were broadly accepted by copyright owners to identify copyrighted works.

The court could, in the case of an injunction under section 502, order an ISP that either would or would not qualify for safe harbor provisions, to stop providing access to infringing material or activity, terminate the account of a subscriber, or order any other injunctive relief to the ISP to restrain infringement (the latter is only the case for other conduct that does not normally qualify for safe harbor). In granting injunctive relief, the court would have to consider whether or not such an injunction would burden the provider significantly, the likely harm suffered by the copyright owner if no steps were taken, whether it would be technically feasible or effective to grant such an injunction, and whether there were less burdensome means to prevent infringement. This injunctive relief would only be available after notice to the service provider and an opportunity for the service provider to appear was provided.

Section 512 of Title 17 of the US Code provided ISPs with protection from liability if they acted as a conduit. However, this protection only applied if those ISPs had "(A) Adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers; and (B) accommodates and does not interfere with standard technical measures."

The article did not specify the type of termination policy and how it should be applied. Thus far, it seemed that ISPs had not adopted such a policy. However, the ISP 'Suddenlink' had been reported to apply a graduated response procedure to its subscribers. They disconnected users'

Internet access for 6 months after three DMCA notices.¹³¹⁹ YouTube did the same with repeat infringers.

A counter notice would have to state, under penalty of perjury, that the material was not infringing, and should not have been removed. It would also consent to local federal court jurisdiction, giving the copyright owner the opportunity to file a lawsuit to resolve the matter once and for all. Unless the copyright owner filed a lawsuit within 14 days of the counter notice, the hosting provider could (and generally did) restore the material to its original online location. Essentially, the counter notice would tell the complaining copyright owner to “put up or shut up”.¹³²⁰

The counter notification process was created to protect alleged infringers from mistaken takedowns and misuse.¹³²¹

9.3 The procedure in practice

Google Search: Notice and Takedown

Through the “contact us” page, Google linked to a page that said “remove illegal content from Google.”¹³²² Clicking on the link would lead the complainant to a web tool that could help you remove content from Google’s services, including search, on the basis of applicable laws.¹³²³ It specifically directed them to another site if the complaint referred to content on YouTube. The web tool first asked you to specify the product to which the removal request related. This could be Gmail, Google music, or other things, including web search. Tagging “web search” would open up another box that said that a copy of each legal notice they received could be sent to the Chilling Effects project for publication and annotation (while that website would redact the contact details).¹³²⁴ Google also wrote that they could send the notice to the alleged infringer and to the rights holder (if they had reason to doubt the validity of the complaint). They could also publish the information in their transparency report.¹³²⁵

It also opened another box that allowed the complainant to specify the nature of your request, ranging from the request to remove personal confidential information from search results, or sites that engage in “suspicious behavior”, to “I have a legal issue that is not mentioned above”, which would be the way to copyright claims.

Tagging that opened yet another box that allowed the complainant to choose the legal reason for the removal request. One of the options would be: “I have found content that may violate my copyright.” Clicking it required verification that the complainant was the copyright owner, or authorized to act on behalf of the owner of an exclusive right that is allegedly infringed. Verifying this would open up a warning box, that would say that knowingly misrepresenting that material or activity is infringing, may make the complainant liable for damages. It specifically warned (in red letters) not to make false claims. Another box would ask whether the complainant had read the above and wished to proceed. After clicking Yes, another box opened that asked what the allegedly

¹³¹⁹ Ernesto, “US ISP Disconnects Alleged Pirates for 6 Months,” (24 September 2010), <https://torrentfreak.com/us-isp-disconnects-alleged-pirates-for-6-months-100924/>.

¹³²⁰ Fred Von Lohmann, “Fair use, film, and the advantages of Internet distribution.” *Cinema Journal* (2007): 128-133. P.131.

¹³²¹ Jennifer Urban and Laura Quilter, “Efficient Process or ‘Chilling Effects’? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act,” *Santa Clara Computer and High Technology Law Journal* 22 (2006): 621. P.622-623.

¹³²² “Contact,” *Google.nl*, <https://www.google.nl/intl/en/contact/>

¹³²³ “Legal Removal Requests,” *Google.com*, <http://support.google.com/bin/static.py?hl=en&ts=1114905&page=ts.cs>

¹³²⁴ www.chillingeffects.org

¹³²⁵ “Copyright removal requests,” *Google Transparency Report*, <https://www.google.com/transparencyreport/removals/copyright/>

infringing work in question was, which could be: Text, Image, Music, Video, Name/Address, Other. Videos and images could be of the complainant in question.

For the types, it specified what Google needed to know to process the complaint, and it referred to an online form, in which one had to submit their request. It requires the complainant to be logged in on a Google account in order to open this form.¹³²⁶

This form, titled “Copyright removal” allowed the complainant to report alleged copyright infringement, relating to web search. It referred to the Digital Millennium Copyright Act (and provides a link to the legal text), and “other applicable intellectual property laws.” It said that Google could remove or disable access to certain content, and/or terminate subscribers, but also that they would notify them, and that they could make the notice public. They again referred to the chilling effects project.

Furthermore, it again provided a warning that misrepresentations could make the complainant liable for damages. They referred to a court case and say that complainants must take copyright defenses, limitations and exceptions into account before sending a notice. It also referred to one case in which fair use was not taken into account, and a company was forced to pay more than 100,000 dollars in costs and attorney fees.

The infringement notification would ask the complainant to provide contact information, and the copyright holder they represent (which could be the same person). It then required that the complainant identify and describe the copyrighted work, and asked to provide an authorized example of the work. It then asked to provide the URL of the infringing material. It further asked the complainant to make a sworn statement, in which he/she swore to have good faith that the use of the copyrighted materials above was not allowed by the copyright owner, and that the information provided is accurate, and that they were, under penalty of perjury, the copyright owner, or authorized to act on behalf of the owner.

Google Search: TCRP

Around the time of my interview with them, Google released a report called ‘How Google Fights Piracy’ which could be found on their public policy blog.¹³²⁷ In this report, and in my interview with them, they talked about the Trusted Copyright Removal Program for Web Search (TCRP), an additional system to submit notices about infringing search results. It was aimed at “copyright owners who have a proven track record of submitting accurate notices and who have a consistent need to submit thousands of URLs each day.”¹³²⁸

The program streamlined the submission process, allowing its partners to submit more notices at a time. They aimed to “scale efficiently.” At the end of 2012, there were around 50 TCRP partners, whose combined takedown notices accounted for 95% of the total.¹³²⁹ So the vast majority of notices came from a small minority of submitters.

After the introduction of the TCRP system, Google search experienced substantial growth in takedown notices. They receive more takedown requests now (2013) than they did in the twelve years from 1998 to 2010 combined. The removal time on average was less than 6 hours.¹³³⁰

Google itself invested in the technology to find inaccurate notices, but also relied on the public to detect abusive notices in the transparency report.¹³³¹ At the same time, TCRP affected the

¹³²⁶ “DMCA Notice,” *Google.com*, <https://www.google.com/webmasters/tools/dmca-notice?pli=1&rd=1>

¹³²⁷ Google, *How Google Fights Piracy*, (Google Report, September 2013). See: <https://docs.google.com/a/google.com/file/d/0BwxyRPFduTN2dVFqYm15UENUeUE/edit?pli=1>

¹³²⁸ Google, *How Google Fights Piracy*, (2013) 14.

¹³²⁹ Google, *How Google Fights Piracy*, (2013) P. 14.

¹³³⁰ Google, *How Google Fights Piracy*, (2013) P. 15.

¹³³¹ Google, *How Google Fights Piracy*, (2013) P. 16.

search ranking of websites: sites that get a lot of removal requests get a lower place in their search ranking.¹³³²

In my interviews, Google commented on this program. On the trusted complainants, they said that they tended to be experienced and tended to want to be accurate. “We thought we could do better for them, without harming the accuracy of the system.” Google said the remaining notifiers have a much higher error rate.¹³³³

The system also aimed to detect and prevent abuse. For example in 2012 they terminated two partners who had a bad track record because they repeatedly sent inaccurate notices. Access to the program can thus be revoked. Google said it was “almost a market force” and that during the implementation rights holders agreed with the system (which would mean they would accept this market pressure). This market force relied on the nature of the complainants. Although movie studios said they did not want mistakes either, and while some complainants were anti piracy enforcement agencies or representatives of the music industry with their own in-house enforcement, most of the other content (software, adult, and the movie industry) relied on outside independent enforcement vendors. Degban, one of the largest complainants, focused on the adult industry for example.¹³³⁴ This created a market mechanism, because according to Google, those independent enforcement vendors “know it is very important for their ability to attract customers that they can offer the TCRP access. So they have a strong incentive to not get kicked out.”¹³³⁵

To become a trusted complainant, there was an application process. Google: “we found that there is only a small number of people who have any need for this. The standard web form allows 1000 URLs a day as a limit. There aren’t many people that want to notify more. The ones that do are usually professionals. They all talk to each other and know how to reach us.”¹³³⁶

At the start, Google contacted them. “Because we could see who actually had the volume.” Those were about 50 members. They said that it was “almost everyone.”¹³³⁷

Google said that “none of it has resulted in perfection and mistakes still happen. We are doing as good a job as we know how: as error resistant as is reasonable possible.” “We would like to do better, and we’re trying to improve.”¹³³⁸

YouTube: DMCA Notice and takedown

Whenever users would upload content to YouTube, they would receive a warning: “Do not upload TV shows, music videos or commercials without permission, unless they consist entirely of content that you created yourself.”¹³³⁹

YouTube’s website had its own “copyright on YouTube” page, dedicated to make copyright conflicts for users and rights holders easy.¹³⁴⁰

There were a number of tools available for content owners: Content owners could submit copyright infringement notifications when they believed their work was posted on YouTube without their authorization. They could do this through a web form. The website warned that submitting a notification “initiates a legal process” and advised against misuse of the process, as it “may result in the suspension of your account or other legal consequences.”

¹³³² Google, *How Google Fights Piracy*, (2013) P. 17.

¹³³³ Fred von Lohmann (Intellectual Property Director Google) interviewed by author, August 2013.

¹³³⁴ Fred von Lohmann (Intellectual Property Director Google) interviewed by author, August 2013.

¹³³⁵ Fred von Lohmann (Intellectual Property Director Google) interviewed by author, August 2013.

¹³³⁶ Fred von Lohmann (Intellectual Property Director Google) interviewed by author, August 2013.

¹³³⁷ Fred von Lohmann (Intellectual Property Director Google) interviewed by author, August 2013.

¹³³⁸ Fred von Lohmann (Intellectual Property Director Google) interviewed by author, August 2013.

¹³³⁹ “Rhodri Marsden: Why did my YouTube account get closed down?”, *The Independent* (Aug 12, 2009), <http://www.independent.co.uk/life-style/gadgets-and-tech/features/rhodri-marsden-why-did-my-youtube-account-get-closed-down-1770618.html>

¹³⁴⁰ “Copyright on Youtube,” *Youtube.com*, <http://www.youtube.com/yt/copyright/>

Apart from the web form, YouTube also accepted free-form copyright infringement notifications, submitted through email, fax, and mail.¹³⁴¹

As a defense, users could file counter notifications. This was a legal request for YouTube to reinstate a video that was removed after a notification of copyright infringement. Counter notifications could, according to the website, “only be pursued in instances where the upload was removed or disabled as a result of a mistake or misidentification of the material to be removed or disabled, such as fair use.” Counter notifications could only be submitted by the original up loader or an agent authorized to act on his or her behalf. They could be submitted through a web form as well. Those counter notifications would be forwarded to the complainant, including personal information. This process could take 10 business days. If an account was suspended for multiple violations, one could file a counter notification free-form.¹³⁴²

On the other hand, rights owners could also choose to retract their notification. This required an owner to send YouTube a statement of retraction, accompanied with the URL of the video in question and an electronic signature.¹³⁴³

Users affected by copyright claims could also try to reach rights owners directly through YouTube or its copyright desk, in search of a retraction.¹³⁴⁴

At the copyright notices section of ‘your account,’ it said whether or not videos of a user had been taken down by copyright strikes or Content ID claims.¹³⁴⁵ If a user received three copyright strikes, their account would be suspended and all the videos uploaded to that account removed. Already receiving one strike could limit a user’s access to certain YouTube features. A strike would not be the same as a Content ID match. A strike expired after six months, and after completing copyright school.¹³⁴⁶

A DMCA complaint could be filed, but needed:

- Physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right allegedly infringed.
- Identification of the work, or a list of works that allegedly infringed.
- Identification of the material that was claimed to be infringing or to be the subject of infringing activity and that was to be removed or to which access was to be disabled, and information that could permit YouTube to locate the material (usually an URL is enough).
- Information that was sufficient for YouTube to contact the complaining party (address, telephone number, email)
- Statement in which the complaining party showed the good faith belief that the way in which their material was used was not authorized.
- Statement that the information in the notification was accurate.

This information had to be send to YouTube’s designated agent.¹³⁴⁷

¹³⁴¹ “Submit a Copyright takedown notice,” *Youtube.com*, <http://www.youtube.com/yt/copyright/copyright-complaint.html>

¹³⁴² “Counter Notification Basics,” *YouTube website*, <http://www.youtube.com/yt/copyright/counter-notification.html>

¹³⁴³ “Retract a claim of copyright infringement,” *YouTube website*, <http://www.youtube.com/yt/copyright/retractions.html>

¹³⁴⁴ “Retract a claim of copyright infringement,” *YouTube website*.

¹³⁴⁵ “Understanding the copyright claim on your video,” *YouTube website*, <http://support.google.com/youtube/bin/answer.py?hl=en&answer=2818443&topic=2778545&ctx=topic>

¹³⁴⁶ “Understanding the copyright claim on your video,” *YouTube website*.

¹³⁴⁷ “YouTube help,” *YouTube website*, <http://support.google.com/youtube/bin/answer.py?hl=en&hlrm=nl&topic=10553&answer=58127>

YouTube: Content ID

Content ID was a system that allowed for the easy identification and management of copyright protected content on YouTube. YouTube had a database of files, submitted to it by content owners. New content was scanned against that database, and whenever content was recognized, the policy chosen by the rights holder would be applied, varying between: Monetization (Ads), Block (video is no longer visible, or audio muted), Track (owner can keep track of viewership statistics).¹³⁴⁸

Content ID matches could be disputed. Users could fill out a short form with the reason for the dispute. YouTube would then notify the content owner, who would uphold the match, or not. Users could then appeal this as well.¹³⁴⁹

Content ID scanned over 100 years of video's each day. More than 3000 partners used Content ID, including the most important American TV-networks, film studios and music labels. These partnerships were only engaged with rights holders that offered a large body of protected material that is frequently uploaded to YouTube. This excluded smaller rights holders. Content ID had over 8 million reference files (more than 500,000 hours of material) in the Content ID database. This number in 2013 was twice the number of reference files it had in 2012. More than one third of all the content on YouTube that allowed for income used Content ID. More than 120 million videos had been claimed through Content ID at the time. More than 1 billion had been paid to rights holders through the Content ID program alone.¹³⁵⁰

Enforcers:

Digimarc Guardian

Digimarc was a technology company based in Beaverton, Oregon (USA).¹³⁵¹ According to the company website, they enabled "businesses and governments worldwide to enrich everyday living with the means to identify all forms of content, including audio, video and imagery. We develop solutions, license intellectual property and provide development services to business partners across a wide range of industries."¹³⁵²

Their 'Guardian' department was the anti-piracy department. According to the website, they were a "global leader in protecting books, publications and documents from the threat of digital piracy. Our service finds and removes pirated content across the web to protect publisher revenues and author rights through an integration takedown process that delivers high removal rates across various website types."¹³⁵³ They were formerly called 'Attributor Guardian.'

According to the company themselves, they "protect books, journalism, audio books." They claimed to be the "leading forensic company protecting the intellectual property rights of books and documents."¹³⁵⁴

To do this, they brought in "metadata from customer, like for example a title, ISBN, names, and then automate crawling of the net." They had software for this. They said they looked at thousands of websites but that it was different for each customer.¹³⁵⁵

When they found content, they said they looked at it, and had two separate people that verified that it was a full copy of their content and that it was infringing.¹³⁵⁶

¹³⁴⁸ "How Content ID works," *YouTube website*, <http://support.google.com/youtube/bin/answer.py?hl=en&answer=2797370>

¹³⁴⁹ "Dispute a Content ID claim," *YouTube website*.

¹³⁵⁰ "Press Statistics," *YouTube website*, http://www.youtube.com/t/press_statistics

¹³⁵¹ "Digimarc Company Overview," *Digimarc website*, <http://www.digimarc.com/company>

¹³⁵² "Digimarc Company Overview," *Digimarc website*, <http://www.digimarc.com/company>

¹³⁵³ "Digimarc Guardian," *Digimarc website*, <http://www.digimarc.com/guardian>

¹³⁵⁴ Digimarc Guardian, interviewed by author, October 2013.

¹³⁵⁵ Digimarc Guardian, interviewed by author, October 2013.

After that, enforcement started. This meant they could send a takedown notice. According to them: “in some cases we send customers a list of files so they can decide which ones they want us to go after and which ones they don’t. This applies especially to the journal side – people can send a different notice.”¹³⁵⁷ Also, “sometimes somebody doesn’t want to send a notice.”¹³⁵⁸

To prevent errors, they said they “have lots of people working, across the globe,” because it was “very important to us and our customers that we don’t send something out that’s incorrect.”¹³⁵⁹

On false positives they said that they themselves “don’t take anything down.” And that it “happens infrequently that it goes wrong. We’ve been good and lucky so far. We have to be very careful.”¹³⁶⁰

DtecNet

DtecNet was a company owned by the company Markmonitor. On its website Markmonitor called itself the “global leader in enterprise brand protection,” and said that “more than half the Fortune 100 depend on Markmonitor to help safeguard their brands online.”¹³⁶¹ Apart from ‘brand protection’, Markmonitor also published reports on the “prevalence of brand abuse on the Internet.”¹³⁶²

In my interviews, DtecNet said they were networks of computers all over the world that examined sources of content. They claimed to identify and validate when content was infringing, which they did in a number of ways: “we look at signatures, we do human validation in some cases (like for high profile content or in a high profile environment), and there are hundreds and hundreds of servers engaged in this activity.” They do “lots of technical crawling and combing of data.”¹³⁶³

They had 80 people working on this, from a customer/technology service perspective, according to DtecNet. They said these people dealt with the content sources they “police” and that they policed on behalf of organizations that tried to protect the rights or artists. Bu they also said they enforced on behalf of individual producers of content. Mostly they identified things, and they did not deal with end users. The only direct enforcement they did was notice and takedown, and “claimed infringement kind of work.”¹³⁶⁴

They said they did more human validation in high profile cases, which were for example pieces of content on a network of a large media producer. They said: “before we take down something that is on a high profile media site, we validate it, because of the risk of error.” “When it occurs on a legitimate site and not on sites that engage in trading of music or movies. We’re talking about big legitimate media sites. Those need more validation.”¹³⁶⁵

Their customers included “Music, television, movies, live performances, sports, books, all sort of flavors of media.” They did direct enforcement, like notice and takedown, and also supplied notices of claimed infringement, for escalation path enforcement they supply data. They also said “we are not in a position to judge the intent, or where/how it occurs, so we pass that off to some of the organizations that are better suited at that, we just play it off. We find and identify as likely infringement.”¹³⁶⁶

¹³⁵⁶ Digimarc Guardian, interviewed by author, October 2013.

¹³⁵⁷ Digimarc Guardian, interviewed by author, October 2013.

¹³⁵⁸ Digimarc Guardian, interviewed by author, October 2013.

¹³⁵⁹ Digimarc Guardian, interviewed by author, October 2013.

¹³⁶⁰ Digimarc Guardian, interviewed by author, October 2013.

¹³⁶¹ “Company,” *Markmonitor website*, <https://www.markmonitor.com/company/>

¹³⁶² “Markmonitor,” *Wikipedia.org*, <http://en.wikipedia.org/wiki/MarkMonitor>

¹³⁶³ Fred Felman (DtecNet) interviewed by author, November 2013.

¹³⁶⁴ Fred Felman (DtecNet) interviewed by author, November 2013.

¹³⁶⁵ Fred Felman (DtecNet) interviewed by author, November 2013.

¹³⁶⁶ Fred Felman (DtecNet) interviewed by author, November 2013.

DtecNet also mentioned that the data they collected were often more valuable than notices sent to take down. “Data on piracy is very indicative of demand and popularity, so data is used for those purposes as well.” So clients can use this data to map consumption patterns.¹³⁶⁷ “Is the pricing strategy right? The translation? Are there legitimate distribution channels in a region?”¹³⁶⁸

Brein

Brein was the main copyright enforcement authority in the Netherlands, financed by collective rights organizations and trade organizations.¹³⁶⁹ To enforce, they focused on two things: they took action against specific titles, and against “unlawful” sites.

They had a large database containing copies of protected content, and rights holders authorized them to enforce on their behalf. They developed special in-house software that scanned the Internet for unauthorized content, or for links pointing towards unauthorized content.¹³⁷⁰

This is what happened at Google search. They used the TRCP to be able to do that. About taking content down, the director Tim Kuik said: “you can’t just do that. You have to show that you are a trustworthy notifier.” He also said it did require some start up time setting up a system like that. “Right now we are at more than 10,000 notifications per day, and they are all removed. Sometimes a notification is refused, but we can always show that it should’ve been removed. We have never had wrongful notifications yet.”¹³⁷¹ He did say about 1% is returned: “very sporadic.” And that it was necessary to notify in the right way, because “reputation is important.”¹³⁷²

At Google search, through the TRCP, Brein removed about 11,000 links per week. They said this also depended on the amount of titles in your data base. Brein performed well, they said, because they had the capacity and the right software. “Software with 100% score results and cases of doubt that need to be checked by people.”¹³⁷³

In other cases, rights holders notified them about infringing content.¹³⁷⁴ So one of the things Brein did was enforce, when requested by the rights holder. This happened at YouTube mostly. They did not scan for content there, except for when the rights holders told them. This was because rights holders could also choose to participate in the exploitation model of YouTube.¹³⁷⁵

Brein employed 12 people and was financed by collective rights organizations and branch organizations.¹³⁷⁶

RIAA

The Recording Industry Association of America (RIAA) represented the music industry and was also one of the larger players doing many takedowns from Google search. When asked how they found, verified, and took down infringing content, they told me in an email: “First, we ourselves don’t take down anything, but we submit take down notices to Google after we have confirmed that a file is illegal. We do that by employing a hash-matching technology that identifies replicas of music files to ensure that the file is indeed an identical, copyrighted song owned by one of our members. Google provides us, along with other content owners,

¹³⁶⁷ Fred Felman (DtecNet) interviewed by author, November 2013.

¹³⁶⁸ Fred Felman (DtecNet) interviewed by author, November 2013.

¹³⁶⁹ Tim Kuik (BREIN), email to author, July 2013.

¹³⁷⁰ Tim Kuik (BREIN), email to author, July 2013.

¹³⁷¹ Tim Kuik (BREIN), interviewed by author, May 2013.

¹³⁷² Tim Kuik (BREIN), interviewed by author, May 2013.

¹³⁷³ Tim Kuik (BREIN), interviewed by author, May 2013.

¹³⁷⁴ Tim Kuik (BREIN), interviewed by author, May 2013.

¹³⁷⁵ Tim Kuik (BREIN), interviewed by author, May 2013.

¹³⁷⁶ Tim Kuik (BREIN), interviewed by author, May 2013.

an automated tool to submit takedown notices. After our staff reviews the matched file, we send the notice to Google via the tool. As you note, Google allows content owners to increase the number of take downs requested if the take downs consistently prove accurate and in good faith, and Google has increased our limit several times.”¹³⁷⁷

Regarding the amount of takedowns they did at YouTube, they said: “I don’t know the exact frequency, but it is fair to say very rarely given our members have business relationships with YouTube and much of the music content is monetized in some way. RIAA is not involved in those business decisions.”¹³⁷⁸

9.4 Scale, severity and procedural safeguards

Scale

Google search (DMCA and TCRP)

On its ‘Google transparency report’, Google showed the amount of URLs they were asked to remove, who submitted the notices, on behalf of which copyright owners, and for which websites.¹³⁷⁹

Originally there were restrictions on the amount of URLs that could be taken down, but they had been removed for complainants with a good reputation, like the RIAA and Brein.¹³⁸⁰

In total, the amount of takedown requests gradually rose over the years. In 2013, Google received 235 million takedown requests from rights holders. They acted on 91% of those requests, but rejected 21 million of them because they were illegitimate or because the links had already been removed.¹³⁸¹

According to Google’s website; “Google is a leader in addressing the concerns of copyright owners, responding to more copyright removal notices, and faster, than ever before. During 2012, copyright owners and their agents sent us removal notices for more than 57 million web pages. Our turnaround time on those notices was, on average, less than 6 hours. That’s faster than we managed in 2011, despite a 15-fold increase in the volume of requests.”¹³⁸²

In 2012 Google received 50 million requests, compared to 10 million in 2011. The track records of companies differed. For NBC, Fox, and Lynda, more than a quarter of their requests were refused. The most active reporting organizations were in the music industry: BPI sent 41.7 million requests. The RIAA sent 30.8 million requests. In the case of 11% of BPI requests, no action was undertaken. That corresponded to 520,000 links. Lynda has the worst track record. Google took no action for 57% of the 1,178,809 URLs the company sent in. RIAA, Adobe and Brein had the best track record, because only 2% was refused.¹³⁸³

The biggest notifier was Degban, which represented the adult industry. They reported over 65 million URLs. MarkMonitor (which includes DtecNet) is at over 23 million URLs. Brein reported a

¹³⁷⁷ Cara Duckworth (Communications at the Recording Industry Association of America) email to author, October 2013.

¹³⁷⁸ Cara Duckworth (Communications at the Recording Industry Association of America) email to author, October 2013.

¹³⁷⁹ “Copyright removal requests,” *Google Transparency Report*, <https://www.google.com/transparencyreport/removals/copyright/>

¹³⁸⁰ Ernesto, “Google relaxes DMCA Takedown restrictions, eyes abuse,” *Torrentfreak* (April 11, 2013), <http://torrentfreak.com/google-relaxes-dmca-takedown-restrictions-eyes-abuse-130411/>.

¹³⁸¹ Ernesto, “Google discarded 21,000,000 takedown requests in 2013’, *Torrentfreak* (December 27, 2013), <http://torrentfreak.com/google-discarded-21000000-takedown-requests-in-2013-131227/>.

¹³⁸² Google, *How Google Fights Piracy* (2013).

¹³⁸³ Ernesto, “Google discarded 21,000,000 takedown requests in 2013’, *Torrentfreak* (December 27, 2013), <http://torrentfreak.com/google-discarded-21000000-takedown-requests-in-2013-131227/>.

fairly high number of allegedly infringing links for a national organization,¹³⁸⁴ and attributed this high number to their capacity and the right software.¹³⁸⁵ Brein removed over 2,9 million URLs at the time of this research. Digimarc stood at almost 2 million URLs, but that figure could be higher, as Digimarc resurfaced under different names in the transparency report (like the company Attributor).¹³⁸⁶

This means that in terms of scale, the TCRP allowed for the takedown of hundreds of millions of links. It was more difficult to estimate the amount of takedowns by others. Google themselves wrote that the TCRP accounted for 95% of the total, which would mean other takedowns still range in the millions.¹³⁸⁷

YouTube (DMCA and ContentID)

The amount of takedowns at YouTube was much smaller than it was at Google search, according to Google. Details on these takedowns, or even the amount, were not published, but in terms of Google services, the amount ranked at second place, after search.

There were many reasons for not publishing these details. First of all, it was difficult to measure, according to Google. The vast majority of rights holders opted for Content ID, which was a separate thing from notice and takedown. There were also engineering reasons. For example, takedowns could come in different forms, like email, or fax even, according to Google. There were more products for which they did not publish these details at Google.¹³⁸⁸

Brein confirmed the smaller scale. Most rights holders handled takedowns themselves instead of asking representatives. They estimated the amount of YouTube takedowns they did at about hundreds per month.¹³⁸⁹

Content ID in turn, happened on an enormous scale. They said they did not publish the numbers, but what they could say was that there were 72 hours of video uploaded to YouTube every minute, and that Content ID immediately scanned all the new content, plus that it rescanned all existing videos (which applies when new digital fingerprints are added to Content ID).¹³⁹⁰

They had over 4,000 content ID partners, with many millions of fingerprints in the database. However, the majority of those partners monetized, and did not block videos.¹³⁹¹ The program scanned over 250 years of video each day, claimed more than 200 million videos, and had over 1.5 million active reference files.¹³⁹² In terms of scale, it was difficult to estimate based on the information available. We know that after a couple of years, the program had claimed more than 200 million videos, but there was no information on the general takedowns. However, recent information released on Youtube can help this estimation, although this information is from 2015 and 2016, and falls outside of the scope of this research. An article from 2015 claims that in 2014 alone, 180 million infringing videos were taken down from Youtube.¹³⁹³ In a newer report from Google on how it fights piracy, the company claims that 98% of all takedowns run through the Content ID program.¹³⁹⁴ This still leaves millions of general takedowns.

¹³⁸⁴ "Reporting organizations", *Google Transparency Report*, <https://www.google.com/transparencyreport/removals/copyright/reporters/?r=all-time>

¹³⁸⁵ Tim Kuik (BREIN), interviewed by author, May 2013.

¹³⁸⁶ "Reporting organizations", *Google Transparency Report*, <https://www.google.com/transparencyreport/removals/copyright/reporters/?r=all-time>

¹³⁸⁷ Google, *How Google Fights Piracy*, (2013) P. 14.

¹³⁸⁸ Fred von Lohmann (Intellectual Property Director Google) interviewed by author, August 2013

¹³⁸⁹ Tim Kuik (BREIN), interviewed by author, May 2013.

¹³⁹⁰ Fred von Lohmann (Intellectual Property Director Google) interviewed by author, August 2013.

¹³⁹¹ Fred von Lohmann (Intellectual Property Director Google) interviewed by author, August 2013.

¹³⁹² Google, *How Google Fights Piracy*, (2013) P. 10.

¹³⁹³ Zach Miners, "Google scores a win in SOPA-tinged Mississippi case," *PC World* (2 March 2015), <http://www.pcworld.com/article/2891852/google-scores-a-win-in-sopatinged-mississippi-case.html>

¹³⁹⁴ Google, *How Google Fights Piracy*, (Google, 2016 report) P.26.

Although users could be blocked from YouTube after receiving three strikes (because they uploaded infringing content three times for example), this was actually uncommon according to Google. They spoke of a “Very very small number.” In fact, the vast majority of users did not have a single strike. Content ID protected users from strikes, because an initial match would not (automatically) result in a strike. Regarding the partners, larger right holders understood Content ID, Google says, but smaller ones were not yet familiar with it.¹³⁹⁵

If users disputed whether certain content should be monetized or blocked, it could escalate into a DMCA notice (if the rights holder would insist). Then, that user could get a strike. One strike already led to punishments in copyright school.¹³⁹⁶

Rights holders often complained about Multiple Channel Networks (MCN) content. Google said: “We say clear you own rights.”¹³⁹⁷

This makes it clear that ContentID was applied on an enormous scale and manual takedowns still happen on a very large scale as well.

Severity

The severity of takedowns by Google search (in both normal takedowns and the TCRP) meant that search results were delisted worldwide.

YouTube was a different story. The severity of these takedowns involved blocking videos. YouTube has been a popular website, used for public dialogue, which meant removal could have negative effects on free speech. Another option, offered by the ContentID program, would be to monetize (Ads) the video, block (video is no longer visible, or audio muted) it, or track the viewership statistics.¹³⁹⁸ At the time, there was no data on how these choices were distributed. However, recent information released on YouTube can help this estimation, although this information is from 2016, and falls outside of the scope of this research. In a newer report from Google on how it fights piracy, the company claims that 90% of all videos are monetized.¹³⁹⁹

If YouTube uploaders upload content illegally, this would result in a copyright strike. One strike would lead to punishments in YouTube’s “copyright school”, an educational tool intended to teach uploading users about copyright by obligating them to follow “class” before continuing their usage of the site. Users (which could involve artists) could be banned from YouTube after receiving three strikes for uploading illegal content and have all their videos removed.¹⁴⁰⁰ ContentID claims would not result in a strike.

Safeguards

The DMCA received severe criticism in the past, because it allowed for abuse. The most common abuses of the DMCA reported were that notices that often superseded fair use doctrine, that they were also often sent by people other than the copyright holder, and third, that they were used for

¹³⁹⁵ Fred von Lohmann (Intellectual Property Director Google) interviewed by author, August 2013.

¹³⁹⁶ Fred von Lohmann (Intellectual Property Director Google) interviewed by author, August 2013.

¹³⁹⁷ Fred von Lohmann (Intellectual Property Director Google) interviewed by author, August 2013.

¹³⁹⁸ “How Content ID works,” *YouTube website*,

<http://support.google.com/youtube/bin/answer.py?hl=en&answer=2797370>

¹³⁹⁹ Google, *How Google Fights Piracy*, (Google, 2016 report) P.6.

¹⁴⁰⁰ “Understanding the copyright claim on your video,” *YouTube website*,

<http://support.google.com/youtube/bin/answer.py?hl=en&answer=2818443&topic=2778545&ctx=topic>

censorship.¹⁴⁰¹ Similarly, YouTube's Content ID system has been the subject of much criticism for disregarding fair use.¹⁴⁰²

Privacy

The question is to what extent personal data are processed, stored or used to enforce copyrights in this strategy.

For Google search and YouTube, rights holders could 'spot' the infringement themselves, by searching for it. On a large scale, all enforcers, whether being the rights holders themselves or independent enforcement vendors hired by rights holders, said they used automated software to spot infringement. The section on the procedure in practice shows that infringement required crawling of the web and scanning content for matches with a catalog of copyright protected content, and was therefore not privacy invasive. In the case of Google search, none of these enforcement actions directly involved the infringer, unless the removed search result was put up by a Google tools user, who would be sent a notification. However, rights holders did not have access to this data.

In the case of YouTube, infringement would relate back to a YouTube user. This was in part a public profile that involved a Google account. Contacts initially ran through Google but could escalate to a more official legal process. However, complainants had no access to personal details unless the process escalated that far.

Impartial, competent and independent judge

Ten years before this research, a review of the law had been done by Urban and Quilter. They noted that it was difficult to review takedown notices, because they were private actions (like cease-and-desist letters) and therefore not part of the public record.¹⁴⁰³ The Chilling Effects Project by various law schools and the Electronic Frontier Foundation collected numerous letters, including notices received by Google inc., to examine their questions.

They collected cease-and-desist letters between 2002 and 2005 and said that they noticed that they were mostly sent by corporations and business entities, and that there were few individual senders. There were also a lot of repeat senders. According to the research, the targets of the notices were often competitors of the complainants (41%). One third of the notices were flawed. There was an "unfortunately high incidence of questionable uses of the process."¹⁴⁰⁴

In their evaluation of the DMCA notice and takedown provisions as applied by ISPs (in the research, also Google), they referred to the procedure as "ISPs self-interested mediation of copyright infringement instead of official and neutral judicial mediation."¹⁴⁰⁵ Google would lose its safe harbor in the case of erroneous inaction, and would have an incentive to judge in favor of the claimant. They had less to lose if they erroneously did so.

This created incentives for ISPs in the DMCA Notice and takedown procedures that made ISPs err on the side of caution and more likely to go with accusations to not lose their safe harbors. This led to some complaints about ISP compliance departments being too eager to remove legitimate content protected by fair use or other defenses, and caving in to "overzealous rights holders."

¹⁴⁰¹ Jeffrey Cobia, "The Digital Millennium Copyright Act Takedown Notice Procedure: Misuses, Abuses, and Shortcomings of the Process," *Minn. J.L. Sci. & Tech.* 10 (2008): 387. P.392.

¹⁴⁰² Fred von Lohmann, "Testing YouTube's Audio Content ID System," *Electronic Frontier Foundation* (April 29 2009), available at <https://www.eff.org/deeplinks/2009/04/testing-youtubes-aud>

¹⁴⁰³ Jennifer Urban and Laura Quilter, "Efficient Process or 'Chilling Effects'? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act," *Santa Clara Computer and High Technology Law Journal* 22 (2006): 621.

¹⁴⁰⁴ Urban and Quilter, "Efficient Process or 'Chilling Effects'?"

¹⁴⁰⁵ Urban and Quilter, "Efficient Process or 'Chilling Effects'?" P.639.

As a judge in Google Search takedowns and YouTube, Google could hardly be seen as impartial for the reasons stated above. In the large-scale process of the TCRP, Google removed itself from the process as an adjudicator, by effectively placing that burden on the plaintiffs themselves. Their position could hardly be seen as impartial or independent, although Google created an additional safeguard by awarding reputation and discouraging wrongful takedowns. For ContentID, the other large-scale process, the process was completely automated.

In my interviews, I investigated this relationship further. It was interesting that neither party was willing to take full responsibility for the takedown of content. For example, when asked about the possibilities of false positives, Digimarc Guardian said that they themselves “don’t take anything down.”¹⁴⁰⁶ When asked about how they found, verified and took down infringing content, the RIAA said: “First, we ourselves don’t take down anything, but we submit take down notices to Google after we have confirmed that a file is illegal.”¹⁴⁰⁷ Google in turn said the responsibility to submit notices fell on the rights holder and that they had taken steps to encourage that responsibility, for example through the trusted removal program.¹⁴⁰⁸

The notifying parties (rights holders and their representatives) were the first parties to judge whether content was infringing. They had an obvious interest in the process. Some enforcers had business models that required them to submit a specific number of notices for their client. This could incentivize a broader application of copyrights than necessary, or cause those parties to err on the side of more enforcement. On the other hand, the TCRP was based on reputation. As Google mentioned, independent enforcement vendors had a strong financial incentive to be part of the program. And if they submitted too many notices erroneously, they were kicked out. Google said that when too many wrong notices were sent, “we take it seriously, check, and contact them about it.” They ask them: “What happened here? What are you going to do to make sure it doesn’t happen again?”¹⁴⁰⁹

The Electronic Frontier Foundation claimed that even those “teeny percentages” of erroneous takedowns were troublesome. They said that it was still a large amount considering the total takedowns ranged in the millions.¹⁴¹⁰

Google said it was actually quite rare that TCRP members made mistakes. They said the error rate was much higher for casual submitters. These casual submitters could have other motives for takedowns too, like censorship. But Google said that the “pure bad guys always submit in low volume,” and that there were a number of procedures, both algorithmic and human to filter this out. They however conceded that this was sometimes very hard to catch.¹⁴¹¹ They gave an example of a claim over a content website that was backdated to make it appear as if the content had been put up earlier and therefore the copyright claim would be merited. These things were hard to check, according to Google.¹⁴¹²

Presumption of innocence

The procedure put the burden of proof on the notifying parties. For both Google search and YouTube the infringement notification asked the complainants to provide detailed information about themselves, the protected work and the infringement. In both cases some form of a sworn statement was required to submit the notice (for more details, see the section on the procedure in practice).

¹⁴⁰⁶ Digimarc Guardian, interviewed by author, October 2013.

¹⁴⁰⁷ Cara Duckworth (Communications at the Recording Industry Association of America) email to author, October 2013.

¹⁴⁰⁸ Fred von Lohmann (Intellectual Property Director Google) interviewed by author, August 2013.

¹⁴⁰⁹ Fred von Lohmann (Intellectual Property Director Google) interviewed by author, August 2013.

¹⁴¹⁰ Corynne McSherry (Intellectual Property Director Electronic Frontier Foundation) interviewed by author, September 2013.

¹⁴¹¹ Fred von Lohmann (Intellectual Property Director Google) interviewed by author, August 2013.

¹⁴¹² Fred von Lohmann (Intellectual Property Director Google) interviewed by author, August 2013.

Although the system required some information to process takedown requests, it was not clear if it checked for how infringement takes place, whether it took place over a long time, what the purpose was of the infringement, and to what extent the infringement affected the artist. So although there was some burden of proof on the notifying parties, it was unclear how much weight this burden was given.

Although the system repeatedly warned against abuse/misuse, those warnings could only potentially lead to sanctions or trouble for the notifying party after the takedown had taken place. Arbitrators in this case did not evaluate the complaints, although Google said they had a system “algorithmic and human to catch mistakes in the pile.”¹⁴¹³ Urban and Quilter called the DMCA notice and takedown process “an extra-judicial temporary restraining order, based solely on the copyright holder’s allegation of copyright infringement.”¹⁴¹⁴

To highlight failed takedowns, the Electronic Frontier Foundation created the “Takedown Hall of Shame”,¹⁴¹⁵ that exposed erroneous takedowns. There have been numerous, like in the case when “Cyberpranksters” removed all of Justin Bieber’s videos from YouTube.¹⁴¹⁶ There were hardly economic or legal costs to penalize copyright holders for sending wrong or overbroad copyright notices. This incentivized them to send notices for cases of questionable infringement, *de minimis* infringement, or in clear cases of fair use.¹⁴¹⁷

A problem with a lot of these takedowns was that they disregarded fair use exceptions. For example, a mother posted a video on YouTube, of her toddler dancing to a Prince song.¹⁴¹⁸ Even though it was blurred sound, and only 29 seconds, Universal Music Publishing Group (UMPG) claimed the use of the song infringed their copyrights. YouTube removed access to the video, but reinstated it after a counterclaim. EFF filed suit against UMPG to protect the free speech rights of the mother. The judge rules that from then on, copyright owners had to consider fair use before issuing take down notices.¹⁴¹⁹ The above however suggests that the burden of proof still moved towards the defendant, or the uploading user in this case.

For the larger scale applications of notice and takedown, the sheer volume could make it difficult for notifying parties to assure the correctness of their notifications. Those notifying parties said they validated what they took down, but it is still clear that Google did not act in many cases. It is also unclear how those notifying parties made sure they validated what they took down. Digimarc for example had two separate people that validated for each notification, and DTECNET said they had more human validation in cases of high profile content. It was however uncertain how they were able to validate every notification considering the thousands of notices sent out (to this Digimarc responded: “we have a lot of people working here”).¹⁴²⁰

For Content ID, there had been a lot of criticism, mainly because Content ID is a “system where the accuser can serve as the judge, jury, and executioner,” and because the system did not understand context and parody. It has been called a system of “algorithmic copyright cops.”¹⁴²¹ For example, if a channel would use clips of video games to review them, this might be recognized as a

¹⁴¹³ Fred von Lohmann (Intellectual Property Director Google) interviewed by author, August 2013.

¹⁴¹⁴ Urban and Quilter, “Efficient Process or ‘Chilling Effects?’” P. 639

¹⁴¹⁵ “Takedown Hall of Shame,” *Electronic Frontier Foundation*, <https://www.eff.org/takedowns>.

¹⁴¹⁶ “Justin Bieber Music Videos Yanked from YouTube,” *TMZ* (August 29, 2011), <http://www.tmz.com/2011/08/29/justin-bieber-music-video-vevo-youtube-hacked-ilcreation-baby-somebody-to-love-that-should-be-me/>.

¹⁴¹⁷ Charles W. Hazelwood Jr, “Fair Use and the Takedown/Put Back Provisions of the Digital Millennium Copyright Act,” *Idea* 50 (2009): 307. P.307.

¹⁴¹⁸ Still online: “Let’s Go Crazy”, *YouTube*, <https://www.youtube.com/watch?v=N1KfJHFWlhQ>

¹⁴¹⁹ *Stephanie Lenz v. Universal Music Group Corp., Universal Music Publishing, Inc., and Universal Music Publishing Group*, No. C 07-3783, Second Amended Complaint (N.D. Cal. Apr. 18, 2008).

¹⁴²⁰ Digimarc Guardian, interviewed by author, October 2013.

¹⁴²¹ Geeta Dayal, “The Algorithmic Copyright Cops: streaming video’s robotic overlords,” *Wired* (June 9, 2012), <http://www.wired.com/threatlevel/2012/09/streaming-videos-robotic-overlords-algorithmic-copyright-cops/all/>.

copyright violation, although it would technically qualify as fair use. There were no rules of evidence at play here.

Notice, right to be heard (prior to conviction), defenses and appeal

Alleged infringers were subject to removal (or silence) of their expressive materials, before they received a notice of the complaint.¹⁴²² For Google search and YouTube, only after their material had been removed, did they receive a notice. This applied to YouTube users, who would receive a notification on their Google account, and in case of the TRCP Google notified webmasters (if they used Google's webmaster Tools) that a webpage in their domain had received a takedown notice.¹⁴²³ There was no right to be heard prior to conviction for any of the different takedowns.

Users only entered the process after the blocking took place. They could object the takedown, and file a counter notice. In this counter notice, they had to notify the original complainant that the material did not infringe copyrights. If the original complainant would not bring a lawsuit at district court within 14 days, the content would be restored.¹⁴²⁴ This situation remained in place as long as the holder was willing to sue within the 10-14 days, and regardless of the likelihood of success "on the merits."¹⁴²⁵

At YouTube, users could also file counter notifications as a defense. This was a legal request for YouTube to reinstate a video that was removed after a notification of copyright infringement. Counter notifications may, according to the website, "only be pursued in instances where the upload was removed or disabled as a result of a mistake or misidentification of the material to be removed or disabled, such as fair use." Counter notifications could only be submitted by the original up loader or an agent authorized to act on his or her behalf. They could be submitted through a web form as well. Those counter notifications, including the personal information of the plaintiff, would be forwarded to the complaining party. This process would take 10 business days. If the account of the plaintiff was suspended for multiple violations, they could file a counter notification free-form.¹⁴²⁶ Counter notifications were rarely sent, and few cases actually went to trial.¹⁴²⁷

Remedies available to people whose expression was improperly subject to a takedown were generally limited to situations where there was "knowing material misrepresentation" by the entity filing the DMCA notice. That was a difficult standard to meet, legally speaking.¹⁴²⁸ It also required a lawyer and was therefore costly for end users.

According to the statute, the material, after removal, had to stay down at least 10-14 days. This could affect human rights, especially where it concerned expressions that could suffer by being postponed by numerous days (like a call to protest, etc).¹⁴²⁹ The EFF said: "it all depends on whether you care whether speech gets taken down for a week. Speech should not be taken down. We take it seriously." Being careful about speech should be the rule. For copyright everyone all of the sudden forgets."¹⁴³⁰ It was also difficult to hold someone responsible for a bogus takedown.¹⁴³¹

¹⁴²² Urban and Quilter, "Efficient Process or 'Chilling Effects'?" P.636.

¹⁴²³ Google, *How Google Fights Piracy*, (2013) P.15.

¹⁴²⁴ "The Digital Millennium Copyright Act of 1998 - U.S. Copyright Office Summary" (December 1998). P.12. See: <http://www.copyright.gov/legislation/dmca.pdf>

¹⁴²⁵ Urban and Quilter, "Efficient Process or 'Chilling Effects'?" P. 639.

¹⁴²⁶ "Counter Notification Basics," *YouTube website*, <http://www.youtube.com/yt/copyright/counter-notification.html>

¹⁴²⁷ Jeffrey Cobia, "The Digital Millennium Copyright Act Takedown Notice Procedure: Misuses, Abuses, and Shortcomings of the Process," *Minn. J.L. Sci. & Tech.* 10 (2008): 387. P. 392.

¹⁴²⁸ Urban and Quilter, "Efficient Process or 'Chilling Effects'?" P.639.

¹⁴²⁹ Jennifer Urban and Laura Quilter, "Efficient Process or 'Chilling Effects'? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act," *Santa Clara Computer and High Technology Law Journal* 22 (2006): 621. P.637.

¹⁴³⁰ Corynne McSherry (Intellectual Property Director Electronic Frontier Foundation) interviewed by author, September 2013.

Content ID originally lacked a dispute mechanism, but added one after criticism.¹⁴³² This dispute mechanism could escalate in a DMCA notice (if the rights holder would insist the takedown was correct) and into a strike for the uploading user. One strike led to punishments in copyright school.¹⁴³³ The ContentID dispute mechanism allowed users to fill out a short form with the reason for the dispute. YouTube would then notify the content owner, who would uphold the match, or not. Users could then appeal this as well.¹⁴³⁴

It was only after the whole process that the notice and counter notice could escalate into a legal trial.

Transparency

The design and implementation of Google's copyright enforcement program was made public in numerous ways.

The DMCA procedure itself was the result of a public legislative process. How Google applied it was revealed in their document called 'How Google fights Piracy' which described the different options available to copyright holders.¹⁴³⁵

Apart from that, Google took numerous steps to improve transparency: they launched a Transparency report website in 2012. The website showed the amount of URLs they were asked to remove, the different complainants, the copyright owners represented, and the websites that were delisted.¹⁴³⁶ According to Google, they were "basically crowd sourcing corrections. Torrentfreak does a good job to embarrass copyright owners to embarrass them. The responsibility for takedown notices falls on copyright owners."¹⁴³⁷

They notified webmasters (if the use Google's webmaster Tools) that a webpage in their domain had received a takedown notice.¹⁴³⁸

They informed users by displaying a message in search results that a result had been removed. The result would then say: "In response to a complaint we received under the US Digital Millennium Copyright Act, we have removed 1 result(s) from this page. If you wish, you may read the DMCA complaint that caused the removal(s) at ChillingEffects.org."¹⁴³⁹

Meanwhile they provided copies of notices to Chilling Effects, which was a website that also gathered removal notices from other services like Twitter, and facilitated research of those notices.¹⁴⁴⁰

For YouTube, this was different. The amount of takedowns was "smaller than for Google search." Those takedowns were not published. According to Google, the takedowns were "not very illuminating" because they did not include ContentID, which would be a large omission. Google said they "are always trying to make more data available" but that there were policy reasons for not doing so in the case of YouTube, and that there were engineering reasons for not having published them yet.¹⁴⁴¹

¹⁴³¹ Mike Masnick, "Why It is Almost Impossible To Get Punished For A Bogus DMCA Takedown," *Techdirt* (October 17, 2012), <http://www.techdirt.com/articles/20121017/10355320733/why-its-almost-impossible-to-get-punished-bogus-dmca-takedown.shtml>.

¹⁴³² <http://fairusetube.org/youtube-copyfraud> and <http://fairusetube.org/articles/25-content-id-victory>

¹⁴³³ Fred von Lohmann (Intellectual Property Director Google) interviewed by author, August 2013.

¹⁴³⁴ "Dispute a Content ID claim," *YouTube website*.

¹⁴³⁵ Google, *How Google Fights Piracy* (2013).

¹⁴³⁶ "Reporting organizations", *Google Transparency Report*,

<https://www.google.com/transparencyreport/removals/copyright/reporters/?r=all-time>

¹⁴³⁷ Fred von Lohmann (Intellectual Property Director Google) interviewed by author, August 2013.

¹⁴³⁸ Google, *How Google Fights Piracy*, (2013) P.15

¹⁴³⁹ Google, *How Google Fights Piracy*, (2013) P.15

¹⁴⁴⁰ Google, *How Google Fights Piracy*, (2013) P.15

¹⁴⁴¹ Fred von Lohmann (Intellectual Property Director Google) interviewed by author, August 2013.

Proportionality

To be proportional, sanctions need to be necessary, suitable and not an unreasonable burden on individual rights. Google disputed that search was a large driver for infringement.¹⁴⁴² However, the large number of search results delisted did suggest that many ways in which Google search could be a pathway to infringement were now cut off. Meanwhile, YouTube had been the subject of lawsuits for allegedly enabling infringement on its servers.¹⁴⁴³ This led to the creation of ContentID. The above would certainly suggest that implementing this system had been necessary. Its suitability was more difficult to verify. It was disputed whether Google search actually enabled infringement. In the case of YouTube, the large-scale system certainly seemed suitable to allow rights holders to have control over their content.

Google search delisting is not a very heavy burden on speech rights, as the content remained up on the source site. In the case of YouTube however, speech was removed for numerous days before a trial had taken place. This is why the EFF for example argued that the option 'block' should not be possible for Content ID.¹⁴⁴⁴ However, according to Google, the majority of their clients chose monetize, not block.¹⁴⁴⁵

9.5 Impact on infringement levels

It was difficult to estimate how "effective" Google could be on infringement levels. Although Google was the most important and largest search engine, infringement did not take place on Google's servers.

Google said they received takedown notices on less than 1% of the results they indexed.¹⁴⁴⁶ The report also mentioned there were 60 trillion addresses on the web and that only an infinitesimal amount of those addresses contained copyright infringing content.¹⁴⁴⁷ In their report on piracy, Google said that search was not a real driver of traffic to infringing sites anyway. They said, and research confirmed this, that popular infringement sites either had a lot of publicity or notoriety and that they did not rely on search for their traffic, because users found popular infringement websites through social networks or word of mouth.¹⁴⁴⁸

¹⁴⁴² Google, *How Google Fights Piracy*, (2013) P. 20, and: BAE Systems Detica, "The six business models for copyright infringement," *Google & PRS for Music* (June 27, 2012), <http://www.prsformusic.com/aboutus/policyandresearch/researchandconomics/Documents/TheSixBusinessModelsofCopyrightInfringement.pdf>, and:

Matt Schruers, "The Search Fixation: Infringement, Search Results, and Online Content," Computer & communications Industry Association research paper (August 2013), http://cdn.cciinet.org/wp-content/uploads/2013/08/CCIA_TheSearchFixation.pdf

¹⁴⁴³ Eric Gardner, "YouTube Again Beats Viacom's Massive Copyright Infringement Lawsuit," *The Hollywood Reporter* (April 18, 2013), <http://www.hollywoodreporter.com/thr-esq/youtube-again-beats-viacoms-massive-442233>.

¹⁴⁴⁴ Corynne McSherry (Intellectual Property Director Electronic Frontier Foundation) interviewed by author, September 2013.

¹⁴⁴⁵ Fred von Lohmann (Intellectual Property Director Google) interviewed by author, August 2013.

¹⁴⁴⁶ Google, *How Google Fights Piracy*, (2013) P.3.

¹⁴⁴⁷ Google, *How Google Fights Piracy*, (2013) P. 13.

¹⁴⁴⁸ Google, *How Google Fights Piracy*, (2013) P. 20, and: BAE Systems Detica, "The six business models for copyright infringement," *Google & PRS for Music* (June 27, 2012), <http://www.prsformusic.com/aboutus/policyandresearch/researchandconomics/Documents/TheSixBusinessModelsofCopyrightInfringement.pdf>, and:

Matt Schruers, "The Search Fixation: Infringement, Search Results, and Online Content," Computer & communications Industry Association research paper (August 2013), http://cdn.cciinet.org/wp-content/uploads/2013/08/CCIA_TheSearchFixation.pdf

The report also stated that taking down search results did not remove the websites, and that sites were easily replicated. So attempts to make sites disappear should focus on the money behind them.¹⁴⁴⁹ This was also confirmed by research.¹⁴⁵⁰

Finally, Google said that the amount of queries aimed at piracy was “dwarfed” by broader queries.¹⁴⁵¹

For YouTube, it was difficult to get reliable estimates on the amount of infringement on YouTube. One would suspect them to be very high. In the lawsuits launched by Viacom against YouTube, rights holders claimed that 75% to 80% of the videos on YouTube contained copyright protected material (which is not the same as infringing).¹⁴⁵² Also, YouTube is a popular channel for amateur cover songs, which under copyright law, were illegal without a license.

An interesting development seemed to be the thousands of infringing uploads that claimed “no copyright infringement intended” or that contained a copyright disclaimer citing fair use, both statements that in the context of YouTube had little legal consequences. One website called it “as effective as a drug dealer asking if you’re a cop.” The same website found over a million of these disclaimers.¹⁴⁵³

The large number of takedowns through Content ID alone (more than 120 million videos at the time) would suggest that infringement numbers were high.¹⁴⁵⁴

However, apart from just fighting infringement, YouTube pays rights holders as well. More than 1 billion had been paid to rights holders through the Content ID program alone.¹⁴⁵⁵

9.6 The costs of the system

It was difficult to estimate the costs of this system, because there were no official reports on expenditures. Therefore, the only information available was the broad description of the procedure and the answers of the interviewees.

Notice and takedown placed part of the enforcement burden on platform owners, because they had to establish procedures for notice and takedown and thus absorb some of the costs of enforcement. In this case, it meant that Google had to invest in enforcement as well.¹⁴⁵⁶

According to Google, they had hundreds of people who work on anti-piracy. They said it was “not a trivial cost.” Creating such a system, according to them, required a “major technology innovation.” Both the ContentID and the TCRP program required an engineering effort, they said. They said they also had to invest in the transparency report, which was a “substantial expenditure.” According to Google, it seemed as if rights holders always said they carried the entire burden, but “there are very real costs to receive notices, and process them, and catch errors.” Although Google also mentioned there was no obligation to produce a transparency report, it did not seem responsible not to do it. They also said that for cost reasons, smaller ISPs had no choice but to simply accept notices.¹⁴⁵⁷

In its report on fighting piracy, Google mentioned: “we continue to invest substantial resources and engineering effort into improving our procedures for receiving and processing

¹⁴⁴⁹ Google, *How Google Fights Piracy*, (2013) P. 20.

¹⁴⁵⁰ Tobias Lauinger et al.,

“Clickonomics: Determining the Effect of Anti-Piracy Measures for One-Click Hosting,” Presentation at the NDSS Symposium (2013), http://www.Internetsociety.org/sites/default/files/07_1_0.pdf

¹⁴⁵¹ Google, *How Google Fights Piracy*, (2013) P. 20.

¹⁴⁵² Eric Gardner, “YouTube Again Beats Viacom’s Massive Copyright Infringement Lawsuit,” *The Hollywood Reporter* (April 18, 2013), <http://www.hollywoodreporter.com/thr-esq/youtube-again-beats-viacoms-massive-442233>.

¹⁴⁵³ “No Copyright Intended”, *Waxy* (December 9, 2011), http://waxy.org/2011/12/no_copyright_intended/.

¹⁴⁵⁴ “Press Statistics,” *YouTube website*, http://www.youtube.com/t/press_statistics

¹⁴⁵⁵ “Press Statistics,” *YouTube website*, http://www.youtube.com/t/press_statistics

¹⁴⁵⁶ Urban and Quilter, “Efficient Process or ‘Chilling Effects’?” P.636.

¹⁴⁵⁷ Fred von Lohmann (Intellectual Property Director Google) interviewed by author, August 2013.

copyright removal notices.”¹⁴⁵⁸ One of those new investments was an increased turnaround time. At first, Google search takedowns would take 8 hours. In 2012 it went down to less than 6 hours. As they said, it was “not cost free to be that quick.”¹⁴⁵⁹

Rights holders had substantial costs as well. They had to hire or finance anti-piracy organizations or independent enforcement vendors. Brein was financed by collective rights organizations and trade organizations. There were 12 people working at Brein, but they refused to comment on budgetary issues.¹⁴⁶⁰ They claimed to be able to represent a relative large proportion of takedown requests compared to anti-piracy organizations of other countries because they had the capacity and software.¹⁴⁶¹

Digimarc Guardian had over a hundred different clients.¹⁴⁶² But “all clients have different needs and wants.” “Some are protecting revenues, some are protecting content, and some have subscription they charge a lot for.” Therefore they made different business agreements with their customers.¹⁴⁶³ “Some contacts pay us if we do every month 1-2-3-4000 notices, some want us to cover their entire catalogue and do some takedowns, sometimes they want us to cover their entire catalogue and we do limited takedowns, some want us to cover a smaller amount of what they consider their priority and we do unlimited takedowns, and some have the 80-20 rule. This means that 20 % of titles have 80% of the infringement. This applies mostly to the Hunger Games or Harry Potter stuff.”¹⁴⁶⁴

DtecNet had 80 people working on enforcement, from a customer/technology service perspective. Their customers included “Music, television, movies, live performances, sports, books, all sort of flavors of media.”¹⁴⁶⁵

They maintained different performance standards than Digimarc in their relations with clients. For example, they claimed it was not based on the number of notices they sent out. “It can be based on the relative popularity of some titles, based on frequency that we’re looking at various sources, based on speed with which something needs to come down, the number of hours or minutes in the day we do it, because some of these things, if you’re for example on a launch schedule for a big record/movie, or it is a very popular concert or performer, it requires a lot of resources to protect people from infringing on that, or to discover infringement. That’s where it lies. How popular and how diligent must we be to provide a level of protection, so it can be very different pricing and packaging. Most of our clients are very large organizations and they have very sophisticated operations with respect to how they guard their content.”¹⁴⁶⁶ When asked about the difference between this and Digimarc, they said that the latter “probably work with smaller companies.”¹⁴⁶⁷

9.7 Conclusion

This case describes different enforcement actions that have been divided into 4 subcases (the way Google designed large-scale automated takedowns and smaller scale takedowns at its two largest sites (so the subcases are Google search takedowns, the Trusted Copyright Removal Program, YouTube takedowns and ContentID).

¹⁴⁵⁸ Google, *How Google Fights Piracy*, (2013) P. 15.

¹⁴⁵⁹ Fred von Lohmann (Intellectual Property Director Google) interviewed by author, August 2013.

¹⁴⁶⁰ Tim Kuik (BREIN), interviewed by author, May 2013.

¹⁴⁶¹ Tim Kuik (BREIN), interviewed by author, May 2013.

¹⁴⁶² Digimarc Guardian, interviewed by author, October 2013.

¹⁴⁶³ Digimarc Guardian, interviewed by author, October 2013.

¹⁴⁶⁴ Digimarc Guardian, interviewed by author, October 2013.

¹⁴⁶⁵ Fred Felman (DtecNet) interviewed by author, November 2013.

¹⁴⁶⁶ Fred Felman (DtecNet) interviewed by author, November 2013.

¹⁴⁶⁷ Fred Felman (DtecNet) interviewed by author, November 2013.

Google search was notified of infringing URLs either by individuals or through a trusted removal program which used trusted parties for removal of search results that point to infringing content. Google then delisted those search results. At YouTube notifications were sent by individuals. ContentID is a large-scale automated content management system that allows rights holders to block, monetize or track their content.

Regarding scale and severity, millions of links have been delisted from Google search as a result of the notice and takedown procedure and its content removal program. ContentID claimed hundreds of millions of videos, while Youtube a fraction of that amount, we estimate, although still ranging in the millions. A YouTube claim can take a video down, but ContentID offered rights holders the choice to monetize the video or track user statistics. The overwhelming majority is estimated to have chosen monetize.

Spotting infringement in the program at Google required web crawling and taking the content down, and no processing of personal data. The system was privately administered, and parties did not take responsibility for takedowns. Accusations were hardly checked and biased towards the complainant. There was appeal but it took place after the delisting. There was no right to be heard. Google had introduced a separate large-scale takedown program for trusted complainants, who would be able to submit more notices that were not reviewed for accuracy, but they created additional safeguards by rewarding reputation: parties could lose their status of trusted complainant if they made too many mistakes. Regarding transparency, Google released a report that described some of the links which have been delisted, all the complainants and additional data. The system was suitable and necessary and the burden on individual rights was small, so proportional. For YouTube personal data was processed as infringement related back to an individual Google account. The takedown system was privately administered and biased towards the complainant. There was no chance to be heard, and appeal was possible only after the takedown. There was little transparency. Some have argued that taking content from youtube without safeguards is disproportional.

It was difficult to measure the effect on infringement, as infringement did not take place on Google's servers. Google itself claimed search was not a popular driver for infringement. For YouTube millions of videos were taken down. It was difficult to get reliable estimates on the level of infringement on YouTube although that number is likely high. However, YouTube has paid over a billion to rights holders as a result of its enforcement program.

Enforcement was expensive, with the costly involvement of enforcement vendors and costs distributed to Google. These outcomes will be highlighted again in the conclusion and compared with the outcomes of the other cases.

10. NOTICE AND TAKEDOWN IN THE NETHERLANDS IN 2009-2013

10.1 Introduction

Notice and takedown in the Netherlands allowed rights holders to submit notifications to ISPs to ask them to take infringing content down. This could be websites or specific infringing content. In this case study, I have looked at how one hosting provider (Leasweb) and two access providers (Ziggo and XS4ALL) apply this procedure. This case is divided in two subcases. One subcase for the regular procedure and one for the trusted removal program as applied by Leasweb.

The first section on the legal background will describe the Dutch copyright law and specifically the history and provisions on notice and takedown. For this, I relied on academic and legal sources. It shortly describes the Dutch ISPs featured in this chapter for which I have also relied on their statements. After this, the chapter describes the procedure in practice. For this I relied on official documents, but also on interviews with practitioners. I spoke to two ISPs that mainly provide access (XS4ALL and ZIGGO), one hosting provider (Leasweb), a social network site (Hyves - they could not provide enough information, hence their numbers are not included), I tried to get into contact with an auction site (Marktplaats), but they refused to be included in the research, and I spoke to an enforcer (Brein) and a digital rights organization (Bits of Freedom). Through email, I spoke with a legal aid organization (the Clinic) and with Marjolein Durinck of ECP-ECN, the organization which governs the code of conduct for notice and takedown in the Netherlands.

This is followed by a section on the variables, for which I relied on the above cited information, supplemented with news articles, academic research and reports by NGOs on notice and takedown. Some of those evaluated and tested notice and takedown procedures in the Netherlands in the past. The information was collected from January 2012 until the end of 2013. After this, changes were made to the law that have not been accounted for, the main change being that downloading from illegal sources is no longer allowed in the Netherlands.

10.2 Legal background

The main provisions on Dutch copyright law were in the 'Auteurswet' (Aw) and on neighboring rights in the 'Wet Naburige rechten' (Wnb). These laws provided the exclusive competence to publish and reproduce creative content.¹⁴⁶⁸ The Dutch copyright law was created in 1912 and was amended mainly to comply with new European laws, creating new protections and increased enforcement capabilities.

Dutch copyright law was lenient compared to other European Union member states, because of its home copying exception, regulated in articles 16b and 16c of the Dutch copyright law. Article 16c applied to the digital domain.¹⁴⁶⁹ The Dutch legislature recognized that digital technology allowed for easy copying of any content, therefore they allowed

¹⁴⁶⁸ Charles Gielen, et al., *Kort begrip van het Intellectuele Eigendomsrecht*, (Deventer: Uitgeverij Kluwer, 2011). P.423.

¹⁴⁶⁹ MVT, Kamerstukken II 2001/02, 28 482, nr. 3, p.44-48.

authors to get ‘royalties’ for sold records or any other exploitation of their work, though not for ‘home copies’ made for private use or study. This meant individual users could copy works to blank media, copy CDs or DVDs, or download music or movies.

Until recently the law did not distinguish between material that originated from a legal or illegal source.¹⁴⁷⁰ This meant that downloading copyright protected content from an illegal website without consent of the rights holders, like through P2P services, was allowed.¹⁴⁷¹ Paragraph 7 of article 16c stated that it was illegal to issue these private copies to other people, but the question remained to what extent this was enforceable. Home-copying did not apply to software (article 45n) or databases (16c -8 Aw).¹⁴⁷²

To compensate creators, article 16c paragraph 2 to 16ga contained provisions that created a levy on blank media (like empty, writable CDs).¹⁴⁷³ The levy applied to articles intended to capture images or sounds, articles that allowed for the playback of content, or articles that displayed other recorded information (such as text or data). The obligation to pay money rested on the manufacturer or importer of these articles. The Minister could create additional rules on the objects that require a levy.¹⁴⁷⁴

This exception had important consequences for enforcement. Whereas France had the graduated response procedure, Germany had individual lawsuits against end users, and other EU member states had similar initiatives, end users in the Netherlands were generally left alone. Enforcement concentrated itself on the supply side; by for example going after large file sharing platforms or blocking access to them. Because enforcement was not targeted at end users, notice and takedown procedures played an important role in the Dutch context.

Enforcement was done by rights holders themselves, and originally by collective rights organizations like Buma and Stemra. However, the biggest players in enforcement, especially in terms of scale, were special enforcement organizations. By far the most important one was BREIN. The BREIN (Bescherming Rechten Entertainment Industrie Nederland - Dutch for “Protection Rights Entertainment Industry Netherlands”) foundation was created by numerous collective rights organizations in 1998 to combat piracy of audio, video and multimedia products.¹⁴⁷⁵ It brought together participants from all entertainment industries in the Netherlands, “in the fight against intellectual property theft.” BREIN had an anti-piracy program that consisted of lobbying for legislation, of investigation, litigation, sentencing, and education.¹⁴⁷⁶ The Business Software Alliance (BSA) represented software makers and fought software piracy by for example raiding and seizing companies that were suspected of using pirated software.

Until 2003, Buma and Stemra had their own investigative officers who were transferred to the government Team for Investigating Piracy (Team Opsporing Piraterij – TOP), a part of the Fiscal Information and Investigation Service/Economic control service

¹⁴⁷⁰ As of April 10, 2014, this no longer applies. Downloading from an illegal source is no longer allowed.

¹⁴⁷¹ Gielen, et al., *Kort begrip van het Intellectuele Eigendomsrecht*, P.495, NnNV, Kamerstukken II 2001/02, 28 482, nr. 8, p.13; Kamervragen van het lid Gerfkens met antwoord, Kamerstukken II 2006/07, nr. 2030; Hof 's-Gravenhage 15 nov. 2010, IER 2011/27, p.174 m.nt. Koelman (ACI Adam c.s./Thuiskopie, cassatie ingesteld); Hof 's-Gravenhage 15 nov.2010, IER 2011/28, p.197 m.nt. Koelman (FTD/Eyeworks).

¹⁴⁷² J.H. Spoor, D.W.F. Verkade, D.J.G. Visser, *Auteursrecht, naburige rechten en databankenrecht* (Deventer: Kluwer, Third print, 2005). P.271-273.

¹⁴⁷³ Spoor, Verkade, Visser, *Auteursrecht, naburige rechten en databankenrecht*, P.270-271.

¹⁴⁷⁴ Spoor, Verkade, Visser, *Auteursrecht, naburige rechten en databankenrecht*, P.273.

¹⁴⁷⁵ Spoor, Verkade, Visser, *Auteursrecht, naburige rechten en databankenrecht*, P.477.

¹⁴⁷⁶ “The Brein Foundation,” *Brein website*, <http://www.anti-piracy.nl/english.php>

(Fiscale Inlichtingen- en Opsporingsdienst/Economische controle dienst – FIOD/ECD). This put ‘Intellectual property fraud’ into one centralized institution, which was under the direction of a unit (functioneel parket –FP) of the public prosecutor (Openbaar Ministerie – OM). This team mainly dealt with combating large-scale piracy.¹⁴⁷⁷ BREIN cooperated with the (now called) FIOD, and provided the FIOD with information and expertise for criminal enforcement.

Each year, Brein took action against hundreds of websites and thousands of illegal ‘offers.’ Google’s transparency report revealed that Brein took down 137.339 search results in the last quarter of 2012. That is 10,000 a day.¹⁴⁷⁸ The Dutch government also ordered the removal of search results, though on hate speech grounds.¹⁴⁷⁹

Brein chased access- and hosting providers to block access to infringing websites. They first appealed to the infringing websites themselves, and if unsuccessful, appealed to the access providers or hosting providers to block access. This eventually led to numerous cases against the pirate bay in the Netherlands. According to their yearly report they closed down hundreds of sites in 2011 and 2012.¹⁴⁸⁰

Ziggo and XS4ALL were two of the most well-known access providers in the Netherlands. XS4ALL was one of the oldest Internet providers, and known for its idealistic roots, and willingness to take on controversial issues. In 1998 it was bought by KPN, but it retained a separate position within the company.¹⁴⁸¹ Apart from being an access provider, XS4ALL offered some content online, which consisted mostly of old movies.¹⁴⁸² XS4ALL also allowed for hosting.¹⁴⁸³ Ziggo was the largest cable operator of the Netherlands, and also provided Internet services.¹⁴⁸⁴ Ziggo offered internet access and some hosting services.¹⁴⁸⁵ It was also a large content provider, with around 30/35% of the market.¹⁴⁸⁶ In an interview they said they had contacts with all the big parties¹⁴⁸⁷ and were shareholder of HBO in Holland (a very popular content provider). They therefore offered a large catalogue of content on demand.¹⁴⁸⁸

Leaseweb was one of the largest hosting providers in the world at the time, and based in the Netherlands.¹⁴⁸⁹ They had 60,000 servers and generated 3-4% of all Internet traffic worldwide. They did not handle content, but their business revolved around providing infrastructure. They considered the content a responsibility of the client. The Leaseweb

¹⁴⁷⁷ Spoor, Verkade, Visser, *Auteursrecht, naburige rechten en databankenrecht*, P.542-544.

¹⁴⁷⁸ Chris Koenis, “BREIN meldt 10.000 ‘illegale’ zoekresultaten per dag,” *Webwereld* (January 15, 2013), <http://webwereld.nl/nieuws/113045/brein-meldt-10-000--illegale--zoekresultaten-per-dag.html> and: “Reporting Organization: Stichting BREIN,” *Google Transparency Report*,

<http://www.google.com/transparencyreport/removals/copyright/reporters/11759/Stichting-BREIN/>

¹⁴⁷⁹ “Netherlands,” *Google Transparency Report*,

<http://www.google.com/transparencyreport/removals/government/NL/?metric=requests&by=reason&p=2012-06>

¹⁴⁸⁰ 2011: “BREIN statistieken 2011: ongeveer 600 sites, 60.000 advertenties en 60 beunhazen gesloten,” *BREIN* (February 20, 2012), <http://www.anti-piracy.nl/nieuws.php?id=252>.

2012: “BREIN jaarstatistieken 2012,” *BREIN* (January 1, 2013), <http://www.anti-piracy.nl/nieuws.php?id=285>.

¹⁴⁸¹ “Wie we zijn,” *XS4ALL website*, <http://www.xs4all.nl/overxs4all/wiewijzijn/>

¹⁴⁸² Margreth Verhulst (XS4ALL), interviewed by author, May 2013

¹⁴⁸³ “Hosting,” *XS4ALL website*, <https://www.xs4all.nl/zakelijk/hosting/>

¹⁴⁸⁴ “Het Bedrijf,” *Ziggo website*, <https://www.ziggo.com/nl/#en-GB/start/>

¹⁴⁸⁵ “Zakelijk,” *Ziggo website*, https://www.ziggozakelijk.nl/extra_diensten/hosting

¹⁴⁸⁶ Marcel Eswilder (Ziggo), interviewed by author, May 2013

¹⁴⁸⁷ Marcel Eswilder (Ziggo), interviewed by author, May 2013

¹⁴⁸⁸ “Televisie,” *Ziggo website*, <https://www.ziggo.nl/televisie/>

¹⁴⁸⁹ “Leaseweb,” *Leaseweb website*, <http://www.leaseweb.com/en>

company consisted of three judicial entities; a Dutch one (+/- 50,000 servers, the largest one), and a US and a German one. These three entities were separated by “legal firewalls” meaning the US servers fell under the DMCA and the patriot act for example.¹⁴⁹⁰

Towards notice and takedown

Apart from the main provisions in the Dutch copyright law, Dutch Torts law (article 6:162 BW) provided supplemental protection to copyright holders, especially where it concerned copyright infringement online. Torts law protected the interests of creators, if they were not protected by copyright law. This applied to cases in which personal interests were in jeopardy or in which exploitation interests were involved. However, one could not conclude that these provisions always favored the creator.

These provisions could also provide private law protection against acts that in criminal law would normally be considered as instigation or complicity to infringement. This was the case for example when people created material that could only be understood as meant to provide unauthorized access to copyright infringing material, like a machine that would decode cable television that normally required payment.¹⁴⁹¹

On the Internet, this applied in the same way. The Dutch courts held that making P2P software available was not a direct infringement of copyright law in relation to reproducing or publishing. According to those courts one had to look at whether making that technology available was wrongful. This depended on whether that technology could be used for legitimate purposes and whether the operator of that technology had the means to prevent infringement.¹⁴⁹²

For this reason, the Amsterdam Court of Appeal upheld the judgment of the Haarlem Court that KaZaA was lawful.¹⁴⁹³ The Haarlem Court ruled that a search engine meant to find mp3 music files was lawful. The operator of that search engine was however obligated by the court to remove any links that pointed towards infringing content if he or she received a notification on this.¹⁴⁹⁴

In the scientology/XS4all case, the question was raised whether or not ISPs were liable for content of their users.¹⁴⁹⁵ The district court of the Hague ruled that the ISPs in the case conducted activities that were limited to the transfer of information between users and the storage of that information. The ruling also stated that ISPs did not select the information or alter it. They only supplied the technical facilities that made publishing by others possible. Therefore the Court concluded that ISPs only provided the opportunity to publish instead of publishing themselves. The Court also concluded that the activities of ISPs did not include copyright law relevant reproduction. In the case at hand parties were dealing with technological acts that were not caused by an act of the ISP, but by the owner of a website or the consumer at home requesting the information.¹⁴⁹⁶

¹⁴⁹⁰ Alex de Joode (Leaseweb), interviewed by author, May 2013

¹⁴⁹¹ Spoor, Verkade, Visser, *Auteursrecht, naburige rechten en databankenrecht*, P.404-405.

¹⁴⁹² Spoor, Verkade, Visser, *Auteursrecht, naburige rechten en databankenrecht*, P.406.

¹⁴⁹³ Hof Amsterdam 28 maart 2002, AMI 2002, nr 13, p. 134, LJN AE805, Mf 2002, nr 19, p. 188 m.nt. K.J.Koelman (Buma/KaZaA).

¹⁴⁹⁴ Rb. Jaarlem 12 mei 2004, AMI 2004, nr 15, p. 185 m.nt. Koelman, LJN AO9318 (Techno Design/Brein).

¹⁴⁹⁵ Gielen, et al., *Kort begrip van het Intellectuele Eigendomsrecht*, and: Rb. 's Gravenhage 9 juni 1999, BIE 1999, 458, IER 1999, 237, AMI 1999, 110.

¹⁴⁹⁶ Gielen, et al., *Kort begrip van het Intellectuele Eigendomsrecht*, P.512.

However, the Court added that ISPs could be held liable on the basis of due diligence for what happened in their networks, even though they did not reproduce or publish material themselves. Moreover, the decision stated that ISPs had duties to care and take appropriate action if they were notified that their users had used the ISPs system to infringe copyright law through websites or through other illegal acts. In fact, the Court made clear that ISPs could be held liable if the accuracy of such a notification was reasonably unquestionable. In such a case the ISP had to remove the infringing material and hand over the name and address of the infringer to the rights holder if he or she so requested.¹⁴⁹⁷

The EU e-commerce Directive (2000/31/EC) created a provision that made Internet providers potentially liable for infringing content of their subscribers, unless they removed that infringing content upon receiving a complaint (by rights holders).¹⁴⁹⁸ Article 14 of the directive applied to all illegal activity or information. The directive did not specify how the notice and takedown (called 'Notice and action' by the European Commission) procedures should work, while expecting that these would be developed by private players and governments, as a result of liability. They envisaged private agreements. Recital 40 of the Directive said: "this Directive should constitute the appropriate basis for the development of rapid and reliable procedures for removing and disabling access to illegal information; such mechanisms could be developed on the basis of voluntary agreements between all parties concerned and should be encouraged by Member States; it is in the interest of all parties involved in the provision of information society services to adopt and implement such procedures. (...)". The articles in the directive provided for both removing and disabling access (blocking). Disabling access was added in case the takedown of illegal content was impossible because the activity or information stored happened outside of the EU.¹⁴⁹⁹

The notice and takedown procedures were primarily defined in other regulations. Articles 9 and 11 of the Enforcement directive provided that member states had to ensure that rights holders were able to file injunctions against intermediaries if their services were used by third parties to infringe on intellectual property rights. Article 17 of that same directive provided that Member states should encourage the development of self-regulatory codes of conduct that helped the enforcement of intellectual property rights.¹⁵⁰⁰ This was relevant because the Netherlands had such a code of conduct for notice and takedown. In the Netherlands, the e-commerce Directive had been implemented through the *Aanpassingswet richtlijn inzake elektronische handel* (The Adaptation law for the directive concerning e-commerce, hereafter referred to as the '*Aanpassingswet*') in 2004.

This law introduced the notice and takedown adjustment in the civil code in article 6:196c BW¹⁵⁰¹ with specific provisions for all three ISP services (caching, mere conduit and

¹⁴⁹⁷ Gielen, et al., *Kort begrip van het Intellectuele Eigendomsrecht*, and: Vزر. Rb. 's-Gravenhage 5 jan. 2007, IER 2007/22, p.96 (Brein/KPN) en Vزر.Rb.Haarlem 12 mei 2004, IER 2004/57, p.263 (Brein/Techno Design)

¹⁴⁹⁸ Bits of Freedom, "Providers verwijderen tekst Multatuli," *Bits of Freedom website* (October 13, 2004). <https://www.bof.nl/2004/10/13/providers-verwijderen-tekst-multatuli/>

¹⁴⁹⁹ European Commission, Commission staff working document on Online services, P.39.

¹⁵⁰⁰ European Commission, Commission staff working document on Online services, P.40.

¹⁵⁰¹ Nico van Eijk et al., *Moving Towards Balance - A study into duties of care on the Internet*, (University of Amsterdam - Institute for Information Right (IViR), WODC, 2010). P.64: In the explanatory memorandum to the law implementing the InfoSoc Directive (2001/29/EG), it is explicitly stated that liability for intermediaries through involvement in the online traffic of copyright infringing materials is covered by the safe-harbour provisions of the E-commerce Directive, Kamerstukken II 2001-02, 28482, nr 3, p. 38-39. [explanatory memorandum to the Implementation Law Directive on Copyright and Neighboring Rights in the Information Society] See also: Kamerstukken II 2005-06, 30 392, nr. 6, p. 7. [Note on parliamentary discussion on the

hosting).¹⁵⁰² For some actions, provisions were added to the criminal code. Article 54a of that code now also handled notice and takedown (for example in the case of child pornography).

On the basis of torts law, Internet providers could be held accountable for copyright infringement if they have been notified of an infringement on their networks. The first part of article 6:196c BW dealt with mere conduit by the providers. This was the transmission of information of others and giving access to the provider's communication facilities. The second part of the article dealt with temporary storage and rules on measures. As a ground rule the ISPs did not have to act as long as they did not cache or host information on their servers, did not initiate the transmission, did not decide who would receive the information and did not select or amend the transmitted information.¹⁵⁰³

The third part of article 6:169c BW dealt with caching, which meant storing information for others for the purpose of making this information available at the request of third parties more efficiently, in an automated, interim and temporary manner. To avoid liability, the article said ISPs (1) could not alter the information, (2) had to comply with the conditions on access to information, (3) needed to comply with rules, widely recognized and used by the relevant industry sector, on updating the information, (4) they should not alter the technology widely recognized and used in the relevant industry sector to obtain information on the use of the information, (5) ISPs had to make sure they could react, by being able to promptly take measures to remove or disable access to the cached info, upon obtaining knowledge that at the original location in the communication network the infringing information had been removed or access to it had been blocked, or that a competent authority had ordered to remove or block the info.¹⁵⁰⁴

The fourth part of article 6:169c BW dealt with hosting providers. The article provided that an Internet service provider was not liable for stored data on his network, if (a) he was not aware of the activity or information that had an infringing nature and, in the case of damages, could not reasonably be expected to know of this activity or information, or (b) when he could be reasonably expected to know about this, immediately removed the information or prevented access.¹⁵⁰⁵ Removal happened when the operator "has no reason to doubt the accuracy of the notification."¹⁵⁰⁶

Apart from those torts law provisions, Dutch criminal law contained provisions to exempt ISPs from prosecution, if they acted upon requests from the prosecutor. There were no further statutory notice and takedown procedures in the Dutch law providing further substance on this issue.¹⁵⁰⁷

In the explanatory memorandum to the law implementing the directive in article 6:196c BW, it was written that requirements for safe harbors should be reasonable and proportionate considering the costs and the technical and personnel requirements for the

explanatory memorandum to the Implementation Law Directive on Enforcement of Intellectual Property Rights].

¹⁵⁰² Cyril van der net, "De Civielrechtelijke Aansprakelijkheid van Internetproviders na de Richtlijn Elektronische Handel," *JAVI* (2002/1), P.10-15.

¹⁵⁰³ van Eijk et al., *Moving Towards Balance*, P.50.

¹⁵⁰⁴ van Eijk et al., *Moving Towards Balance*, P.50.

¹⁵⁰⁵ Spoor, Verkade, Visser, *Auteursrecht, naburige rechten en databankenrecht*, P.407. and article 6:196c BW, 4th provision.

¹⁵⁰⁶ Rb. 's-Gravenhage 9 June 1999, AMI 1999 (Scientology/XS4ALL)

¹⁵⁰⁷ van Eijk et al., *Moving Towards Balance*, P.51.

ISPs concerned, and should be subsidiary.¹⁵⁰⁸ However, there were no statutory regulations that described who would have the competence to judge the proportionality of these measures.¹⁵⁰⁹

In the *Lycos v. Pessers* case, the Dutch supreme court confirmed a lower court decision that ISPs could provide identifying data of information providers of allegedly unlawful content, though only under certain conditions: if there was a substantial likelihood that the content was unlawful and could cause harm, the person requesting the data had an actual interest in obtaining the data, there was no less far-reaching measure available to obtain the data and these interest of the requesting party outweighed the interests of the ISP and, in this case, the website owner.¹⁵¹⁰

Some case law dealt with intermediaries which according to the courts fell outside of the scope of the safe harbor provisions. In the cases of BREIN against Mininova, and BREIN against The Pirate Bay, the defendant parties had been ordered to stop facilitating continuous infringement of copyrights and other IP rights, considered unlawful under general tort law. The owners of these websites were considered to do more than provide “information society services” because of their involvement in infringement and could therefore not be seen as ISPs in the sense of article 6:196c BW.¹⁵¹¹

Article 26d Aw further provided that civil action could be brought against ISPs or other intermediaries to make them cease services that were used to infringe on copyrights. The court would balance their interests, taking into account the goal of the action or claim, the interests of the rights holder, and the possible damage to the ISP if the action was granted. The ISP needed to be reasonably able to comply and not suffer any excessive costs. Another requirement was that the goal of the claim had to be autonomously directed at the ISP (instead of that it also could have been done by the infringer him/herself). The claim was limited to the order to suspend the infringing activities. It did not make the ISP liable for the actions of third parties.¹⁵¹² The ISP could be ordered to supply the personal data of the infringer.¹⁵¹³

Notice and takedown code of conduct

The provisions on notice and takedown as originally laid down in the law were rather vague, especially concerning the role of intermediaries in the procedure. As a result, in 2007 XS4all was the first ISP to release a code of conduct on how it dealt with complaints.¹⁵¹⁴

¹⁵⁰⁸ van Eijk et al., *Moving Towards Balance*, P.53, and: Kamerstukken II 2001-02, 28197, nr. 3, p. 51. [Explanatory memorandum to the Implementation Law Directive on Electronic Commerce].

¹⁵⁰⁹ van Eijk et al., *Moving Towards Balance*, P.53.

¹⁵¹⁰ van Eijk et al., *Moving Towards Balance*, P.52.

¹⁵¹¹ van Eijk et al., *Moving Towards Balance*, P.65, and: Rechtbank [District Court] Utrecht 26 August 2009, LJN BJ6008, BREIN versus Mininova; Rechtbank [District Court] Amsterdam (preliminary relief judge) 22 October 2009, LJN BK1067 The Pirate Bay versus BREIN. [both in Dutch].

¹⁵¹² Gielen, et al., *Kort begrip van het Intellectuele Eigendomsrecht*, P.513, and MvT, Kamerstukken II 2005/06, 30 392, nr.3, p.26-27

¹⁵¹³ Gielen, et al., *Kort begrip van het Intellectuele Eigendomsrecht*, P.514. From European case law (HvJ 29 jan. 2008, NJ 2009, 551, with annotation by Hugenholtz (Promusicae/Telefónica de España) it follows that this does not have to be a violation of EU law. More information in ECHR 2 dec. 2008, NJ 2009, 470 (K.U./Finland); HR 25 nov. 2005, NJ 2009, 550 with annotation by P.B. Hugenholtz (Lycos/Pessers); Vzr. Rb. Utrecht 12 jjune 2005, NJ 2005, 387 (Brein/UPC), Hof Amsterdam 7 nov. 2002, NJ 2003, 54 (XS4ALL/Deutsche Bahn).

¹⁵¹⁴ “Klachten Procedure,” *XS4ALL website*, http://www.xs4all.nl/overxs4all/contact/media/beleidsregels_klachten.pdf .

In 2008, companies, the government and interest groups, led by the NICC (National Infrastructure to Combat Cybercrime), established the code of conduct for notice and takedown (Gedragscode Notice-and-takedown). This code of conduct was presented to state secretary for economic affairs Frank Heemskerk in October 2008.¹⁵¹⁵ The procedure created by XS4all in the previous year was influential in the development of this code of conduct.

The code was drawn up under the flag of the National Infrastructure Cybercrime (Ministry of Economic Affairs) by market parties including KPN, XS4ALL, ISPCONnect, Dutch Hosting Provider Association, NLKabel, Ziggo, UPC, CAIW, Zeelandnet and SIDN. Ministries, the police and investigation services and organizations including Marktplaats/eBay and the BREIN foundation collaborated in the drafting of the code.¹⁵¹⁶

In the code of conduct, a number of articles and the explanatory memorandum dealt with the way intermediaries should treat complaints about unlawful and punishable content. Moreover, different types of content were defined, that all required different notice and takedown procedures. Intermediaries could decide for themselves what types of information they considered to fall under each type of content and how they dealt with it. Article 3b suggested that customer agreements should describe their criteria on how to deal with undesirable content. The code also provided guidelines on how to assess whether content was valid or not and which steps needed to be taken by the intermediary after takedown.¹⁵¹⁷

There was no formal list of members that adhered to the code of conduct, which was voluntary and unenforceable.¹⁵¹⁸ It could be viewed as a guideline intended to help deal with notice and takedown procedures.¹⁵¹⁹

The code of conduct advised the following: that intermediaries had their own notice and takedown procedure, that the public had to be able to consult it, and that the ISP acted according to this code. In this procedure should be written how intermediaries dealt with reports of unlawful content on the Internet. Meanwhile, intermediaries should always deal with reports and make sure that unlawful content is removed from the Internet. This procedure could be published by the intermediary, and could be in the service provision agreement (Article 3).¹⁵²⁰

It also stated that for requests that did not fall under criminal law (so in this case copyright), the complainant should provide: contact details, information that the intermediary needed to be able to evaluate the content, at least including the location (URL), a description of why the content was unlawful according to the complainant, or why it was in conflict with the criteria published by the intermediary governing undesirable content, and a statement of the reason why this intermediary was being approached as the most appropriate intermediary to deal with the matter. Complainants could also request that intermediaries dealt with the report as a matter of urgency. Furthermore, an intermediary could request compensation from a notifier against claims from the content provider, if measures had been taken to deal with the report (Article 4).¹⁵²¹

¹⁵¹⁵ "Werkgroep Notice and Takedown," *ECP-EPN Website*, <http://www.ecp-epn.nl/werkgroep-notice-and-takedown>

¹⁵¹⁶ Press release accompanying code of conduct.

¹⁵¹⁷ van Eijk et al., *Moving Towards Balance*, P.52.

¹⁵¹⁸ van Eijk et al., *Moving Towards Balance*, P.54.

¹⁵¹⁹ Notice-and-Take-Down Code of Conduct, version 1.04, 9 October 2008.

¹⁵²⁰ Notice-and-Take-Down Code of Conduct, version 1.04, 9 October 2008.

¹⁵²¹ Notice-and-Take-Down Code of Conduct, version 1.04, 9 October 2008.

The intermediary evaluated the reports to determine whether they were unequivocally unlawful or punishable.¹⁵²²

Article 6 set out the procedure after notice. If the intermediary thought the content was not unequivocally unlawful, they would inform the notifier, with their reasons for it. If they thought it was unequivocally unlawful, they would remove the content. If the intermediary was not sure, they could notify the content provider with the request to remove the content or contact the notifier. If the notifier and content provider were unable to reach an agreement, they could bring the dispute before the courts. If the content provider was unwilling to make him or herself known to the notifier, the intermediary could decide to provide the notifier with the content provider's name, and contact details. All the while the intermediary exercised due caution.¹⁵²³

Parties adhering to the code, should make that known, article 7 further provided, but notifiers and intermediaries could make their own mutually acceptable agreements as well.¹⁵²⁴

The explanatory notes added that notice and takedown should be done within a reasonable time limit, which would be 5 working days for example. However, it also said that the time limit should be related to the severity of the alleged infringement and the social upheaval related to it.

Intermediaries could establish criteria for content that they found undesirable and for content they did not want to facilitate. There was however a difference between undesirability (up to the intermediary) and unlawfulness (up to the law).

Regarding the notifier, the code suggested that he should be as precise as possible in the notice he sent to the intermediary (for example which part of the website was considered unlawful). When the same content showed up elsewhere, the notifier could be less detailed in the notification (notice and stay-down) and could ask for some urgency. The responsibility to report lay with the notifier. The intermediary and the notifier could agree that the intermediary is indemnified against claims from the content provider as a consequence of the measures taken in dealing with the report. (This would for example happen in the case of 'professional' notifiers). This was especially helpful in cases where the unlawfulness of content was difficult to determine. If an intermediary was of the opinion that content was not unlawful they had to state their reasons to the notifier.

Case law suggested that contact details could be given, if the published information (a) could be unlawful in respect of the notifier, (b) could lead to damage being caused to the notifier, and (c) if a less drastic way to obtain the name and contact details was unavailable to the notifier.¹⁵²⁵

European Commission evaluation of Notice and takedown

The European Commission evaluated the workings of the Notice and 'action' procedures in the EU. They had a public consultation with stakeholders to provide their views on how the procedures worked thus far, in preparation of a possible new proposal in the following years. There were some issues that repeatedly surfaced. There were some uncertainties where it concerned the differences between the procedures between different member states.

¹⁵²² Notice-and-Take-Down Code of Conduct, version 1.04, 9 October 2008.

¹⁵²³ Notice-and-Take-Down Code of Conduct, version 1.04, 9 October 2008.

¹⁵²⁴ Notice-and-Take-Down Code of Conduct, version 1.04, 9 October 2008.

¹⁵²⁵ Notice-and-Take-Down Code of Conduct, version 1.04, 9 October 2008.

One of the main criticisms concerned the requirements of a notice. Rights holders complained that often the amount of information required for a notice was too detailed and amounted to procedure that was “too burdensome.” They argued that notices should not require specific information like URL references or information regarding the illicitness of the content. They also thought notice and takedown should as a rule be electronic.¹⁵²⁶ Intermediaries however demanded these levels of detail, because they wanted to be able to assess the alleged illegality of the information. Therefore, they needed to be able to identify the complainant, locate the content, and assess the illegality.¹⁵²⁷

In terms of defense for information providers, civil society organizations and most intermediaries were in favor of providing some sort of counter notice system that would protect content providers. No such legal obligation existed in the Netherlands. Rights holders and ISPs considered that a counter notice would make notice and takedown procedures “more burdensome, slower and less effective.” Rights holders further argued that allowing a counter notice might not be appropriate in the context of manifestly illegal information, like child pornography. Moreover, one had to consider the principles of data protection, because a counter notice would require identifying the content provider.¹⁵²⁸ Others suggested that as a defense it should be possible to hold accountable the people who submitted wrongful information.¹⁵²⁹ There was also some discussion on the time frame in which a decision on the alleged illegality of content should be made, which was often unclear.¹⁵³⁰

In particular civil rights organizations were worried about the lack of transparency and democratic oversight, especially where it concerned the policies of individual companies that handled the takedown of or blocking access to content.¹⁵³¹ According to these organizations it would be risky to have private operators decide the alleged illegality of certain information, especially because there was no transparency or oversight with regard to these companies. According to stakeholders this argument did not apply to “manifestly illegal” information.¹⁵³² Some rights holders proposed that prevention in the form of filtering would be an option.¹⁵³³

10.3 The procedure in practice

Upon receiving a complaint, Internet providers were responsible for checking whether or not publications by its subscribers were legitimate/legal or not, and if they were not, block access to them. To determine whether an ISP was liable, three steps were followed. A provider was liable if he received a complaint, if from the complaint it was apparent there was clear copyright infringement, and if the provider did not act after that. During the debates in the *Tweede Kamer* (the Dutch lower house of parliament), this liability was extended: if the party that filed a complaint demanded damages, a provider risked a more heavy fine, if they should have had reasonable grounds to know that this was infringing content. This was however, unspecified.

¹⁵²⁶ European Commission, Commission staff working document on Online services, P.43.

¹⁵²⁷ European Commission, Commission staff working document on Online services, P.43.

¹⁵²⁸ European Commission, Commission staff working document on Online services, P.44.

¹⁵²⁹ European Commission, Commission staff working document on Online services, P.45.

¹⁵³⁰ European Commission, Commission staff working document on Online services, P.44-45.

¹⁵³¹ European Commission, Commission staff working document on Online services, P.41.

¹⁵³² European Commission, Commission staff working document on Online services, P.45-46.

¹⁵³³ European Commission, Commission staff working document on Online services, P.46.

Enforcers: Brein

As mentioned in the previous case, Brein was the main copyright enforcement authority in the Netherlands and was financed by collective rights organizations and trade organizations.¹⁵³⁴ To enforce, they focussed on action against specific titles, and against “unlawful” sites. They had a large database containing copies of protected content, and rights holders authorized them to enforce on their behalf. They had developed special in-house software that scanned the Internet for unauthorized content, or for links pointing towards unauthorized content.¹⁵³⁵ In other cases, rights holders notified them about infringing content.¹⁵³⁶

How Brein used notice and takedown depended on the websites themselves. According to Brein, some websites infringed copyrights “incidentally”, in which case notice and takedown worked, while others were according to Brein “systematically and structurally aimed at the illegal supply of unauthorized content,” in which case notices were not properly responded to; there would always be a delay, and content would be placed back faster than they could remove it. In that case, Brein went after the websites themselves. According to Brein, they offered to help those websites clean up their act, for example by helping them take preventative measures. However, according to Brein, most of these sites had a business model aimed at the availability of unauthorized content which made them not interested in Brein’s help. Most of these sites therefore operated anonymously. In 99% of the cases sites did not react when they tried to contact them, according to Brein.

In case direct contact did not work, Brein directed its efforts to the hosting provider, for which it brought evidence against those sites. In 80% of the cases the sites got locked down through the hosting provider. Some hosting providers did not take the content down in an acceptable time frame, which was why Brein built files against these hosting providers as well. In other cases, Brein tried to get the real contact details of the people operating the websites. This could run through the hosting provider as well (although people tended to register under false names, and used anonymous payment methods), however Brein usually knew how to get the real names, for example through payment providers. It was their experience that when they had the real identity of the site operator, these operators tended to quit rapidly.¹⁵³⁷

If Brein found infringing websites that were hosted in other countries, they contacted the organizations of that country. Sometimes Brein took action directly against hosting providers in other countries as well.¹⁵³⁸ In other cases, they asked access providers to block access to websites, like in the case of the pirate bay.

Access providers (XS4ALL & Ziggo)

XS4ALL adhered to the Notice and takedown code of conduct, and according to their website, their policy was in accordance with the code as well.¹⁵³⁹ Their website included a form that rights holders or their representatives could use to notify XS4ALL of infringement.

¹⁵³⁴ Tim Kuik (BREIN), email to author, July 2013

¹⁵³⁵ Tim Kuik (BREIN), email to author, July 2013

¹⁵³⁶ Tim Kuik (BREIN), interviewed by author, May 2013

¹⁵³⁷ Tim Kuik (BREIN), interviewed by author, May 2013

¹⁵³⁸ Tim Kuik (BREIN), interviewed by author, May 2013

¹⁵³⁹ “Klacht over inhoud website,” *XS4ALL website*, <https://www.xs4all.nl/overxs4all/contact/juridisch/>

These complaints were submitted through an online form that had to be filled in, printed, signed, and then faxed to XS4ALL.¹⁵⁴⁰ The website provided a link to policy guidelines regarding the alleged unlawful expressions on the Internet by customers of XS4ALL.¹⁵⁴¹ These policy guidelines described the way complaints, notices, and requests were submitted relating to the alleged unlawful information by customers of XS4ALL. In those guidelines, XS4ALL pointed out it had created a commission of experts that provided advice for the judgments of complex cases.¹⁵⁴²

After notification, XS4ALL would notify its customer, by sending a letter to the customers' invoice address, by sending an email, and through a website notification. The notifier remained anonymous unless he/she requested otherwise. If he/she and the customer could not agree on a solution, the notification would be treated by XS4ALL.¹⁵⁴³ Notifications were subject to requirements: by submitting, the notifier exempted the expert commission or XS4all from claims by third parties that could result from the rejection or acceptance of certain complaints. In the case of copyright law, the notifier had to "sufficiently" make clear that he or she was the rightful owner, or acted on behalf of the rightful owner. The notification had to also be clear and supported by facts.¹⁵⁴⁴ XS4ALL also had agreements with certain parties that could notify in an automated way, and these took into account privacy and proportionality.¹⁵⁴⁵ Notifications could contain a number of requests: to delete or make inaccessible information by a customer, to get the name and address information of a certain customer, or a combination of both.¹⁵⁴⁶

After receiving a notification, XS4ALL would take a decision within 3 working days, unless this was impossible. In that case they would inform the notifier about the reasons for the delay.¹⁵⁴⁷ If XS4ALL believed certain information to be "unmistakably unlawful" (following the latest case law), the decision on deletion or inaccessibility would be taken immediately.¹⁵⁴⁸ XS4ALL would motivate its decisions towards the notifier and their customer and inform them how they could appeal the decision.¹⁵⁴⁹ Stakeholders could appeal the decision through an email that had to be received by XS4ALL not later than 10 days after the decision.¹⁵⁵⁰ This email had to contain the reasons for appeal.¹⁵⁵¹ Following this, XS4ALL would sent the appeal to the other party within 2 days.¹⁵⁵² Within 10 days XS4ALL would take a decision on the appeal.¹⁵⁵³ Notifications would be judged by the provider in accordance with Dutch law and would take into account as much as possible on the latest jurisprudence.¹⁵⁵⁴ They could contain a number of requests: to delete or make

¹⁵⁴⁰ "Klacht over inhoud website," *XS4ALL website*, <https://www.xs4all.nl/overxs4all/contact/juridisch/>

¹⁵⁴¹ For the policy guidelines, see: "Klachten Procedure," *XS4ALL website*, http://www.xs4all.nl/overxs4all/contact/media/beleidsregels_klachten.pdf .

¹⁵⁴² Page 1 of policy guidelines.

¹⁵⁴³ 1.2 of the policy guidelines.

¹⁵⁴⁴ 1.3 of policy guidelines.

¹⁵⁴⁵ 1.4 of policy guidelines.

¹⁵⁴⁶ 4.3 of policy guidelines.

¹⁵⁴⁷ 2.1 of policy guidelines.

¹⁵⁴⁸ 2.2 of policy guidelines

¹⁵⁴⁹ 2.4 of policy guidelines.

¹⁵⁵⁰ 3.1 of policy guidelines.

¹⁵⁵¹ 3.3 of policy guidelines.

¹⁵⁵² 3.2 of policy guidelines.

¹⁵⁵³ 3.4 of policy guidelines.

¹⁵⁵⁴ 4.1 of policy guidelines.

inaccessible information by a customer, to get the name and address information of a certain customer, or a combination of both.

Article 5 of the policy guidelines dealt with concrete requests. When XS4ALL hosted information or served as a mere conduit for information for a customer, and a notifier requested that information to be deleted or made inaccessible, XS4ALL would, if they thought this information was without a doubt unlawful, request the customer to delete the information himself. If the customer did not comply XS4ALL would make sure the information was deleted or inaccessible. XS4ALL would reject a request if the information was not perceived as unlawful by XS4ALL.¹⁵⁵⁵

XS4ALL would only apply notice and takedown to mere conduit if the information could technically be made inaccessible or deleted by them. If this was not the case, they would point the notifier to the possibility to get into contact themselves and provide address details of the customer.¹⁵⁵⁶ If the request involved the alleged unlawful offering of files through P2P software, the notification needed to be about the supply of a significant amount of unlawful files.¹⁵⁵⁷

If a notifier requested the information of a customer that used XS4ALL for hosting or mere conduit, contact and address details were only given if all of the following requirements were met:

- the notifier had sent a pressing request to the customer, through XS4ALL, to hand over his details voluntarily, and the customer had not done so within 5 working days, or claimed he or she did not commit an unlawful act,
- the notifier had not acquired the information collected thus far on the customer in an unlawful manner,
- the possibility that the information or conduct by the customer was unlawful, was reasonable,
- the notifier had shown an interest in getting the details,
- balancing all the interests, the interest of the notifier was the most important,
- it was without a doubt that the information as provided by the notifier related to the customer. In case of P2P conduct this meant that the notifier had to hand over documents that showed how the research to find these acts was done, or in those cases when the notifier provided an IP address, he or she had to show at least three points of time when these acts were committed, or in the case of P2P it would have to be about the supply of a significant amount of alleged unlawful files.¹⁵⁵⁸

When the customer appealed the decision to hand over address details, no details would be handed over, until a decision on this appeal had been reached.

Ziggo was also one of the parties that originally created the notice and takedown code of conduct. They did not have a specific page dedicated to notice and takedown, like XS4ALL. As a large content provider, they had a lot of contact with the larger content providers.

Hosting providers (Leaseweb)

¹⁵⁵⁵ 5.1 of policy guidelines.

¹⁵⁵⁶ 5.2 of policy guidelines.

¹⁵⁵⁷ 5.3 of policy guidelines.

¹⁵⁵⁸ 6.1 of policy guidelines.

Leaseweb made references to the notice and takedown code of conduct in the legal section of its webpage. There was no specific form available, although the webpage referred specifically to DMCA takedown notices (USA) for Leaseweb US.¹⁵⁵⁹

In my interviews, Leaseweb said they could not monitor “everything” users of their services did. Siteds were created very quickly. People ordered space, paid through PayPal for example, and had a site within 15 minutes. The notice and takedown procedure was referenced in the terms of service, and the acceptable use policy.¹⁵⁶⁰

Leaseweb told me they received copyright complaints from numerous organizations and that they followed the notice and takedown procedure to handle those notifications. Usually when they received complaints about copyright violations, they asked the complainant to first address the website host and come back with the answer of the website if that did not work out. According to them, 90% of all problems were solved when complainants first contacted the website.¹⁵⁶¹

When problems were not solved by the website host the abuse department of Leaseweb looked at whether something was “unmistakably illegal”. If they decided it was illegal they took the website down. They argued that deciding this was usually pretty straightforward. Three people looked into the notification, and if they all agreed to take it down, it would be taken down. They said these cases were usually pretty clear and mentioned the hypothetical website “fakerolex.nl” as an example. In the case of doubt, Leaseweb did not take action.¹⁵⁶²

Sending notifications to Leaseweb could be done form free. People could notify by sending an email to abuse@leaseweb. Thereafter, Leaseweb processed the notification taking into account the notice and takedown procedure.¹⁵⁶³

In other cases, third parties looked into torrent traffic to see which IP addresses were being used in torrent swarms. Some of those IP addresses could fall under Leaseweb. If that was the case Leaseweb received a notification. Usually Leaseweb would reply by asking for more information, but they would generally not get a reply in return.¹⁵⁶⁴

Also, Leaseweb used a system of trusted complainants. These were parties, like Brein, that had first established contact with Leaseweb to work together in combating infringement over BitTorrent sites, websites, trackers, pictures on websites, and also live streaming. To cooperate smoothly Leaseweb and these third parties made agreements about enforcement.¹⁵⁶⁵

Regarding copyright, Leaseweb had five trusted complainants, all organizations with a good reputation in their field, according to Leaseweb. To become a trusted complainant, these organizations took up contact with Leaseweb, after which Leaseweb met with the organizations, “to see who they are” and to judge their trustworthiness on making correct notifications.¹⁵⁶⁶ People could lose their trusted complainant status if notifications became incorrect. Trusted complainants had to provide this data on infringement in a dossier, which could be send to the customers of Leaseweb, so they could react to the notifications.¹⁵⁶⁷

¹⁵⁵⁹ “Legal Information,” *Leaseweb website*, <http://www.leaseweb.com/en/legal>

¹⁵⁶⁰ Alex de Joode (Leaseweb), interviewed by author, May 2013

¹⁵⁶¹ Alex de Joode (Leaseweb), interviewed by author, May 2013

¹⁵⁶² Alex de Joode (Leaseweb), interviewed by author, May 2013

¹⁵⁶³ Alex de Joode (Leaseweb), interviewed by author, May 2013

¹⁵⁶⁴ Alex de Joode (Leaseweb), interviewed by author, May 2013

¹⁵⁶⁵ Alex de Joode (Leaseweb), interviewed by author, May 2013

¹⁵⁶⁶ Alex de Joode (Leaseweb), interviewed by author, January 2014

¹⁵⁶⁷ Alex de Joode (Leaseweb), interviewed by author, January 2014

10.4 Scale, severity and procedural safeguards

Scale

Enforcers: Brein

In 2009, Brein shut down 615 websites, of which 393 were BitTorrent sites, 35 were eDonkey servers, 38 were video streaming sites, and 14 were Usenet portals.¹⁵⁶⁸ In 2010, Brein shut down more than 600 websites, mostly BitTorrent sites, streaming sites, and link sites that used cyber lockers. At Dutch cyber lockers more than 45,000 unauthorized files were removed.¹⁵⁶⁹ In 2011 they took down 594 websites that granted access to illegal files, most of them BitTorrent sites (383), but also link sites, streaming sites, and Usenet link sites.¹⁵⁷⁰ In 2012, Brein removed 571 sites.¹⁵⁷¹ In 2013, BREIN shut down 206 Pirate Bay proxies, 280 Cyber locker linking sites, 10 file-hosting sites, 66 streaming sites and 38 Usenet sites.¹⁵⁷²

Apart from the websites, Brein chased auction sites that offered illegal copies of content or illegal carriers of content. They removed the advertisements on auction sites as well (thousands), and cooperated with police to stop traffic in goods that contained protected content.¹⁵⁷³

Access providers (XS4all and Ziggo)

For XS4ALL, most copyright conflicts were solved outside of the notice and takedown procedure. The number of requests they got was limited, at about one request a month. Before the code was introduced, this number was higher (around 20 a month). These complaints were usually about photos. According to XS4all, Brein has never sent any requests.¹⁵⁷⁴

Apart from that, there were a lot of automated requests, mostly from other countries. Like XS4ALL, usenet providers all over the country received these. Although XS4ALL did not carry out these requests as a principle,¹⁵⁷⁵ they were collected (in an anonymous fashion).¹⁵⁷⁶ These requests were related to Usenet and to IP addresses and came mostly from three major enforcement players.

They were sent in on an XML format through email. The standards for sending in were the same, offered open source, to make it as easy as possible (which also means cheap) for the receiving party to do something with this. Notices were also PGP signed to make them easy to verify.¹⁵⁷⁷ In 2.5 years, XS4ALL received 133,000 unique notifications.¹⁵⁷⁸

¹⁵⁶⁸ "BREIN logboek: Resultaten 2009 en koers 2010," *BREIN* (January 1, 2010), <http://www.anti-piracy.nl/artikelen.php?id=5>.

¹⁵⁶⁹ "BREIN jaarboek 2010," *BREIN* (January 4, 2011), <http://www.anti-piracy.nl/artikelen.php?id=13>.

¹⁵⁷⁰ "BREIN statistieken 2011: ongeveer 600 sites, 60.000 advertenties en 60 beunhazen gesloten," *BREIN* (February 2, 2012), <http://www.anti-piracy.nl/nieuws.php?id=252>.

¹⁵⁷¹ "BREIN jaarstatistieken 2012," *BREIN* (January 15, 2013), <http://www.anti-piracy.nl/nieuws.php?id=285>.

¹⁵⁷² "Software Piracy Stat Watch," *V.i.labs*, <http://www.vilabs.com/resource-section/stat-watch/#sthash.IQLZ7L4j.dpuf>.

¹⁵⁷³ "BREIN jaarstatistieken 2012," *BREIN* (January 15, 2013), <http://www.anti-piracy.nl/nieuws.php?id=285>.

¹⁵⁷⁴ Margreth Verhulst (XS4ALL), interviewed by author, May 2013

¹⁵⁷⁵ Joost Schellevis, "Usenetproviders zien flinke toename takedown-requests," *Tweakers* (November 9, 2012), <http://tweakers.net/nieuws/85442/usenetproviders-zien-flinke-toename-takedown-requests.html>.

¹⁵⁷⁶ Arjan van Hattum (XS4ALL), interviewed by author, November 2013

¹⁵⁷⁷ Arjan van Hattum (XS4ALL), interviewed by author, November 2013

This meant there had been complaints about approximately 10% of all XS4ALL users. Throughout time, the number of notifications increased, probably because detection measures became better, according to XS4ALL.¹⁵⁷⁹ Notifiers went after movies and TV mostly, and it concerned popular protocols. Although XS4ALL did not undertake any action on these requests, they told me that most of these complaints seemed to be justified (by which they meant that the complaint was related to an infringing uploader on their networks).

Ziggo rarely received complaints, although they did tell me that Brein complained once about the Pirate Bay, and that Brein also did a NAW data request. The latter did not work out because according to Ziggo Brein had not spotted infringement in a legal way. Ziggo told me they never got notifications on news groups. Moreover, they were not familiar with any automated requests. They claimed that they probably received no automated requests because the hosting they offered on their networks only allowed for limited space and was at the same time personal. According to Ziggo their customers did nothing illicit because “on their personal space, people won’t do illegal stuff.” Ziggo did get requests from the justice department, but they concerned criminal behavior.¹⁵⁸⁰

Hosting providers (Leaseweb)

Unfortunately, Leaseweb did not release any official numbers, so all the data I received through this interview I could not verify. They said that the notifications Leaseweb received through the notice and takedown procedure came mainly from Brein, 84 in 2012.¹⁵⁸¹ In addition Leaseweb had five trusted complainants that issued about the same amount of notifications as Brein.¹⁵⁸² These takedowns were usually about small breaches like samples. There was a difference between notifications and infringements. Some notifications would concern sites that provided 1000 links, or 1,000 notices concerning 1,000 different links.¹⁵⁸³ An estimate of the total amount of notifications per year through this program would then be around 400.

They involved all kinds of content, mostly from Youstream sites. These notifications also targeted sites that normally had conditional access, or boxes to intercept cable.¹⁵⁸⁴ In some cases enforcers asked for contact details. Leaseweb told me that between 2008 and 2013 this happened twice, and Leaseweb refused both times (both requests came from Brein).¹⁵⁸⁵

Apart from that they received other notifications that did not refer to notice and takedown, or were automatically generated. The number of received automated requests was particularly big. Leaseweb offered a lot of bandwidth and infrastructure, which was why they had big clients that offered user generated content. These were sites where people could upload movies, or files, which could be downloaded by others.¹⁵⁸⁶

¹⁵⁷⁸ Arjan van Hattum (XS4ALL), interviewed by author, November 2013

¹⁵⁷⁹ Arjan van Hattum (XS4ALL), interviewed by author, November 2013

¹⁵⁸⁰ Marcel Eswilder (Ziggo), interviewed by author, May 2013

¹⁵⁸¹ Alex de Joode (Leaseweb), interviewed by author, May 2013

¹⁵⁸² Alex de Joode (Leaseweb), interviewed by author, January 2014

¹⁵⁸³ Alex de Joode (Leaseweb), interviewed by author, May 2013

¹⁵⁸⁴ Alex de Joode (Leaseweb), interviewed by author, January 2014

¹⁵⁸⁵ Alex de Joode (Leaseweb), interviewed by author, May 2013...

¹⁵⁸⁶ Alex de Joode (Leaseweb), interviewed by author, May 2013

Nonetheless, the number of requests that actually required action was not that large, according to Leaseweb. They did not keep a record of automated requests, or as they said “don’t count” automated requests. According to Leaseweb, these requests were usually aimed at IP addresses in use at Leaseweb, which would send torrent traffic. Leaseweb claimed that the senders of these automated requests were made by a “money Machine” for link reporting, meaning those specific companies were funded per reported link.¹⁵⁸⁷ According to Leaseweb the amount of requests ranged in the 100,000 in total, of which 5% were notifications they “can do something with.”¹⁵⁸⁸

Severity

The severity of notice and takedown in the Netherlands ranged from taking down advertisements on auction sites, to taking down specific links and whole websites. Enforcement organizations like Brein tried to get access to contact details to be able to pressure them to taking websites down.

Safeguards

Like in the US, the Dutch notice and takedown provisions have been researched by different organizations.

In 2004, Bits of Freedom, a Dutch NGO that aimed to protect digital human rights, did research on how providers handled complaints on copyright infringement, called ‘the Multatuli project’). To test copyright safeguards they selected an Old Dutch text that had been in the public domain for almost 50 years, and placed that text online with different providers. After sending the providers a complaint from a free Hotmail address, posing as a legal advisor for a rights holder, 70% of all providers removed the content, without verifying if the complaint was justified or not.¹⁵⁸⁹

In this research Bits of Freedom tested three business hosting providers (Active 24, iFast, and Yourhosting), who all removed the content and two free access providers (Tiscali and Wannadoo) who also removed the text right away. The three paid access providers (Demon, Planet Internet, and xs4all) all used written checklists in their procedure. XS4ALL checked and did not remove the content, whilst another provider (UPC) did not accept complaints from an unverifiable email address. Freeler, another provider, completely ignored the complaint and did not react.¹⁵⁹⁰ This research created some controversy, and led to the adoption of the code of conduct for notice and takedown.

In 2009, the legal consultancy firm ‘ICT Recht’ conducted research similar to the above cited research of Bits of Freedom.¹⁵⁹¹ They placed a text that was in the public domain on a number of weblogs and profile pages made on community sites (Web-log.nl, punt.nl, Netlog.com, Hyves.nl, WaarBenJij.Nu, Blogger.com, and Myspace.com). After notification,

¹⁵⁸⁷ Alex de Joode (Leaseweb), interviewed by author, May 2013

¹⁵⁸⁸ Alex de Joode (Leaseweb), interviewed by author, January 2014

¹⁵⁸⁹ Bits of Freedom, "Providers verwijderen tekst Multatuli," *Bits of Freedom website* (October 13, 2004). <https://www.bof.nl/2004/10/13/providers-verwijderen-tekst-multatuli/>

¹⁵⁹⁰ Bits of Freedom, "Providers verwijderen tekst Multatuli."

¹⁵⁹¹ Matthijs van Bergen, "Communitysite geven te gemakkelijk toe bij auteursrechtclaims," *Hostingrecht.nl*, <https://hostingrecht.nl/auteursrecht/communitysites-geven-te-gemakkelijk-toe-bij-auteursrechtclaims/>, the full study by ICT Recht can be found here: <https://ictrecht.nl/notice-takedown-rapport-communitysites-ictrecht-20090306.pdf>

almost every site reacted by removing the post, the whole blog or even the whole profile. That meant these websites did not follow their own policy for notice and takedown. Appeals by the person posting the content online were to no avail.

In the end of 2012, Bits of Freedom did more research on the takedown policy of hosting providers.¹⁵⁹² They chose 10 hosting providers (STRATO, TransIP, Hostnet, Flexwebhosting, Vevida, Antagonist, Hostingdiscounter, WatSnel.nl, Yourhosting en Sity). The researchers created a website with public domain content, and then sent the providers a notice and takedown complaint on behalf of a foundation supposedly protecting the copyrights of the content, from a Gmail address. The research reveals that 9 out of 10 hosting providers had no actual information or procedure that showed how they handled complaints or notices. None of the providers used the code of conduct, as provided by the Dutch ministry and a number of private organizations. The terms and conditions of these providers generally did not provide any guidance on how the complaints were handled either. It was for example often unclear how information would be provided, what information would be provided, and how the procedure would take place. Most general conditions gave providers a lot of freedom to delete or block access to information. Only two providers were interested what the identity was of the complaining party. No provider reacted to the lack of information in the complaint (there was no URL provided).

Four of the ten providers replied to complaints and said that they would only remove material after a judicial decision. Only two providers examined the content and judged the information to be correct. The hosting providers also were not careful with privacy sensitive information. For one provider, the website owner was not notified that there was a complaint. The complaining party was sent all the private information of the owner of the supposedly infringing website.¹⁵⁹³

The experiments cited above intended to show the more problematic aspects of notice and takedown as applied by Dutch companies. The organizations argued that they showed that certain consumer rights, like procedural safeguards, were insufficiently protected. This eventually led to the code of conduct cited in an earlier section. Not having enough safeguards would be problematic, as other outlets have shown that even organizations like Brein made mistakes when applying this procedure.¹⁵⁹⁴ Brein themselves claimed that their error rate was limited.¹⁵⁹⁵ Leaseweb said they received little feedback on takedowns, so they did not know whether or not they did wrongful takedowns.¹⁵⁹⁶ The Clinic, a legal aid organization in the field of information law, said they “assumed” there were wrongful takedowns, but that they did not reach their desk “for some reason,” which according to them, could be because the people putting the content up are not notified of the takedown.¹⁵⁹⁷

Privacy

¹⁵⁹² Bits of Freedom, “Overgeleverd aan willekeur, onderzoek naar de verwijdering van rechtmatige informatie door hostingproviders,” Bits of Freedom website (December 22, 2012). Dutch version can be found here: <https://www.bof.nl/live/wp-content/uploads/20120401-overgeleverd-aan-willekeur-rapport.pdf>

¹⁵⁹³ Bits of Freedom, “Overgeleverd aan willekeur, onderzoek naar de verwijdering van rechtmatige informatie door hostingproviders.”

¹⁵⁹⁴ Niels Westerlaken, “BREIN verwijdert onterecht advertenties: auteurs de dupe,” *Bits of Freedom* (October 10, 2012), <https://www.bof.nl/2012/10/10/brein-verwijdert-onterecht-advertenties-auteurs-de-dupe/>.

¹⁵⁹⁵ Tim Kuik (BREIN), interviewed by author, May 2013

¹⁵⁹⁶ Alex de Joode (Leaseweb), interviewed by author, January 2014

¹⁵⁹⁷ Wilko Miletic (Clinic), email to author, June 2013

The question is to what extent personal data are processed, stored or used to enforce copyrights in this strategy. Rights holders essentially located the infringement themselves, by searching for it. Brein for example said they had a large database containing copies of protected content, and that they used special in-house software to scan the Internet for unauthorized content, or for links pointing towards unauthorized content.¹⁵⁹⁸

The law did not prescribe the processing of personal data to apply notice and takedown at the level of the service providers. None of these enforcement actions directly involved the infringer, unless the rights holders or representatives tried to get contact details of the person responsible for infringing content. Getting these contact details was however subject to strict requirements, as laid down by case law.¹⁵⁹⁹

It was unclear how often these contact details were actually granted. Brein themselves told me they tried to get the real contact details of the people operating the websites. This could run through the hosting provider as well (although people tended to register under false names, and use anonymous payment methods), but Brein usually “had ways” to get the real names, for example through payment providers. Their experience was that when they had the real identity of the site operator, those operators tended to quit rapidly.¹⁶⁰⁰

However, Ziggo and Leaseweb told me that Brein had rarely asked for contact details and that in those cases, they had refused to give them. XS4ALL was never asked for contact details, they claimed. XS4ALL subscribed to the code of conduct on notice and takedown and in their code of conduct described a list of requirements that all had to be met before contact details were given.¹⁶⁰¹ Moreover, their procedure allowed the customer the opportunity to appeal the decision to hand over address details.

It was however unclear to what extent other organizations adhered to similar procedures. In the experiments done by Bits of Freedom, in 2004 one ISP sent on information about their client to the complainant, even without them asking for it.¹⁶⁰² This situation had not improved in 2012, when two hosting providers sent private information to the complainant.¹⁶⁰³

Impartial, competent, and independent judge

There were multiple parties who judged whether or not content was infringing. The notifying parties (rights holders and their representatives) were the first parties to judge whether content was infringing. They had an obvious interest in the process. The previous case showed that some of these parties may be incentivized to do certain amounts of takedowns. Leaseweb suggested something similar. This could incentivize a broader application of copyrights than necessary, or cause those parties to err on the side of more enforcement. It was clear that these parties were not impartial or independent, although these enforcing parties suggested that they made sure they were correct. Brein for example, not only used

¹⁵⁹⁸ Tim Kuik (BREIN), email to author, July 2013

¹⁵⁹⁹ van Eijk et al., *Moving Towards Balance*, P.52.

¹⁶⁰⁰ Tim Kuik (BREIN), interviewed by author, May 2013

¹⁶⁰¹ 6.1 of policy guidelines.

¹⁶⁰² Bits of Freedom, "Providers verwijderen tekst Multatuli."

¹⁶⁰³ Bits of Freedom, "Overgeleverd aan willekeur, onderzoek naar de verwijdering van rechtmatige informatie door hostingproviders."

software, but when results did not score 100% with the back catalog, they used human validation to make sure content was infringing before notifying about it.¹⁶⁰⁴

More important were the ISPs, who would decide on whether to issue a takedown on the basis of the complaints by rights holders. They were the next and more important parties to judge whether content was infringing. With regard to impartiality and independence it was clear that none of those ISPs had a financial dependency on rights holders. However Ziggo offered a large catalogue of content and XS4ALL had started offering some content to its customers.

Individually, ISPs had taken measures to increase the reliability of their judgements. Leaseweb said they had an abuse department which made sure that content would only be taken down if it was “unmistakably illegal”,¹⁶⁰⁵ and XS4ALL had created a commission of experts that would help with the judgement of complex cases.¹⁶⁰⁶

Just like in the last case, many feared that ISPs would be incentivized to simply accept complaints by rights holders, because they could lose their safe harbors if they did not remove illegal content. This could threaten their impartiality.

The above cited experiments done by Bits of Freedom and ICTrecht seemed to confirm this image, but there information was dated. In 2004 it seemed that content was removed by those teams without any idea about copyright basics.¹⁶⁰⁷ The research done by ICT Recht in 2009 showed that out of seven community sites, only one actually displayed legal knowledge, making clear their message was written by the legal department, using correct statements and clearly saying why they did not want to process the claim. Other departments seemed to lack that knowledge, saying that copyright law “can’t just lapse,” or just believing that the book was “apparently” copyright protected after receiving a notification about it.¹⁶⁰⁸ In 2012, again, most ISPs did not properly research the claims sent by fake notifiers. But they also displayed a lack of copyright knowledge. For example, four out of ten hosting providers said they could only make the information unavailable after a judicial order (which was not actually true).¹⁶⁰⁹ These experiments were done some time ago, so it was unclear how the situation was at the time of this research. Meanwhile, it seemed that in 2012 the situation had shifted to an opposite because sites were hesitant to remove any material. It still showed a lack of competence was present at the level of those ISPs.

Leaseweb created an additional system for adjudication. By allowing for trusted complainants, they removed their judgement from the process, by effectively placing that burden on the plaintiffs themselves. Their position could hardly be seen as impartial or independent, although Leaseweb created an additional safeguard by awarding reputation and discouraging wrongful takedowns. It was however uncertain how this was applied.¹⁶¹⁰

¹⁶⁰⁴ Tim Kuik (BREIN), interviewed by author, May 2013

¹⁶⁰⁵ Alex de Joode (Leaseweb), interviewed by author, May 2013

¹⁶⁰⁶ Page 1 of policy guidelines.

¹⁶⁰⁷ Bits of Freedom, "Providers verwijderen tekst Multatuli."

¹⁶⁰⁸ van Bergen, "Communitysite geven te gemakkelijk toe bij auteursrechtclaims."

¹⁶⁰⁹ Bits of Freedom, "Overgeleverd aan willekeur, onderzoek naar de verwijdering van rechtmatige informatie door hostingproviders."

¹⁶¹⁰ Alex de Joode (Leaseweb), interviewed by author, January 2014

Presumption of innocence

The procedure would seem to lay some burden of proof on the notifying parties, but the question remained to what extent this worked out in practice.

Although the system required some information to process takedown requests, it was not clear if there were checks on how infringement took place, whether it took place over a long time, what the purpose was of the infringement, and to what extent the infringement affected the artist.

It was difficult to properly evaluate how the ISPs dealt with the burden of proof differently. All three said they adhered to the code of conduct as agreed on in 2008. However, only XS4ALL had a clear code of conduct on their website which described how they dealt with complaints (mentioned in the section on the procedure in practice). In their code of conduct, XS4ALL placed the burden of proof on the notifying parties by adding numerous requests to the notifications sent to them (these have been described in the section on the procedure in practice). Leasweb tried to get the notifier and their client to sort out the problems themselves before turning to their abuse department.¹⁶¹¹

As mentioned above, Leasweb also used a system of trusted complainants. The burden of proof here would seem to be shifted to the notifying parties, but only in terms of reputation. The actual notifications would be accepted. In that system, wrongful applications by rights holders would be punished, but it was unclear how that would happen.¹⁶¹²

Although it appeared that in principle, ISPs seemed committed to the correct adjudication and standards of evidence, there were hardly economic or legal costs to penalize copyright holders for sending wrong or overbroad copyright notices. This could incentive them to send notices for cases of questionable infringement, de minimis infringement, or in clear cases of fair use.¹⁶¹³ A problem with a lot of the takedowns in previous research was that those takedowns disregarded fair use exceptions. This was problematic because the Dutch system did not allow for a counter notice system. This meant that a user would have to prove his innocence.¹⁶¹⁴

It remained difficult to evaluate how often copyright law was applied erroneously, or whether the burden of proof was placed on rights holders in practice.

Previous experiments, done by Bits of Freedom and ICTrecht suggested that for many other ISPs at the time, the burden of proof seemed to be on content providers, and not on rights holders. However the most recent experiment from 2012 suggested it was in some cases the other way around.¹⁶¹⁵

These changes in performance could be attributed to the attention given to the procedure by media and organizations like Bits of Freedom. One could argue that the reputation of ISPs administering the procedure incentivized them to be more aware of these procedures and the correct application of them.

¹⁶¹¹ Alex de Joode (Leasweb), interviewed by author, May 2013

¹⁶¹² Alex de Joode (Leasweb), interviewed by author, January 2014

¹⁶¹³ Charles W. Hazelwood Jr, "Fair Use and the Takedown/Put Back Provisions of the Digital Millennium Copyright Act," *Idea* 50 (2009): 307. P.307.

¹⁶¹⁴ Jennifer Urban and Laura Quilter, "Efficient Process or 'Chilling Effects'? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act," *Santa Clara Computer and High Technology Law Journal* 22 (2006): 621. P. 635-636.

¹⁶¹⁵ Bits of Freedom, "Overgeleverd aan willekeur, onderzoek naar de verwijdering van rechtmatige informatie door hostingproviders."

Notice, right to be heard (prior to conviction), defenses and appeal

Here again, it was difficult to evaluate how different ISPs dealt with the system. XS4ALL described in their code of conduct an elaborate system that allowed the allegedly infringing customer to be notified (in multiple ways), to solve the problem with the notifier,¹⁶¹⁶ and also for appeal in which customers could state their arguments for appeal.¹⁶¹⁷ Ziggo claimed to adhere to a similar code of conduct.

For Leaseweb, it was unclear whether there was a notification system. However, Leaseweb immediately referred the notifier to the client, which would mean the customer and rights holders had the chance to solve the disagreement before action was undertaken by the ISP.¹⁶¹⁸

In the case of trusted complainants, alleged infringers were subject to removal (generally) of their expressive materials, before they themselves received a notice of the complaint.¹⁶¹⁹

The experiments done by Bits of Freedom and ICT Recht suggested that in 2004, few ISPs notified the client.¹⁶²⁰ According to ICT Recht, community sites mostly notified the client, but hardly allowed for appeal (only one out of seven).¹⁶²¹ In 2012, most hosting providers notified their clients (all except one).¹⁶²²

Transparency

As mentioned before, XS4ALL clearly posted their Notice and takedown code of conduct on their website, and claimed their policy was in accordance with this code as well.¹⁶²³ In here they described exactly how they dealt with notifications of infringement.¹⁶²⁴ XS4ALL also motivated its decisions and would let the notifier and customer know in what way they could appeal the decision.¹⁶²⁵

Ziggo referred to the code of conduct on their website. Leaseweb displayed references to the notice and takedown code of conduct on its legal page. There was no specific form available. It also had a specific reference to DMCA takedown notices (USA) for Leaseweb US.¹⁶²⁶

The experiments done by Bits of Freedom and ICT Recht on other ISPs revealed that other ISPs were not transparent at the time. ICT Recht concluded that most community sites did not have a clear notice and takedown procedure, and that the ones that did, hardly followed them.¹⁶²⁷ Bits of Freedom in 2012 revealed that nine out of ten hosting providers

¹⁶¹⁶ 1.2 of the policy guidelines.

¹⁶¹⁷ 3.1 t/m 3.4 of policy guidelines.

¹⁶¹⁸ Urban and Quilter, "Efficient Process or 'Chilling Effects'?" P. 636.

¹⁶¹⁹ Urban and Quilter, "Efficient Process or 'Chilling Effects'?" P. 636.

¹⁶²⁰ Bits of Freedom, "Providers verwijderen tekst Multatuli."

¹⁶²¹ van Bergen, "Communitysite geven te gemakkelijk toe bij auteursrechtclaims."

¹⁶²² Bits of Freedom, "Overgeleverd aan willekeur, onderzoek naar de verwijdering van rechtmatige informatie door hostingproviders."

¹⁶²³ "Klacht over inhoud website," XS4ALL website, <https://www.xs4all.nl/overxs4all/contact/juridisch/>

¹⁶²⁴ Page 1 of policy guidelines.

¹⁶²⁵ 2.4 of policy guidelines.

¹⁶²⁶ "Legal Information," Leaseweb website, <http://www.leaseweb.com/en/legal>

¹⁶²⁷ van Bergen, "Communitysite geven te gemakkelijk toe bij auteursrechtclaims."

did not have a specific notice and takedown procedure. Terms and conditions did not provide clarity either.¹⁶²⁸

In 2013, both Leaseweb¹⁶²⁹ and XS4ALL¹⁶³⁰ started publishing transparency reports. However, these did not deal with copyright related requests.

Proportionality

To be proportional, sanctions need to be necessary, suitable and not an unreasonable burden on individual rights. It was unclear how much infringement was hosted on the websites that were studied for this research. It was clear however that Brein took down a large amount of infringing content per year. Meanwhile, hosting provider Leaseweb received enough complaints to introduce a trusted removal program. This did suggest that many ways in which content was offered online were now cut off. In that sense it was suitable as well. Brein, the leading anti-piracy authority, think notice and takedown “works,” they told me.¹⁶³¹

Taking down websites or infringing expressions could be a burden on speech, but only when it happens erroneously, or when more content is removed than is actually infringing. Unfortunately, there were not enough examples to verify this.

10.5 Impact on infringement levels

Notice and takedown aimed to deter a particular type of infringement: copyright infringement hosted on servers in the Netherlands. It was difficult to get data on the amount of hosted infringement in the Netherlands and any increase or reduction in those numbers and whether those numbers could be attributed to enforcement. There were general numbers on infringement in the Netherlands. Research done by IVIR and CentERdata suggested that overall file sharing was declining. However, this differed per type of content. Whereas sharing music illegally declined, and while sharing games illegally decreased slightly, sharing audiovisual content increased massively between 2008 and 2012. They hypothesized that the steep drop in the sharing of music could be attributed to the rise of viable legal alternatives.¹⁶³² Follow up research suggested that sharing movies illegally kept increasing the following year, but only slightly, while the use of legal services online for audiovisual content increased steeply to the same level as sharing movies illegally.¹⁶³³

Because there were no numbers related to the specific notice and takedown procedures, I also relied on the statements by the anti-piracy authority, Brein. They said that notice and takedown in the Netherlands “works.” They also thought the amount of

¹⁶²⁸ Bits of Freedom, “Overgeleverd aan willekeur, onderzoek naar de verwijdering van rechtmatige informatie door hostingproviders.”

¹⁶²⁹ Alex de Joode, “LeaseWeb first hosting provider worldwide to launch Law Enforcement Transparency Report,” *leaseweb/blog* (April 11, 2013), <http://blog.leaseweb.com/2013/04/11/leaseweb-first-hosting-provider-worldwide-to-launch-law-enforcement-transparency-report/>.

¹⁶³⁰ “Transparantierapport 2012,” *XS4ALL website*, <https://blog.xs4all.nl/2013/07/11/transparantierapport-2012/>

¹⁶³¹ “Brein: 600 sites offline gehaald in 2011,” *Webwereld* (February 21, 2012), <http://webwereld.nl/e-commerce/56117-brein-600-sites-offline-gehaald-in-2011>.

¹⁶³² Joost Poort and Jorna Leenheer, “File sharing 2@12: Downloading from illegal sources in the Netherlands,” *Institute for Information Law & CentERdata*, Amsterdam/Tilburg (2012). Retrieved from http://www.ivir.nl/publications/poort/Filesharing_2012

¹⁶³³ Jorna Leenheer and Joost Poort, “Alleen maar nette mensen.” *Consumentenonderzoek Downloadgedrag Films.* *IVIR/CentERdata* 14 (2014), http://www.ivir.nl/publicaties/download/alleen_maar_nette_mensen.pdf

infringement hosted in the Netherlands was smaller than before.¹⁶³⁴ Brein argued that other countries should clean up their act, and that if other countries would enforce like in the Netherlands, piracy problems would be relatively small.¹⁶³⁵ They also said that completely eliminating piracy would never work, but that they wanted to bring it down to 20-25%.¹⁶³⁶ Brein said the system did not need to work perfectly. "It doesn't have to be waterproof, but water repellent." They said that "if you can bring down the problem to 25% of the market, you still have 75% of it, which is a lot."¹⁶³⁷

However, according to Brein, infringement was also hosted in other countries, which explained why Brein moved towards the blocking of sites by access providers.¹⁶³⁸ XS4ALL said the blocking of sites would not work, as they thought it would require the blocking the whole Internet, by which they meant sites could return just as easily.¹⁶³⁹

10.6 The costs of the system

None of the organizations were willing to share with what the costs of the system were, apart from general statements. Notice and takedown costs were distributed over the rights holders and their enforcement agents, and the ISPs.

Brein was financed by collective rights organizations and trade organizations. They had 12 people working at Brein, but refused to comment on budgetary issues.¹⁶⁴⁰

Previous research had suggested that there was some burden on ISPs, because they had to establish procedures for notice and takedown and thus absorb some of the costs of enforcement. This was especially burdensome for smaller providers.¹⁶⁴¹

Access providers XS4ALL and Ziggo had little people working on this. Both departments also handled other takedown requests for things like hate speech. In Ziggo's case, they had a department that had 5 to 6 people working mostly on spam notifications and phishing.¹⁶⁴² This would suggest that the burden for these organizations was not that large.

Leaseweb had 2 FTE on this system. According to them, one person could do it, but they had more people working in this system because they thought it was important to spread knowledge at the organization.¹⁶⁴³

10.7 Conclusion

This case treated different enforcement actions. For the empirical study, this conclusion grouped the action taken against websites and against content. Hosting providers, website holders and other providers were notified about infringement on their servers, which was

¹⁶³⁴ "Brein: 600 sites offline gehaald in 2011," *Webwereld* (February 21, 2012), <http://webwereld.nl/e-commerce/56117-brein-600-sites-offline-gehaald-in-2011>.

¹⁶³⁵ Tim Kuik (BREIN), interviewed by author, May 2013

¹⁶³⁶ Tim Kuik (BREIN), interviewed by author, May 2013

¹⁶³⁷ Tim Kuik (BREIN), interviewed by author, May 2013

¹⁶³⁸ "Brein: 600 sites offline gehaald in 2011," *Webwereld* (February 21, 2012), <http://webwereld.nl/e-commerce/56117-brein-600-sites-offline-gehaald-in-2011>.

¹⁶³⁹ Margreth Verhulst (XS4ALL), interviewed by author, May 2013

¹⁶⁴⁰ Tim Kuik (BREIN), interviewed by author, May 2013

¹⁶⁴¹ Urban and Quilter, "Efficient Process or 'Chilling Effects'?" P. 636.

¹⁶⁴² Marcel Eswilder (Ziggo), interviewed by author, May 2013

¹⁶⁴³ Alex de Joode (Leaseweb), interviewed by author, January 2014

subsequently taken down. This case is divided in two subcases. One subcase for the regular procedure and one for the trusted removal program as applied by Leaseweb.

The research showed that hundreds of websites and thousands of expressions of content on websites were taken down. Leaseweb had a trusted removal program, that dealt with hundreds of notifications per year alone. As spotting infringement required web crawling and taking content down, privacy rights were often left untouched. However, sometimes enforcers requested the contact details of website owners to force a site down. There were requirements to getting these contact details.

Although it was difficult to evaluate the performance of different ISPs, they claimed to check the accusations individually, and to ask notifiers to contact the alleged infringer. This would allow alleged infringers to be notified and to present their views. Some ISPs also offered the possibility of appeal. Leaseweb had introduced a separate large-scale takedown program for trusted complainants, who would be able to submit more notices that were not reviewed for accuracy but created additional safeguards by rewarding reputation: parties could lose their status of trusted complainant if they made too many mistakes. Regarding transparency, some providers lacked clear information about how they applied notice and takedown. There was also limited information on how it had been applied in the past. Regarding proportionality, there could have been some burden on free speech, but I could not verify this.

Previously done experiments suggested that safeguards were less present in smaller providers. This research could not verify those claims, although some of those experiments were done in a similar timeframe. They highlighted a lack of competence, no clear privacy protection and little transparency.

It was difficult to measure the effect on infringement as this only targeted hosted infringement and there were no data available on this. The anti-piracy authority claimed that it worked. For the ISPs costs were relatively low, but it was unclear to what extent smaller ISPs had new costs. These outcomes will be highlighted again in the conclusion and compared with the outcomes of the other cases.

11. 'OPERATION IN OUR SITES' (USA) IN 2010-2013

11.1 Introduction

The Immigrations and Customs Enforcement launched 'Operation In Our Sites.' One of the aims of this operation was to block access to websites facilitating large-scale copyright infringement. Blocking access was attained through forfeiture actions against domain names allegedly associated with infringing activity. First websites were seized, then at times forfeited. Sometimes this process could lead to a criminal trial against the people associated with the website. This case is therefore divided into three subcases: seizure, forfeiture and trial.

This chapter will first provide the legal background to this procedure. For this section, I used legal sources and information from an article by Karen Kopel in the *Berkeley Technology Law Journal*, which came out during the time I was conducting my interviews.¹⁶⁴⁴ It will then go into the procedure in practice, for which it used legal sources and academic research, after which it will focus on two notable seizures that happened over the course of this period (the seizures of the websites of Dajaz1 and Rojadirecta). For the latter, I spoke to a number of professionals from the field. I interviewed Steven Welk, a lawyer who was involved in the Dajaz1 case on the government side (but only after the seizure itself). I also interviewed Mark Lemley, a lawyer that represented Rojadirecta, but who cannot speak for them, Andrew Bridges, who represented Dajaz1. After that section, the chapter will further describe how this case performs on the variables. For this I supplemented the information mentioned above with news articles, reports by NGOs and an interview with Corynne McSherry of the Electronic Frontier Foundation. The information was collected from January 2012 until the end of 2013.

11.2 Legal background

This procedure was mainly rooted in two additions to U.S. Copyright Law. The Artists' Rights and Theft Prevention Act of 2005 (ART Act) was part of the Family Entertainment and Copyright Act act passed in 2005. It added a new provision to the US copyright law that made it an offense to make copyright protected works available for download on a computer network.¹⁶⁴⁵

On October 13, 2008, President George W. Bush signed the Pro IP Act into law: the Prioritizing Resources and Organization for Intellectual Property Act of 2008 ("Pro IP Act").¹⁶⁴⁶ The law aimed to increase IP enforcement and penalties for IP infringement. One way to increase enforcement was by applying seizure and forfeiture law to IP violation cases.¹⁶⁴⁷

The Pro IP Act also created the Intellectual Property Enforcement Coordinator (IPEC- 15 USC §8111), a position in the executive branch to coordinate intellectual property enforcement among different federal agencies. One of its tasks was the development of a Joint Strategic Plan against piracy and counterfeiting, and assisting federal agencies engaged with IP enforcement with its

¹⁶⁴⁴ Karen Kopel, "Operation Seizing Our Sites: How the Federal Government Is Taking Domain Names Without Prior Notice," *Berkeley Technology Law Journal* 28, (July 2013).

¹⁶⁴⁵ Family Entertainment and Copyright Act of 2005, Pub. L. No. 109-9, §102, 119 Stat. 218, 220 (codified as amended in 18 U.S.C. S 2319B (2006))

¹⁶⁴⁶ Pub. L. No. 110-403, 122 Stat. 4256 (codified at 18 U.S.C. § 2323 (2006))

¹⁶⁴⁷ Kopel, "Operation Seizing Our Sites," P.862-863.

implementation.¹⁶⁴⁸ These federal agencies included the Department of Justice, the FDA, and the FBI.¹⁶⁴⁹

In its 2010 strategic plan the IPEC laid out a strategy for more protection of IP online. To do this, the Obama administration established 'Operation In Our Sites,' "a multi-agency program to investigate and combat sales of counterfeit goods and criminal copyright infringement committed over the Internet by seizing the domain names suspected of engaging in these illicit activities."¹⁶⁵⁰

ICE created the IPR centre, which coordinated 'Operation in Our Sites' among different federal agencies. "The mission of the IPR centre is to address and combat predatory and unfair trade practices that threaten our economic stability and national security, restrict the competitiveness of U.S. industry in world markets, and place the public's health and safety at risk."¹⁶⁵¹ Specifically, 'Operation In Our Sites' "targets websites and their operators that distribute counterfeit and pirated items over the Internet, including counterfeit pharmaceuticals and pirated movies, television shows, music, software, electronics, and other merchandise as well as products that threaten public health and safety," and involved "federal law enforcement investigating and developing evidence to obtain seizure warrants from federal judges. The website domain names are then seized pursuant to the federal seizure warrants and re-directed to display a seizure notice as opposed to offering the content or goods that violate U.S. copyrights or trademarks."¹⁶⁵²

The Pro IP Act introduced the statutory basis for the ICE domain name seizures. Title 18, United States Code, Section 2323 applied the civil forfeiture procedure to property "used to facilitate, or is the proceed of, certain enumerated IP crimes," like criminal copyright and trademark counterfeiting.¹⁶⁵³ At 18 U.S.C. § 2323 Section 2323(a)(1)(A) stipulated that any property, the creation or distribution of which was prohibited under the criminal copyright statute, 17 U.S.C. § 506, would be subject to forfeiture by the government. What qualified as criminal copyright was laid down in title 17 U.S.C section 506, and title 18 U.S.C section 2319 provided the penalties connected to criminal copyright infringement.¹⁶⁵⁴ This meant that the government had to show that there was a violation of § 506 to be able to forfeit property.

The section also applied the Civil Asset Forfeiture Reform Act of 2000,¹⁶⁵⁵ which in turn prescribed in 18 U.S.C. § 981 that the U.S. government could only seize property after it obtained a seizure warrant in compliance with the Federal Rules of Criminal Procedure.¹⁶⁵⁶

In order to obtain a seizure warrant, government officials had to submit a sworn testimony or affidavit to a judge establishing probable cause. If this satisfied the judge, the property could be immediately seized without notice or hearing.¹⁶⁵⁷

¹⁶⁴⁸ Kopel, "Operation Seizing Our Sites," P.868.

¹⁶⁴⁹ The actors are described in: "2010 Joint Strategic Plan on Intellectual Property Enforcement," *Executive Office of the President of the United States* (june 2010), http://www.whitehouse.gov/sites/default/files/omb/assets/intellectualproperty/intellectualproperty_strategic_plan.pdf

¹⁶⁵⁰ Kopel, "Operation Seizing Our Sites," P.871-872, and: "Press Release – Operation in Our Sites," *National Intellectual Property Rights Coordination Center*, www.iprcenter.gov/reports/fact-sheets/operation-inour-sites/view

¹⁶⁵¹ Kopel, "Operation Seizing Our Sites," P.873, and: "2010 Joint Strategic Plan on Intellectual Property Enforcement," *Executive Office of the President of the United States* (june 2010), http://www.whitehouse.gov/sites/default/files/omb/assets/intellectualproperty/intellectualproperty_strategic_plan.pdf, at P.28.

¹⁶⁵² "Fact Sheets," *National Intellectual Property Rights Coordination Center*, <http://www.iprcenter.gov/fact-sheets/view>

¹⁶⁵³ Kopel, "Operation Seizing Our Sites," P.865.

¹⁶⁵⁴ As mentioned in the affidavit in our sites SACLA, at 98.

¹⁶⁵⁵ Civil Asset Forfeiture Reform Act of 2000. Public Law 106-185 (April 25, 2000). <http://www.gpo.gov/fdsys/pkg/PLAW-106publ185/pdf/PLAW-106publ185.pdf>

¹⁶⁵⁶ U.S.C. § 981(b)(2) (2006).

¹⁶⁵⁷ Federal Rules of Criminal Procedure 41 (d)(1)-(2).

This meant federal agents submitted a sworn affidavit to a neutral federal magistrate judge. According to the fourth amendment, if that magistrate judge found probable cause, he or she could issue a seizure warrant. This warrant had to describe the particularity of the thing to be seized. After this, the government initiated forfeiture proceedings against the property.¹⁶⁵⁸

Civil forfeiture required *in rem* jurisdiction (jurisdiction against the thing), which meant the property itself was 'guilty'. This was different from criminal forfeiture, which required jurisdiction *in personam*, against the person. The latter required constitutional protection. This also meant that in civil forfeiture the property itself could be seized, regardless of the culpability of its owner.¹⁶⁵⁹ *In other words*, law enforcement agencies could gain immediate possession of the property before resolution of the action. Also, because these seizures are civil actions, lower burdens of proof, such as probable cause, were enough to establish the forfeiture. The government would only have to demonstrate that they believed the property was in some way connected with an underlying criminal offense.¹⁶⁶⁰

The difference from ordinary seizure was that in the online world the property was not actually seized but the domain name registry would redirect traffic from a seized domain name to a banner explaining that the site had been seized.¹⁶⁶¹ As the affidavit that seized Dajaz1 mentioned: "neither a restraining order nor an injunction is sufficient to guarantee the availability of the subject domain names for forfeiture. By seizing the subject domain names and redirecting them to another website the government will prevent third parties from acquiring the names and using them to commit additional crimes. Furthermore, seizure of the domain names will prevent third parties from continuing to access the five websites listed above."¹⁶⁶² Although the Pro IP Act never mentioned that civil forfeiture rules applied to domain names, the DOJ and ICE used the article as their legal basis.¹⁶⁶³

Forfeiture meant the permanent taking of property by the government or other party without compensation, because of a breach or default of a legal obligation or commission of a crime.¹⁶⁶⁴ For 'Operation In Our Sites,' sites were first seized to later commence a civil forfeiture proceeding.¹⁶⁶⁵

Interestingly, Microsoft used a similar strategy to use trademark law to seize botnet infected networks. In that case, the botnet operators had been using a letter template with Microsoft's logo on it.¹⁶⁶⁶

11.3 The procedure in practice

Chapter 46 of Title 18 prescribed the steps the government had to follow to conduct civil forfeiture (in particular 18 U.S.C. §981 and §983): first, federal officers investigated suspected websites. In the case of trademark, they could order certain items to see whether they were trademark protected or cheap knockoffs for example, and compare those with originals, with the help of rights holders. For copyright, this meant they could download or stream content and then check with rights holders to

¹⁶⁵⁸ Kopel, "Operation Seizing Our Sites," P.865.

¹⁶⁵⁹ Kopel, "Operation Seizing Our Sites," P.864. and: Robert Lieske, "Civil Forfeiture Law: Replacing the Common Law with a Common Sense Application of the Excessive Fines Clause of the Eighth Amendment," *WM. MITCHELL L. REV.* 21 (1995):265. P.266-271.

¹⁶⁶⁰ Michael J. Harrell, "Fighting Piracy with Censorship: The Operation in Our Sites Domain Seizures v. Free Speech," 21 *Journal of Intellectual Property Law* 137 (2013). P.146.

¹⁶⁶¹ Kopel, "Operation Seizing Our Sites," P.866.

¹⁶⁶² As mentioned in the affidavit in our sites SACLA, 100

¹⁶⁶³ Kopel, "Operation Seizing Our Sites," P.867.

¹⁶⁶⁴ Kopel, "Operation Seizing Our Sites," P.866.

¹⁶⁶⁵ Kopel, "Operation Seizing Our Sites," P.866-867.

¹⁶⁶⁶ Brian Fung, "How Microsoft killed off a massive botnet, with trademark law," *The Washington Post* (July 24, 2013), <http://www.washingtonpost.com/blogs/wonkblog/wp/2013/07/24/how-microsoft-killed-off-a-massive-botnet-with-trademark-law/>.

see whether the content was protected.¹⁶⁶⁷ For example, in the affidavit aimed at rapgodfathers.com, torrent-finder.com, rmx4u.com, dajaz1.com, and onsmash.com, the special agent responsible mentioned talks he had with RIAA officials or the MPA.¹⁶⁶⁸

DOJ attorneys then evaluated this sort of evidence and would check whether there was enough information to get a seizure order for the sites investigated. These attorneys would take into consideration the popularity of the website, whether it was commercial in nature and profitable, and whether the seizure of the domain would have a substantial impact on piracy. They also had to determine whether the domain names were registered in the US, for jurisdictional reasons.¹⁶⁶⁹

The ICE and the IPR centre then presented the affidavits to a federal magistrate judge who determined whether probable cause had been established.¹⁶⁷⁰ If that was the case, the judge granted a seizure order that would be served on the domestic domain name registry.¹⁶⁷¹ Action brought were thus limited to domain names with a U.S. based registry.

This domain name registry then had to lock and restrain the domain name until the completion of the forfeiture proceeding, which would lead to the U.S government acquiring title, rights and interests of the domain name.¹⁶⁷² In the affidavit: "Upon execution of the seizure warrant, the registry for the ".net" and ".com" top-level domains, Verisign, Inc.,(.....) shall be directed to restrain and lock the (...) domain names pending transfer of all right, title, and interest in the (.. domain names...) to the United States upon completion of forfeiture proceedings, to ensure that changes to the (..domain names..) cannot be made absent court order or, if forfeited to the US, without prior consultation with ICE."¹⁶⁷³ In other words, an actual 'seizure' would not take place. Instead, the ISPs were required to redirect traffic away from the domain name towards a webpage saying the domain had been seized.¹⁶⁷⁴ As a result, the IP address associated with the domain would be replaced with the IP address of the webpage mentioning the domain had been seized.¹⁶⁷⁵

Only after the seizure had taken place, interested individuals like the owner of the website could contest the measure. The government had to send written notice to the website owner within sixty days of seizure or had to file a judicial forfeiture action against the property and provide notice of that to the interested parties (as laid down in 18 U.S.C. § 983(a)(1)(A)(i)-(ii)).¹⁶⁷⁶

This deadline could be extended if the government could show there was reason to believe that the provision of a notice would have an adverse effect on the proceedings (§ 983(a)(1)(C)-(D)).

After notice, the website owner (or any other interested party) would be allowed to file a claim with the agency within a deadline set in the written forfeiture notice. As a result the government had to file a complaint for forfeiture within ninety days of filing the claim, or return the property (as laid down in 18 U.S.C. § 983(a)(2) and (3)).¹⁶⁷⁷ If the website owner did not file a petition

¹⁶⁶⁷ Kopel, "Operation Seizing Our Sites," P.874. AND: Affidavit in Support of Application for Seizure Warrant at ¶¶ 8, 17, 28, United States v. The Following Domain Names: rojadirecta.org, and rojadirecta.com, No. 11-MAG-262 (S.D.N.Y. Jan. 31, 2011) [hereinafter Rojadirecta Affidavit]; Application and Affidavit for Seizure Warrant at ¶¶ 79–82, In re Seizure of The Following Domain Names:RapGodFathers.com, et al., No. 10-2822M (C.D. Cal. Nov. 17, 2010), available at <http://s3.amazonaws.com/nytdocs/docs/543/543.pdf>

¹⁶⁶⁸ Mentioned in affidavit, at: "In the Matter of the Seizure of the Internet Domain Name "Dajaz1.com"", Electronic Frontier Foundation, <https://www.eff.org/nl/cases/matter-seizure-internet-domain-name-dajaz1com>

¹⁶⁶⁹ Kopel, "Operation Seizing Our Sites," P.874.

¹⁶⁷⁰ Kopel, "Operation Seizing Our Sites," P.875.

¹⁶⁷¹ Kopel, "Operation Seizing Our Sites," P.875.

¹⁶⁷² Kopel, "Operation Seizing Our Sites," P.875.

¹⁶⁷³ As mentioned in the affidavit in our sites SACLA, 102.

¹⁶⁷⁴ Michael J. Harrell, "Fighting Piracy with Censorship: The Operation in Our Sites Domain Seizures v. Free Speech," 21 *Journal of Intellectual Property Law* 137 (2013). P.142

¹⁶⁷⁵ Michael J. Harrell, "Fighting Piracy with Censorship: The Operation in Our Sites Domain Seizures v. Free Speech," 21 *Journal of Intellectual Property Law* 137 (2013). P.143

¹⁶⁷⁶ Kopel, "Operation Seizing Our Sites," P.876.

¹⁶⁷⁷ Kopel, "Operation Seizing Our Sites," P.876.

or claim before the set deadline, the domain name automatically would become property of the U.S. government.¹⁶⁷⁸

If they did file a complaint, they had to show that not having the property would cause substantial hardship (§ 983(f)(1)(A)-(D)). If they did, the government had 90 days to comply with the request or initiate a judicial forfeiture action (§ 983(a)(3)(A)).

In April 2011, a public service announcement was launched linked to the banner of forfeited sites that had a video aimed to educate visitors of the site about criminal consequences of trafficking in counterfeit goods and the economic impact of that on the US and the global economy.¹⁶⁷⁹

Two notable examples and their aftermath

Property was seized (*in rem*) without prior notice and without an opportunity for the party that originally owned the seized property to contest the original seizure (*ex parte*).¹⁶⁸⁰ This caused some controversy, because the ICE agents and DOJ attorneys only needed to show the magistrate judge probable cause to get a seizure warrant. The controversy was whether this could hamper due process rights. After establishing probable cause, warrants were served to the domestic domain name registries that would then have to redirect traffic from the website to a page displaying a banner saying the site had been seized under federal law.¹⁶⁸¹

This process became frontpage news when two sites, Dajaz1 and Rojadirecta, challenged the seizures. They were the only challenging sites, and their challenges questioned the constitutionality of the process, when they showed the struggles these websites faced in getting their domains back.

Dajaz1.com was a popular hip-hop blog, registered with Verisign. It was seized in November 2011 because it provided links to four copyrighted songs. But apart from being a linking site, it was also a blog and place for people to discuss their favorite artists. After seizure, it was later revealed that the supposedly infringing songs were sent to Dajaz1 by the rights holders for promotion, prompting the government to return the domain name after more than a year.

The other website, Rojadirecta, was a Spanish sports website, owned by Puerto 80, registered with the American company GoDaddy.com, Inc. A large part of the Rojadirecta site consisted of streams of sporting events, posted by users.¹⁶⁸² At the time of the seizure, its legality in the EU was not clear. The EU Court of Justice since held that there was no copyright infringement so according to Mark Lemley, who represented Rojadirecta, it seemed clear that this particular streaming activity was legal in Europe.¹⁶⁸³

The government eventually withdrew both cases, and the domains were given back. The Electronic Frontier Foundation filed a few amicus briefs, to get the court to decide on whether the takedowns violated first amendment rights, and to have the record unsealed in the case of Dajaz1 to see what had happened during the investigation. But because the government withdrew their case, there never was a ruling on the merits of the copyright claims and the constitutionality of the seizures.

For example, it was not clear whether linking sites were liable for criminal copyright infringement under 17 U.S.C. §506.¹⁶⁸⁴ Dajaz1 lawyer Andrew Bridges also said that forfeiture laws should not apply to streaming sites, as they did not traffic articles, but consisted of transmissions.¹⁶⁸⁵

¹⁶⁷⁸ Kopel, "Operation Seizing Our Sites," P.876.

¹⁶⁷⁹ "ICE, European partners seize 328 Internet domains selling counterfeit goods in coordinated operation," News release, U.S. Immigration and Customs Enforcement (June 26, 2013), <https://www.ice.gov/news/releases/ice-european-partners-seize-328-Internet-domains-selling-counterfeit-goods-coordinated>

¹⁶⁸⁰ Kopel, "Operation Seizing Our Sites," P.860.

¹⁶⁸¹ Kopel, "Operation Seizing Our Sites," P.861.

¹⁶⁸² Ann Chaitovitz et al., "Responding to Online Piracy: Mapping the Legal and Policy Boundaries," 20 *COMmLAW CONSPECTUS* 1, 7 (2011). P.13.

¹⁶⁸³ Mark Lemley (Professor at Stanford Law School), interviewed by author, September 2013

¹⁶⁸⁴ Kopel, "Operation Seizing Our Sites," P.893.

In the case of Dajaz1, the unsealed records suggested that the site was locked down, and its seizure and the investigation kept a secret because the government was waiting for information from the RIAA.¹⁶⁸⁶ Corynne McSherry called this “frustrating”, because “people were trying to do the right thing, and the government doesn’t help.”¹⁶⁸⁷

One of the difficulties in the Dajaz1 case was that the extensions of the seizures were kept secret. Steven Welk, an L.A. attorney that represented the government after the seizure proceeding said that if the government was still doing an active investigation and the deadline was about to pass, they could apply to court with an under seal filing, making extension secret.¹⁶⁸⁸

After some criticism, the ICE director named other options for appeal: a website owner could choose to write a letter to ICE to return the property. If they did not return the property within 15 days, they could petition the U.S. District Court that issued the seizure warrant. They could also choose to file a challenge with the law enforcement agency conducting forfeiture action under administrative processes.¹⁶⁸⁹

Some argue that this did not work out in practice. They said government officials use intimidation tactics to file charges or stall their requests to convince those parties not to file claims.¹⁶⁹⁰

11.4 Scale, severity and procedural safeguards

Scale

Since its start in June, 2010, ‘Operation In Our Sites’ had been affiliated with the seizure of 2.550 websites (by December 2013, so after three and a half years).¹⁶⁹¹ While some proceedings were still pending, in June 2013, of the then 2.252 domain names seized, 1.624 had been forfeited by the US government.¹⁶⁹² In 2014, ICE revealed that since 2010, they had seized over 2700 domain names, and that some proceedings had led to convictions as well. “Collaboration through the IPR Center led to 692 arrests, 401 criminal indictments, and 451 criminal convictions for criminal IPR infringement activities in FY 2013.”¹⁶⁹³

Kopel presented a nice overview of the different phases of the operation until the end of 2012.¹⁶⁹⁴ Further phases were found on the ice website. www.ice.gov had news releases that

¹⁶⁸⁵ Andrew Bridges (Lawyer at Fenwick & West LLP), interviewed by author, September 2013.

¹⁶⁸⁶ Corynne McSherry (Intellectual Property Director Electronic Frontier Foundation) interviewed by author, September 2013

¹⁶⁸⁷ Corynne McSherry (Intellectual Property Director Electronic Frontier Foundation) interviewed by author, September 2013

¹⁶⁸⁸ Steven Welk (USACAC), interviewed by author, October 2013.

¹⁶⁸⁹ Kopel, “Operation Seizing Our Sites,” P.877. AND: Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part II: Hearings Before the H. Subcomm. on Intellectual Property, Competition, and the Internet, 112th Cong.117 (2011) (statement of John Morton, Director, ICE).

¹⁶⁹⁰ Kopel, “Operation Seizing Our Sites,” P.877.

¹⁶⁹¹ “ICE, international law enforcement agencies seize 706 domain names selling counterfeit merchandise,” News release, *U.S. Immigration and Customs Enforcement* (Dec 2, 2013).

<https://www.ice.gov/news/releases/ice-international-law-enforcement-agencies-seize-706-domain-names-selling-counterfeit>

¹⁶⁹² “ICE, European partners seize 328 Internet domains selling counterfeit goods in coordinated operation,” News release, *U.S. Immigration and Customs Enforcement* (June 26, 2013),

<https://www.ice.gov/news/releases/ice-european-partners-seize-328-Internet-domains-selling-counterfeit-goods-coordinated>

¹⁶⁹³ “ICE, CBP announce year-end intellectual property seizure statistics,” *News release, U.S. Immigration and Customs Enforcement* (March 24, 2014), <https://www.ice.gov/news/releases/ice-cbp-announce-year-end-intellectual-property-seizure-statistics>

¹⁶⁹⁴ Kopel, “Operation Seizing Our Sites,” P.878-885.

detailed the different operations they had done thus far. The site also listed individual convictions as a result of these operations, or investigations connected to ICE. The websites seized were “selling allegedly counterfeit luxury goods, sports memorabilia, and pharmaceuticals, to websites that hosted copyrighted music, movies, TV shows, software, and websites that only linked to this content.”¹⁶⁹⁵

- June 30, 2010: seizure of nine domain names and confiscation of \$84,000.¹⁶⁹⁶ This phase mainly targeted domain names allegedly involved in the illegal online distribution of movies and television shows. Among them were the popular NinjaVideo.net, and TVshack.net, a popular linking site run by Richard O’Dwyer. The latter was considered controversial because O’Dwyer was a twenty four year old college student from England, who would later face possible extradition to the US.
- November 2010: Cyber Monday Crackdown. 82 websites closed. Mostly aimed at online retailers of counterfeit goods, but also Dajaz1.com, a popular hip-hop blog.¹⁶⁹⁷
- February 1, 2011: ten domain names seized. Mostly related to sporting events, which coincided with the NFL 2011 Super Bowl. Also shut down two websites on Rojadirecta domain name, which had been declared legal by Spanish Court.¹⁶⁹⁸
- Valentine’s Day 2011 – operation broken hearted: 18 domain names allegedly selling luxury counterfeit goods seized (like Louis Vuitton).¹⁶⁹⁹
- May 2011: five domain names seized, including two for pirated content.
- July 2011, operation Shoe Clerk: aimed at selling fake goods, like face Gucci.
- October 2011: operation strike out: Coincided with Baseball World Series, after month long investigation, aimed at allegedly counterfeit sports memorabilia. 58 domain names seized.
- November 28, 2011: Second cyber Monday initiative. 152 websites seized selling allegedly counterfeit merchandise.¹⁷⁰⁰
- December 4, 2011: seizure of twelve domain names, selling allegedly pirated copies of video content, and software.
- October 2011 – February 2012: Operation Fake Sweep. Leading up to Super Bowl. Seizure of 307 domain names, of which 291 selling allegedly counterfeit game-related sportswear, and 16 allegedly illegal streaming of sports.¹⁷⁰¹
- May 11, 2012: seizure of money mostly.¹⁷⁰²

¹⁶⁹⁵ Kopel, “Operation Seizing Our Sites,” P.860, And: “Press Release – Operation in Our Sites,” *National Intellectual Property Rights Coordination Center*, www.iprcenter.gov/reports/fact-sheets/operation-in-our-sites/view

¹⁶⁹⁶ “Operation In Our Sites” Targets Internet Movie Pirates, ICE, Manhattan U.S. Attorney Seize Multiple Web Sites for Criminal Copyright Violations”, News Release, *U.S. Immigration and Customs Enforcement*, (June 30, 2010), available at <https://www.ice.gov/news/releases/1006/100630losangeles.htm>

¹⁶⁹⁷ “ICE Seizes 82 Website Domains Involved In Selling Counterfeit Goods As Part of Cyber Monday Crackdown,” News Release, *U.S. Immigration and Customs Enforcement* (Nov. 29, 2010), available at <https://www.ice.gov/news/releases/1011/101129washington.htm>

¹⁶⁹⁸ “New York Investigators Seize 10 Websites That Illegally Streamed Copyrighted Sporting and Pay-per-view Events,” News Release, *U.S. Immigration and Customs Enforcement* (Feb. 2, 2011), available at <http://www.ice.gov/news/releases/1102/110202newyork.htm>

¹⁶⁹⁹ “Sweetheart, But Fake, Deals Put On ICE “Operation Broken Hearted” Protects Consumers From Counterfeit Valentine’s Day Goods,” News Release, *U.S. Immigration and Customs Enforcement* (Feb. 14, 2011), available at <https://www.ice.gov/news/releases/1102/110214washingtondc.htm>

¹⁷⁰⁰ “Operation In Our Sites Protects American Online Shoppers, Cracks Down on Counterfeiters,” News Release, *U.S. Immigration and Customs Enforcement* (Nov. 28, 2011), available at <https://www.ice.gov/news/releases/1111/111128washingtondc.htm>

¹⁷⁰¹ “Special Agents and Officers Seize More Than \$4.8 Million in Fake NFL Merchandise and Seize 307 Websites During ‘Operation Fake Sweep,” News Release, *U.S. Immigration and Customs Enforcement* (Feb. 2, 2012), available at <https://www.ice.gov/news/releases/1202/120202indianapolis.htm>

Afterwards there was no referral to separate phases. However, some new projects were launched:

- July 2012: Project copy cat: seventy domain names, allegedly counterfeit goods.¹⁷⁰³
- August 2012: Seizing three domain names selling apps allegedly illegally.¹⁷⁰⁴
- October 2012: Project Bitter Pill. Seizures of 686 websites selling allegedly illegal counterfeit pharmaceuticals.¹⁷⁰⁵
- November 2012: 101 domain names selling allegedly counterfeit merchandise online¹⁷⁰⁶
- December 2012: 89 websites also allegedly selling counterfeit merchandise online.¹⁷⁰⁷
- January 2013: Operation Red Zone, 313 websites seized for selling counterfeit NFL merchandise.¹⁷⁰⁸
- April 2013: 10 Internet domain names seized that were illegally selling counterfeit cycling equipment and apparel globally.¹⁷⁰⁹
- June 2013: Two operations in cooperation with enforcement agencies in Europe. The US side: Project American Icons, seized 177 domain names selling counterfeit trademark merchandise manufactured by American-owned companies.¹⁷¹⁰
- December 2013: project cyber Monday iv, ICE worked with international law enforcement agencies to seize hundreds of domain names selling counterfeit merchandise online, of which 297 were connected to the US.¹⁷¹¹

The above cited phases show that most of the operation aimed for trademark crime and intended to stop the trade in counterfeit goods.

¹⁷⁰² "Department of Justice Seizes More Than \$1.5 Million in Proceeds from the Online Sale of Counterfeit Sports Apparel Manufactured in China," News Release, U.S. Immigration and Customs Enforcement (May 11, 2012), available at <http://www.justice.gov/opa/pr/2012/May/12-crm-610.html>

¹⁷⁰³ "ICE-Led IPR Center Seizes 70 Websites Duping Consumers Into Buying Counterfeit Merchandise," News Release, U.S. Immigration and Customs Enforcement (July 12, 2012), available at <https://www.ice.gov/news/releases/1207/120712washington.htm>

¹⁷⁰⁴ "Federal Courts Order Seizure of Three Website Domains Involved in Distributing Pirated Android Cell Phone Apps," Press Release, U.S. Department of Justice, (Aug. 21, 2012), available at <http://www.justice.gov/opa/pr/2012/August/12-crm-1033.html>

¹⁷⁰⁵ "HIS Seizes 686 Websites Selling Counterfeit Medicine to Unsuspecting Consumers," News Release, U.S. Immigration and Customs Enforcement (Oct. 4, 2012), available at <https://www.ice.gov/news/releases/1210/121004washingtondc.htm>

¹⁷⁰⁶ "European Law Enforcement Agencies and Europol Seize 132 Domain Names Selling Counterfeit Merchandise in 'Project Cyber Monday 3' and 'Project Transatlantic Operations'," News Release, U.S. Immigration and Customs Enforcement (Nov. 26, 2012), available at <http://www.ice.gov/news/releases/1211/121126washingtondc.htm>

¹⁷⁰⁷ "Houston HIS Seizes 89 Websites Selling Counterfeit Goods," News Release, U.S. Immigration and Customs Enforcement (Dec. 20, 2012), available at <https://www.ice.gov/news/releases/1212/121220houston.htm>

¹⁷⁰⁸ "ICE, CBP, USPIIS seize more than \$13.6 million in fake NFL merchandise during 'Operation Red Zone'," News Release, U.S. Immigration and Customs Enforcement (Jan 31, 2013) <https://www.ice.gov/news/releases/1301/130131neworleans.htm>

¹⁷⁰⁹ "Houston HSI seizes 10 domain names selling counterfeit cycling products," News Release, U.S. Immigration and Customs Enforcement (April 29, 2013), <https://www.ice.gov/news/releases/1304/130429houston.htm>

¹⁷¹⁰ "ICE, international law enforcement agencies seize 706 domain names selling counterfeit merchandise," News release, U.S. Immigration and Customs Enforcement (Dec 2, 2013), <https://www.ice.gov/news/releases/ice-international-law-enforcement-agencies-seize-706-domain-names-selling-counterfeit>

¹⁷¹¹ "ICE, European partners seize 328 Internet domains selling counterfeit goods in coordinated operation," News release, U.S. Immigration and Customs Enforcement (June 26, 2013), <https://www.ice.gov/news/releases/ice-european-partners-seize-328-Internet-domains-selling-counterfeit-goods-coordinated>

Severity

This operation was divided into two phases: the initial seizure and the eventual trial.

With its operation, ICE targeted websites, instead of targeting specific instances of infringement (which would be the case when the DMCA takedown provisions were applied).¹⁷¹² Apart from the seizures of the websites, assets were also seized.¹⁷¹³

Some were worried that this procedure allowed for the removal of entire websites. Those websites also contained other expressions. According to the lawyer of Dajaz1, it contained “legitimate, lawful speech, including conversations from chat rooms, posts in discussion forums and blogs.”¹⁷¹⁴ This applied especially when different individuals author different parts of the websites.¹⁷¹⁵ Seizing them also took away the opportunity for people to access websites.¹⁷¹⁶ The lawyer of Dajaz1 also contested the merits of the seizure. He compared it to the seizure of a New York Times printing press, where on the page of the concert list, a promoter had listed advertisements for four illegal ones, without paying promotion costs.¹⁷¹⁷

Others expressed concern that the seizures were enough of a sanction in themselves. Some commentators argued that only the seizing seemed to be the purpose, and not the actual forfeiture.¹⁷¹⁸ Congress members expressed their concern that the seizures were a means to an end to get rid of websites that might have prevailed in court. This applied especially to linking websites. They also feared increased chances of improper seizure: over-breadth issues could not come to light. Some people have therefore called it over-aggressive action.¹⁷¹⁹ In my interviews, Dajaz1 lawyer Andrew Bridges said that sanctioning without a trial seemed part of the aim.¹⁷²⁰ Steven Welk, on the government side said: “that’s certainly the way they see it,” referring to the defending parties.¹⁷²¹

Although the seizures were temporary, they lasted long enough to do damage. My interviews gave some perspective on the personal impact they had. The Rojadirecta domain was given back 18 months after it was seized. Their lawyer called it “frustrating” that they did not get a final legal decision from either court on the merits of the copyright claim, or on the constitutionality of the procedure. Also, because the seizure ended unilaterally, Rojadirecta was unable to recover attorney’s fees.¹⁷²² Although Lemley did not want to comment on his client’s personal situation, he said there certainly were consequences for the website. Although it did not shut down and continued to serve customers, definitely a substantial fraction of its traffic disappeared.¹⁷²³

Meanwhile, Dajaz1 also experienced a loss in traffic (“a dramatic drop off from which it will never recover completely”), so there was some reason to believe they lost money. A Hip Hop related blog filled its void, and took off substantially. When the site was returned, Bridges said: “that

¹⁷¹² Michael J. Harrell, “Fighting Piracy with Censorship: The Operation in Our Sites Domain Seizures v. Free Speech,” 21 *Journal of Intellectual Property Law* 137 (2013). P.141.

¹⁷¹³ “ICE, CBP, USFIS seize more than \$13.6 million in fake NFL merchandise during ‘Operation Red Zone,’” News Release, U.S. Immigration and Customs Enforcement (Jan 31, 2013) <https://www.ice.gov/news/releases/1301/130131neworleans.htm>

¹⁷¹⁴ Kopel, “Operation Seizing Our Sites,” P.888-889.

¹⁷¹⁵ Kopel, “Operation Seizing Our Sites,” P.890.

¹⁷¹⁶ Kopel, “Operation Seizing Our Sites,” P.890.

¹⁷¹⁷ Andrew Bridges (Lawyer at Fenwick & West LLP), interviewed by author, September 2013.

¹⁷¹⁸ Kopel, “Operation Seizing Our Sites,” P.867, and: “DOJ/FBI Seize Domain Names by Warrant,” *Tech Law Journal* (August 21, 2012), <http://www.techlawjournal.com/topstories/2012/home.asp>.

¹⁷¹⁹ Letter from Ron Wyden, U.S. Senator, to Eric Holder, U.S. Attorney Gen., & to John Martin, Dir., U.S. Immigration & Customs Enforcement (Feb. 2, 2011), available at <http://www.wyden.senate.gov/download/?id=103d77C-6f30-469b-ab98-8bbfdd4>, and: Kopel, “Operation Seizing Our Sites,” P.887-888.

¹⁷²⁰ Andrew Bridges (Lawyer at Fenwick & West LLP), interviewed by author, September 2013

¹⁷²¹ Steven Welk (USACAC), interviewed by author, October 2013.

¹⁷²² Mark Lemley (Professor at Stanford Law School), interviewed by author, September 2013.

¹⁷²³ Mark Lemley (Professor at Stanford Law School), interviewed by author, September 2013.

exoneration, however, did not remedy the harms caused by a full year of censorship and secret proceedings — a form of “digital Guantanamo” — that knocked out an important and popular blog devoted to hip hop music and has nearly killed it.”

Another problem was that the domain was not renewed and expired during the seizure. When the client tried to renew it, the registrar refused as they had no control over it. This was potentially risky, because “bots can snatch those domains.” Eventually, Dajaz1 was able to get the domain back.¹⁷²⁴

Sanctions went further than seizures and led to arrests and convictions as well. These convictions could be severe. For example, the leader of Internet piracy group “IMAGiNE”, responsible for the release of numerous copyright protected movies onto the web, was sentenced to 60 months in prison for a “criminal copyright conspiracy.”¹⁷²⁵ One of the founders of Ninjavidio, a website that contained links to uploaded videos of TV shows, movies and documentaries, spent 16 months in prison. Another founder spent 6 months in prison.¹⁷²⁶ 24 year old UK citizen Richard O Dwyer, owner and creator of the website TVshack, an indexing site that allowed visitors to find links to copyright protected content, was extradited to the U.S. and avoided a ten-year jail sentence by signing an agreement to pay back profits made with the website.¹⁷²⁷

Safeguards

Privacy

Whether or not this enforcement strategy interfered with privacy rights, depended on whether personal data was processed. This usually happens when infringement is found, and when enforcing parties have access to personal data.

This strategy first aimed for the websites, but could target the people affiliated with the website. Personal data would only be processed as part of the criminal investigation, conducted by ICE agents. This required the approval of a magistrate judge.

Impartial, competent and independent judge

During the investigation, the department of homeland security and its special agent researched whether or not there is infringement of copyright with the help of representatives of rights holders, such as the RIAA or the MPAA. They then presented an affidavit to a neutral federal magistrate judge who would determine whether probable cause had been established.¹⁷²⁸ If it had, the judge would grant an order for the domains to be seized.¹⁷²⁹ These magistrate judges fulfilled the requirement of impartiality, competency and independence. As Steven Welk told me, the government could not just “act on their own.”¹⁷³⁰

¹⁷²⁴ Andrew Bridges (Lawyer at Fenwick & West LLP), interviewed by author, September 2013.

¹⁷²⁵ “Leader of Internet piracy group “IMAGiNE” sentenced in Virginia to 60 months in prison for criminal copyright conspiracy,” News Release, *U.S. Immigration and Customs Enforcement* (Jan 3, 2013), <https://www.ice.gov/news/releases/1301/130103washingtondc2.htm>

¹⁷²⁶ Jenna Wortham, “The Unrepentant Bootlegger,” *The New York Times* (Set. 27, 2014), <http://www.nytimes.com/2014/09/28/technology/the-unrepentant-bootlegger.html>

¹⁷²⁷ Adam Gabbatt and Owen Bowcott, “Richard O’Dwyer’s two-year extradition ordeal ends in New York,” *the Guardian* (December 7, 2012), <https://www.theguardian.com/uk/2012/dec/06/richard-o-dwyer-avoids-us-extradition>

¹⁷²⁸ U.S.C. § 981(b)(2) (2006).

¹⁷²⁹ Federal Rules of Criminal Procedure 41 (d)(1)-(2).

¹⁷³⁰ Steven Welk (USACAC), interviewed by author, October 2013.

However, the lawyers of Dajaz1 and Rojadirecta did suggest that the push back by magistrate judges was not as hard as it would have been in an open court. Dajaz1 lawyer Andrew Bridges said that the process for establishing probable cause was problematic, because the “sad reality” was that US attorneys had a “great deal of credibility” and magistrate judges many times “don’t push back hard enough.” Federal judges in turn (as in the actual forfeiture proceedings) did, because it was a public forum.¹⁷³¹ Mark Lemley confirmed that a Magistrate Judge “rubber stamps” such requests, and that it was rare for them not to issue a warrant.¹⁷³² It was difficult for me to verify this. The (perceived lack of) neutrality of magistrate judges was beyond the scope of this research.

Some cases did end up in court, either for forfeiture proceedings or trial against the people associated with the website. I had no reason to doubt the impartiality, competence or independence of those judges.

Presumption of innocence

Although the burden of proof for forfeiture was on the government as would be the case in the eventual trial against a person, the seizures themselves were subject to lower standards of evidence.

18 U.S.C. Section 981 provided that the U.S. government could only seize property after it obtained a seizure warrant in compliance with the Federal Rules of Criminal Procedure.¹⁷³³ In order to obtain a seizure warrant, government officials had to submit a sworn testimony or affidavit to a judge establishing probable cause.¹⁷³⁴

If the magistrate judge approved, law enforcement agencies could gain immediate possession of the property before definite resolution of the action in court. Because these seizures were civil actions there lower burdens of proof, such as probable cause, were enough to establish the forfeiture. The government would only have to demonstrate that they believed the property was in some way connected with an underlying criminal offense.¹⁷³⁵

In other words, the government had to demonstrate probable cause that a violation of 17 U.S.C. § 506 (criminal copyright) had taken place. The Pro IP act added provisions in the US copyright law that allowed for the seizure of property used, or intended to be used, in any manner or part to commit or facilitate the commission of criminal copyright infringement (at 18 U.S.C. § 2323). “Intended to be used” for this violation was a very low threshold to meet.

In other words, the burden of proof to establish infringement lay with the government side supported by rights holders. However, to only show probable cause was a lower standard to meet. Many commentators have argued that the sanction was heavy in comparison to the standards of evidence required.¹⁷³⁶ This will resurface in the section on proportionality.

Steven Welk, involved in the post-seizure procedure against Dajaz1 on the government side, said that the standards of evidence in the actual forfeiture trial would be much higher. “That’s why you get a 90 day period to decide if it’s worthwhile.”¹⁷³⁷

¹⁷³¹ Andrew Bridges (Lawyer at Fenwick & West LLP), interviewed by author, September 2013.

¹⁷³² Mark Lemley (Professor at Stanford Law School), interviewed by author, September 2013.

¹⁷³³ U.S.C. § 981(b)(2) (2006).

¹⁷³⁴ Federal Rules of Criminal Procedure 41 (d)(1)-(2).

¹⁷³⁵ Michael J. Harrell, “Fighting Piracy with Censorship: The Operation in Our Sites Domain Seizures v. Free Speech,” 21 *Journal of Intellectual Property Law* 137 (2013). P.146.

¹⁷³⁶ Kopel, “Operation Seizing Our Sites,” P.864, and: Robert Lieske, “Civil Forfeiture Law: Replacing the Common Law with a Common Sense Application of the Excessive Fines Clause of the Eighth Amendment,” *WM. MITCHELL L. REV.* 21 (1995): 265. P.271.

¹⁷³⁷ Steven Welk (USACAC), interviewed by author, October 2013.

To find evidence, the government closely worked with certain private entities. Before the seizure of Dajaz1, the affidavit described that the ICE agent responsible had discussions with Carlos Linares, VP of Anti-Piracy Legal Affairs for the RIAA, and that he relied on this information to claim that four songs were in pre-release and therefore not authorized for distribution.¹⁷³⁸ In the case of Rojadirecta, the seizure was part of a larger operation aimed at various sports-related sites at the behest of the National Football League in the week of the Superbowl. According to Rojadirecta's lawyer: the "league said: this is a site where people will or are likely to post streams of the Superbowl, so US government I want you to take it down."¹⁷³⁹

Some have been critical of this cooperation. In the case of Dajaz1, ICE worked with the RIAA, who provided them with information about the rights belonging to the copyright holders and what they were licensing with their product. For the potential civil forfeiture trial, the RIAA was conducting an investigation.¹⁷⁴⁰ According to Andrew Bridges, this made it clear that the declaration was reliant on third hand information, and "hearsay."¹⁷⁴¹ In the declaration, according to Bridges, ICE tried to "lump sites together, making them sound corrupt" and made broad allegations about Dajaz1 to make it sound like a corrupt or bad faith site, even though the seizure is about four specific alleged infringements.¹⁷⁴²

However, according to Steven Welk, working together with private organizations was common in the tech area. In the copyright field for example, the government often worked with private organizations that watched over those rights and protected them.¹⁷⁴³

Some interviewees said that the impact of such a seizure or government pressure presented an additional burden for those pursued. It created additional emotional pressure, they said. "Many people don't want to be prosecuted, even when they are innocent," Bridges said, and "there is a regular viewpoint that says -don't anger the government and stay quiet-." "Those that do the seizures like to say how little seizures are challenged. But the fail to take into account there are many reasons to not challenge," he said.¹⁷⁴⁴

Meanwhile, the burden on the government was relatively low. According to Corynne McSherry of the Electronic Frontier Foundation it was difficult for the government to lose. They could seize sites and then see if someone complains.¹⁷⁴⁵ "Our legal regime has made it very easy to do this." They could just drop the case when they wanted to, according to McSherry, which was why the EFF aimed to make the process "more fair."¹⁷⁴⁶

Notice, right to be heard (prior to conviction), defenses and appeal

The process was an *in rem ex parte* forfeiture, which did not allow for any prior notice,¹⁷⁴⁷ and gave no chance for defense in a hearing prior to the seizure.

The seizure would take place without notice. The government had to send written notice to the website owner afterwards: within sixty days of seizure. They could also choose

¹⁷³⁸ Dajaz1 Affidavit, 56, see at: "In the Matter of the Seizure of the Internet Domain Name "Dajaz1.com"", Electronic Frontier Foundation, <https://www.eff.org/nl/cases/matter-seizure-internet-domain-name-dajaz1com>

¹⁷³⁹ Mark Lemley (Professor at Stanford Law School), interviewed by author, September 2013.

¹⁷⁴⁰ Steven Welk (USACAC), interviewed by author, October 2013.

¹⁷⁴¹ Andrew Bridges (Lawyer at Fenwick & West LLP), interviewed by author, September 2013.

¹⁷⁴² Andrew Bridges (Lawyer at Fenwick & West LLP), interviewed by author, September 2013.

¹⁷⁴³ Steven Welk (USACAC), interviewed by author, October 2013.

¹⁷⁴⁴ Andrew Bridges (Lawyer at Fenwick & West LLP), interviewed by author, September 2013.

¹⁷⁴⁵ Corynne McSherry (Intellectual Property Director Electronic Frontier Foundation) interviewed by author, September 2013.

¹⁷⁴⁶ Corynne McSherry (Intellectual Property Director Electronic Frontier Foundation) interviewed by author, September 2013.

¹⁷⁴⁷ Kopel, "Operation Seizing Our Sites," P.885.

to file a judicial forfeiture action against the property and provide notice of that to the interested parties.¹⁷⁴⁸ This deadline could be extended if the government could show there was reason to believe that the provision of a notice would have an adverse effect on the proceedings.¹⁷⁴⁹ This left the door open to a very late notice. Some commentators have asked that there at least should be notice within a more reasonable time.¹⁷⁵⁰

As mentioned in a previous section, only after notice, the website owner (or any other interested party) would be allowed to file a claim with the agency within a deadline set in the written forfeiture notice. As a result the government had to file a complaint for forfeiture within ninety days of filing the claim, or return the property.¹⁷⁵¹ If website owners or interested parties did file a complaint, they had to show that not having the property would cause substantial hardship.¹⁷⁵² If they did, the government had 90 days to comply with the request or initiate a judicial forfeiture action.¹⁷⁵³

Some argued that this did not work out in practice. Some said government officials used intimidation tactics to file charges or stall their requests to convince those parties not to file claims.¹⁷⁵⁴

Seizure took place before an adversarial hearing had happened. Some authors say not providing notice and hearing violated due process.¹⁷⁵⁵ Some members of congress were concerned that in the light of the debates on the enforcement of copyrights, the operation could be used by law enforcement to take down websites as a means to an end, effectively removing websites that may have prevailed in formal proceedings.¹⁷⁵⁶

In a congressional hearing on 'Operation In Our Sites,' director John Morton said that "Domain names seized under 'Operation In Our Sites' are seized only in furtherance of ongoing criminal investigations into violations of U.S. federal laws. . . . For each domain name seized, ICE investigators independently obtained counterfeit trademarked goods or pirated copyrighted material that was in turn verified by the rights holders as counterfeit. After such verification, ICE applied for federal seizure warrants based on probable cause. Federal magistrate judges approve criminal seizure warrants based on probable cause for the domain names that are targeted. The standard is exactly the same as in any other criminal investigation. As with all judicially authorized seizure warrants, the owners of the seized property have the opportunity to challenge the judge's determination through a petition." They in other words argued that similarly, law enforcement would not notify criminals if they were being investigated for crimes.¹⁷⁵⁷ However, this investigation could be viewed as a sanction in itself.

The interviewees demonstrated the impact not being notified had in practice. As mentioned before, the lack of a notice before seizure and the fact that parties were not heard prior to seizure was one of the most pressing points of criticism of this procedure. For

¹⁷⁴⁸ 18 U.S.C. § 983(a)(1)(A)(i)-(ii)

¹⁷⁴⁹ § 983(a)(1)(C)-(D)

¹⁷⁵⁰ Michael J. Harrell, "Fighting Piracy with Censorship: The Operation in Our Sites Domain Seizures v. Free Speech," 21 *Journal of Intellectual Property Law* 137 (2013). P.148.

¹⁷⁵¹ 18 U.S.C. § 983(a)(2) and (3)

¹⁷⁵² § 983(f)(1)(A)-(D)

¹⁷⁵³ § 983(a)(3)(A)

¹⁷⁵⁴ Kopel, "Operation Seizing Our Sites," P.877.

¹⁷⁵⁵ Douglas Kim, "Asset Fofeiture: Giving Up Your Constitutional Rights," 19 *CAMPBELL L. REV.* 527, 565 (1997)

¹⁷⁵⁶ Letter from Ron Wyden, U.S. Senator, to Eric Holder, U.S. Attorney Gen., & to John Martin, Dir., U.S. Immigration & Customs Enforcement (Feb. 2, 2011), available at <http://www.wyden.senate.gov/download/?id=103d77C-6f30-469b-ab98-8bbfdd4>

¹⁷⁵⁷ "Statement of John Morton, Director of U.S. Immigration and Customs Enforcement, Department of Homeland Security," Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part II: Hearing Before the H. Comm. on the Judiciary, Subcomm. on Intellectual Property, Competition, and the Internet, 112th Cong. 11-12 (2011) (), <http://commcns.org/t38zzN>

Dajaz1, this meant that “one day,” the owner of the website “discovered” it was out of his control. When he went to the website, he saw the emblem of the DOJ and DHS, which advised the world that the domain had been seized.¹⁷⁵⁸ “That’s all he knows for months.” According to Bridges, he could not determine what exactly was happening until he saw a press release from ‘Operation In Our Sites.’¹⁷⁵⁹

The government had two months to send a mail notice of seizure. In the case of Dajaz1 they took nearly the full 60 days to send out this notice. According to Bridges “that’s like police coming and towing your car and then waiting two months to send the parking ticket.”¹⁷⁶⁰

In the case of Rojadirecta, attorney Lemley recounted that in January 2011, the site “suddenly disappeared (.com and .org),” and was routed to the department of justice webpage. When they tried contacting the government, they had a “difficult time” finding “anyone in the government who could talk to us and take responsibility.” They talked to the ICE agent whose name was on the warrant and “he referred us to the US attorney’s office”, so they talked to the lawyer whose name was on the warrant, but he “didn’t know anything either.” Lemley said “we weren’t served with a complaint, we weren’t given any information, we weren’t allowed to contest it, it was just gone.” Lemley said they tried ICE, the white house IP enforcement coordinator, whether they could say anything. He said they could not get anybody to talk to them until they sent a notice saying they were going to file a lawsuit challenging it. After this they got a call back from the US attorney’s office “saying wait I think we can work this out,” so they talked to them over a period of three to four months.¹⁷⁶¹

There were some options to challenge a seizure such as this. The owner of the seized property could within 35 days claim their seized property, in which case the government had to prove that the seizure was correct and in which case the owner asked ICE to refer the case to the US attorney’s office to file a forfeiture lawsuit. Then the government had 90 days to file a forfeiture lawsuit. For that, “all they have to do” was file a bare bones complaint, according to Bridges, saying “this is the action, this file breaks the law, this is the law it violates and we want forfeiture.”¹⁷⁶²

In the case of Rojadirecta, from the contacts they had with the government, it seemed “they offered the possibility to get the domain back.” But later “it became clear they weren’t going to do that.” So they filed a lawsuit challenging the seizure as unconstitutional under the First Amendment of the U.S. Constitution and filed a lawsuit to ask for the property back saying it was seized in error.¹⁷⁶³ The latter request was denied by the district judge because (several months after seizure) the government had finally filed a forfeiture complaint. The district judge therefore wanted to wait for that decision. So Lemley decided to appeal that decision in the Second Circuit.¹⁷⁶⁴ They meanwhile filed a motion to dismiss the government complaint, which was granted by the court but with leave to amend. But then the government amended that complaint which Lemley in turn filed to dismiss. So then they were waiting for their hearing (eight months after seizure) when suddenly the domain was returned.¹⁷⁶⁵

After some criticism because of what had happened with these two websites, the ICE director named other options for appeal: a website owner could choose to write a letter to ICE to return the property. If they did not return the property within 15 days, they could petition the U.S.

¹⁷⁵⁸ Andrew Bridges (Lawyer at Fenwick & West LLP), interviewed by author, September 2013.

¹⁷⁵⁹ Andrew Bridges (Lawyer at Fenwick & West LLP), interviewed by author, September 2013.

¹⁷⁶⁰ Andrew Bridges (Lawyer at Fenwick & West LLP), interviewed by author, September 2013.

¹⁷⁶¹ Mark Lemley (Professor at Stanford Law School), interviewed by author, September 2013.

¹⁷⁶² Andrew Bridges (Lawyer at Fenwick & West LLP), interviewed by author, September 2013.

¹⁷⁶³ Mark Lemley (Professor at Stanford Law School), interviewed by author, September 2013.

¹⁷⁶⁴ Mark Lemley (Professor at Stanford Law School), interviewed by author, September 2013.

¹⁷⁶⁵ Mark Lemley (Professor at Stanford Law School), interviewed by author, September 2013.

District Court that issued the seizure warrant. They could also choose to file a challenge with the law enforcement agency conducting forfeiture action under administrative processes.¹⁷⁶⁶

Bridges suggested that the government simply was not used to people challenging seizures, because it rarely happened, with good reason because in “theory” behind every seizure there was a criminal investigation.¹⁷⁶⁷

Also, the government did not have much to lose. Someone could theoretically argue constitutional violations to get back money,¹⁷⁶⁸ or an abuse of process claim. Both would be difficult.¹⁷⁶⁹

Transparency

Eventual cases would be transparent, as would be the investigation leading to the seizure, unless there were pressing reasons not to.

However, the two cases against Dajaz1 and Rojadirecta were intransparent. In the Dajaz1 case the deadline for filing a forfeiture suit came and went. “Nobody heard anything”, said Bridges. So they checked docket databases, but they could not find anything.¹⁷⁷⁰ So Bridges spoke to the chief of asset forfeiture in California, after talking to ICE, who at the time was Steven Welk, who informed him that there had been an extension. It was kept under seal (secret), by court order, which was kept secret too.¹⁷⁷¹ When Bridges asked to be further notified about extensions and that he wanted to oppose extensions, his request was denied. The first extension lasted 60 days. They did not know the judge granting the extension or the case number.¹⁷⁷² After that, the deadline went, and they found out there had been another extension, again secret. Not just the grounds for extension, but the fact that there had been an extension was kept from Dajaz1.¹⁷⁷³ A third sixty-day extension followed. Then suddenly they received an email saying “upon further investigation the domain will not be forfeited, we will return the domain in due course.”¹⁷⁷⁴

Afterwards, when the documents were unsealed (which was not contested by the government), they were able to look at the papers. “Apparently they were waiting for an RIAA investigation and after some time just gave up.” Bridges thought that there was no justification for this secrecy. This only applied, according to him, to big criminal cases, when “the government tries to put together a big investigation on eight people distributing cocaine, for example.”¹⁷⁷⁵ Or when they wanted to “protect complaining witnesses.” But it was unlikely that this protection was warranted for RIAA officials, he says. And it also was “not a good reason to keep the extension secret.” According to Bridges they were simply “implicitly conceding that they didn’t have enough information to justify filing a lawsuit.”¹⁷⁷⁶

Welk says that it was “potentially harmful to unseal those documents during an investigation.” He said “when the other side calls me, I will tell them that the government has

¹⁷⁶⁶ Kopel, “Operation Seizing Our Sites,” P.877, and: Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part II: Hearings Before the H. Subcomm. on Intellectual Property, Competition, and the Internet, 112th Cong.117 (2011) (statement of John Morton, Director, ICE)

¹⁷⁶⁷ Andrew Bridges (Lawyer at Fenwick & West LLP), interviewed by author, September 2013.

¹⁷⁶⁸ Andrew Bridges (Lawyer at Fenwick & West LLP), interviewed by author, September 2013.

¹⁷⁶⁹ Corynne McSherry (Intellectual Property Director Electronic Frontier Foundation) interviewed by author, September 2013.

¹⁷⁷⁰ Andrew Bridges (Lawyer at Fenwick & West LLP), interviewed by author, September 2013.

¹⁷⁷¹ Andrew Bridges (Lawyer at Fenwick & West LLP), interviewed by author, September 2013.

¹⁷⁷² Andrew Bridges (Lawyer at Fenwick & West LLP), interviewed by author, September 2013.

¹⁷⁷³ Andrew Bridges (Lawyer at Fenwick & West LLP), interviewed by author, September 2013.

¹⁷⁷⁴ Andrew Bridges (Lawyer at Fenwick & West LLP), interviewed by author, September 2013.

¹⁷⁷⁵ Andrew Bridges (Lawyer at Fenwick & West LLP), interviewed by author, September 2013.

¹⁷⁷⁶ Andrew Bridges (Lawyer at Fenwick & West LLP), interviewed by author, September 2013.

obtained the extension in an under seal filing. We will tell the case number. But they don't get to see the paperwork or reason."¹⁷⁷⁷

The Rojadirecta case gradually became more transparent, "merely because we took the initiative," Lemley says. Because they received no information, it was only when they filed a lawsuit that they got access to some information.¹⁷⁷⁸

In both the Dajaz1 and Rojadirecta case the lack of a trial was problematic because it was not clear how the law was applied.¹⁷⁷⁹

Proportionality

To be proportional, sanctions need to be necessary, suitable and not an unreasonable burden on individual rights. *Ex parte* proceedings were usually limited to extraordinary circumstances. Supporters said this was the case here: there was a public interest to prevent criminal activity, and it was also better to be swift to prevent owners to move them out of the jurisdictional reach of ICE. They also said seizure was only of the domain name, so there was less damage.¹⁷⁸⁰

Opponents said this effectively amounted to "prior restraint" of free speech which would almost never be granted in court, especially with probable cause.¹⁷⁸¹ Prior restraint was generally seen as a worse intrusion on free speech that therefore required more scrutinization.¹⁷⁸² Many commentators have argued that the sanction was heavy in comparison to the standards of evidence required.¹⁷⁸³

Congresswoman Zoe Lofgren, an opponent of 'Operation In Our Sites,' stated that "domain seizures without due process are a form of censorship. . . . While this might be enough for the seizure of stolen cars or knock-off handbags, it is not enough for websites and speech on the Internet."¹⁷⁸⁴ In a judicial hearing on the subject in congress, some (like the Center for Democracy & Technology) have argued that not having an adversarial hearing created risks of aggressive over enforcement because legal theories could not be checked.¹⁷⁸⁵

This over-enforcement was particularly troubling, because the enforcement action targeted complete domains, which included lawful content on other subdomains, instead of just the infringing pages. Many opponents of this procedure pointed to the seizure by ICE of the website moo.com. Although they targeted 10 websites that provided explicit child pornographic content, the seizure also led to the wrongful takedown of over 84,000 subdomains.¹⁷⁸⁶ They therefore argued that this amounted to prior restraint.

¹⁷⁷⁷ Steven Welk (USACAC), interviewed by author, October 2013.

¹⁷⁷⁸ Mark Lemley (Professor at Stanford Law School), interviewed by author, September 2013.

¹⁷⁷⁹ Corynne McSherry (Intellectual Property Director Electronic Frontier Foundation) interviewed by author, September 2013.

¹⁷⁸⁰ Kopel, "Operation Seizing Our Sites," P.886-887.

¹⁷⁸¹ Kopel, "Operation Seizing Our Sites," P.890.

¹⁷⁸² Michael J. Harrell, "Fighting Piracy with Censorship: The Operation in Our Sites Domain Seizures v. Free Speech," 21 *Journal of Intellectual Property Law* 137 (2013). P.148-149.

¹⁷⁸³ Robert Lieske, "Civil Forfeiture Law: Replacing the Common Law with a Common Sense Application of the Excessive Fines Clause of the Eighth Amendment," *WM. MITCHELL L. REV.* 21 (1995): 265. P.271.

¹⁷⁸⁴ Rep. Zoe Lofgren, Lofgren, Wyden Question Response to Seizure Inquiries, <http://commcns.org/tyiKZ>

¹⁷⁸⁵ Statement of David Sohn, Senior Policy Counsel, Center for Democracy & Technology, Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part I: Hearing Before the H. Comm. on the Judiciary, Subcomm. on Intellectual Property, Competition, and the Internet, 112th Cong. 6-9 (2011), <http://commcns.org/sCSXbA>

¹⁷⁸⁶ Thomas Claburn, "ICE Confirms Inadvertent Web Site Seizures," *Informationweek* (Feb. 18, 2011), <http://commcns.org/uFeCLE>

11.5 Impact on infringement levels

The public policy discussions surrounding this procedure justified it, by stressing the dangers of counterfeiting and piracy. However, as the scale section showed, very little of 'Operation In Our Sites' was actually aimed at copyright infringement.

It was therefore difficult to determine whether or not this had a substantial effect on infringement. The enforcement actions were intended mainly to fight live streaming and links sites. For those types of sites, general research suggested that the effects were limited-to-none. There was unfortunately no research on the specific impact of the operation on infringement levels or the supply of infringement in the U.S. at the time.

Others said that the method could technically not be very effective. Users could stop using their ISPs DNS servers and turn to DNS servers that would not filter, or use one of the many circumvention tools in existence to still gain access to the website.¹⁷⁸⁷

However, government representatives have argued that it was effective. For one, blocked sites had to move to new domain names, which caused them to lose their Internet ratings history (which impacted their advertising revenues and search result rankings). Furthermore, ICE director John Morton said that many sites that offered pirated content shut down voluntarily after the takedown of illegal sites. He said that he had "never seen that kind of deterrence come from a single law enforcement action" in all his years in law enforcement. Moreover, Attorney General Eric Holder pointed towards the educational effect of these takedowns.¹⁷⁸⁸

Research done by the Institute for Information Law at the University of Amsterdam revealed that website blocking in general was an ineffective mechanism for fighting copyright infringement. After blocking of the Pirate Bay, for instance, only 5% per cent of the interviewees said they started downloading fewer movies and series from an illegal source.¹⁷⁸⁹ Illegal downloading actually increased in the Netherlands, researchers suggested.¹⁷⁹⁰

An earlier study on website blocking in general that analyzed website blocking in the field of child pornography only revealed that blocking resulted in over blocking, and was not effective.¹⁷⁹¹ Researchers from the Munich school of management and the Copenhagen business school revealed that taking down Megaupload reduced box office revenues for movies.¹⁷⁹² Another study suggested

¹⁷⁸⁷ Ann Chaitovitz et al., "Responding to Online Piracy: Mapping the Legal and Policy Boundaries," 20 *COMmLAW CONSPECTUS* 1, 7 (2011). P.37.

¹⁷⁸⁸ Ann Chaitovitz et al., "Responding to Online Piracy: Mapping the Legal and Policy Boundaries," 20 *COMmLAW CONSPECTUS* 1, 7 (2011). P.38.

¹⁷⁸⁹ Joost Poort and Jorna Leenheer, "File sharing 2@12: Downloading from illegal sources in the Netherlands," *Institute for Information Law & CentERdata*, Amsterdam/Tilburg (2012). Retrieved from http://www.ivir.nl/publications/poort/Filesharing_2012

¹⁷⁹⁰ Andreas Udo de Haes, "Downloaden toegenomen na Pirate Bay-blokkade – UPDATE," *Webwereld* (August 22, 2013), <http://webwereld.nl/e-commerce/78996-downloaden-toegenomen-na-pirate-bay-blokkade---update>.

¹⁷⁹¹ Mike Masnick, "Study Shows That Web Blocking Ignores Real Problems, Doesn't Solve Anything & Is Used As A Political Tool," *Techdirt* (September 30, 2010), <http://www.techdirt.com/articles/20100930/10105711238/study-shows-that-web-blocking-ignores-real-problems-doesn-t-solve-anything-is-used-as-a-political-tool.shtml>.

¹⁷⁹² Emil Protalinski, "Researchers find Megaupload shutdown hurt box office revenues, despite gains for blockbusters," *The Next Web News* (November 24, 2012), <http://thenextweb.com/insider/2012/11/24/researchers-find-megaupload-shutdown-had-a-negative-effect-on-box-office-revenues/#!ziy1X>.

that Megaupload's takedown may have increased the legal movie sales.¹⁷⁹³ Although those studies addressed the economic effects of those seizures, the picture painted by studies on the availability of infringing content all suggested that seizing domains was ineffective. A study by NBC Universal showed that online piracy reacted quickly to site closures or seizures; "shifting from locations or arenas impacted by events to others that offer a comparable spread of infringing content via a similar or different consumption models."¹⁷⁹⁴

According to computer science researchers from Northeastern University, seizing domains from infringing sites was ineffective. They said users put up much more content than was taken down. Soon after files were taken down, there usually was a mild short-term drop in the availability of the files, before they reappeared elsewhere, which led to a "cat-and-mouse game between uploaders and copyright owners." They suggested going after economically motivated actors to effectively target parts of the sharing ecosystem.¹⁷⁹⁵

Other enforcement actions aimed at cyber lockers, had been empirically proven not to be very effective, research suggested. They claim the supply is too big to take down, located too globally, and that taking down a single actor is not enough to disrupt the piracy ecosystem.¹⁷⁹⁶

11.6 The costs of the system

The costs of this system were limited to the government costs for a criminal investigation. However, some commentators have raised some questions about resource allocation. For example there was a study by Jonathan Band of the CCIA on the foreign ownership of IP intensive industries.¹⁷⁹⁷ The US government thus enforced criminal law to the benefit of industries that are in foreign hands.

Enforcing criminal law is a public task, but some, including my interviewees, have questioned whether this was the appropriate allocation of resources at the moment (at the time of my interviews, federal institutions were closing because of budget cuts and the sequester). Bridges for example questioned why the government would spend so many resources on this.¹⁷⁹⁸ The Electronic Frontier Foundation said something similar: "priorities people!"¹⁷⁹⁹

11.7 Conclusion

Federal officers investigated suspected websites with the help of rights holders. DOJ attorneys then evaluated this evidence and presented affidavits to a federal magistrate judge who determined whether probable cause had been established. If that was the case, the judge granted a seizure order that was served on the domestic domain name registry. This domain name registry then had to lock and restrain the domain name until the

¹⁷⁹³ Sam Byford, "Megaupload takedown may have increased legal movie downloads, says study," *The Verge* (March 7, 2013), <http://www.theverge.com/2013/3/7/4077484/study-says-megaupload-shutdown-helped-movie-sales>.

¹⁷⁹⁴ David Price, "Sizing the piracy universe", *Netnames* (September 2013), available at: <https://copyrightalliance.org/sites/default/files/2013-netnames-piracy.pdf>

¹⁷⁹⁵ Ian Steadman, "Study: copyright takedown notices are ineffective at stopping piracy," *Wired* (January 10, 2013), <http://www.wired.co.uk/news/archive/2013-01/10/blocking-no-effect-filesharing>.

¹⁷⁹⁶ Tobias Lauinger et al., "Clickonomics: Determining the Effect of Anti-Piracy Measures for One-Click Hosting," Presentation at the NDSS Symposium (2013), http://www.Internetsociety.org/sites/default/files/07_1_0.pdf

¹⁷⁹⁷ Jonathan Band and Jonathan Gerafi, "Foreign Ownership of Firms in IP Intensive Industries" (March 13, 2013). Available at SSRN: <http://ssrn.com/abstract=2333839> or <http://dx.doi.org/10.2139/ssrn.2333839>

¹⁷⁹⁸ Andrew Bridges (Lawyer at Fenwick & West LLP), interviewed by author, September 2013.

¹⁷⁹⁹ Corynne McSherry (Intellectual Property Director Electronic Frontier Foundation) interviewed by author, September 2013.

completion of the forfeiture proceeding. Only after the seizure had taken place, interested individuals like the owner of the website could contest the measure. The government had to send written notice to the website owner within sixty days of the seizure.

This case showed that agents in the US government grouped sites together which were seized in the thousands (although only a tenth of those were copyright related). Regarding severity, a whole domain was seized. At times, the actions would lead to trials against the people associated with the websites.

These websites were found through web crawling and research. A magistrate judge checked probable cause and there could be a trial after the sanction. Although the burden of proof was on the government, for seizures only probable cause had to be established. There were defenses and a right to be heard only after the seizure. Transparency was difficult in some cases, but the affidavit could be made public afterwards. Many argued that because the seizures lacked safeguards and affected entire domains, this strategy was disproportional.

Although proponents have argued that the procedure was effective, there was no research to back this up. There was a lot of research saying this type of action would have limited effects on infringement. Some have also questioned the allocation of public funds to this procedure. These outcomes will be highlighted again in the conclusion and compared with the outcomes of the other cases.

12. LEY SINDE (SPAIN) IN 2012-2013

12.1 Introduction

Ley Sinde created a new copyright enforcement procedure under Spanish intellectual property law. According to this new law, rights holders could serve a complaint to a newly created commission which would have the power to removed web content. The procedure follows a set of step, which can eventually involve a judge, if content is not voluntarily removed. This chapter has been divided into two subcases: voluntary removal and judge-mandated removal of infringing content. Although cases could proceed to civil or criminal proceedings against owners of infringing service providers, I have no data on that.

For this case study, I owe tremendous gratitude to Ana Olmos, of the Foro de Gobernanza de Internet en España, who sent me relevant information, and introduced me to several people involved in the debate on- and the application of this procedure.

The first section will describe the legal background to this procedure and some legislative histroy, relying on official government documents, news articles and legal sources. I spoke to government officials of the ministry of culture who sent me some information on the application of the procedure; among them was the secretary of the second section of the intellectual property commission. Jorge Cancio Melia, Senior Legal Advisor and Legal Coordinator of the Second Section of the Intellectual Property Commission, Deputy Directorate General for Intellectual Property, sent me a WIPO document he prepared on the SINDE procedure.¹⁸⁰⁰ For the legislative history, some of the source material is from the Intellectual Property Alliance (IIPA), a lobby organization, which could make the information biased. They issue a special 301 watch list recommendation for a number of countries every year. Amongst them is Spain. These recommendations are full of analyses on the state of copyright and infringement. I have used the recommendations for 2011, 2012 and 2013 to see how rights holders considered the Sinde law.¹⁸⁰¹ The following section describes the procedure in practice. It relies mainly on official government documents and legal sources. The next section will be on the variables. The information cited above has been supplemented with academic literature and reports by NGO. I furthermore interviewed Miguel Perez Subias, of the AUI. I also had an email conversation with Victor Domingo, of Asociacion de Internautas, a digital rights NGO. The information was collected from January 2012 until the start of 2014.

¹⁸⁰⁰ Jorge Cancio Meliá, "The administrative and judicial Procedure concerning Internet Infringements: much more than a simple notice and takedown procedure," *WIPO Advisory Committee on Enforcement*, WIPO/ACE/9/21 (December 20, 2014).

¹⁸⁰¹ "Spain" International Intellectual Property Alliance (IIPA), *Special 301 Report on Copyright Enforcement and Protection*. (2011), <http://www.iipa.com/rbc/2011/2011SPEC301SPAIN.pdf>, "Spain" International Intellectual Property Alliance (IIPA), *Special 301 Report on Copyright Enforcement and Protection*. (2012), <http://www.iipa.com/rbc/2012/2012SPEC301SPAIN.PDF>, and: "Spain" International Intellectual Property Alliance (IIPA), *Special 301 Report on Copyright Enforcement and Protection*. (2013), <http://www.iipa.com/rbc/2013/2013SPEC301SPAIN.PDF>

12.2 Legal background

After heavy lobbying by the IIPA and Hollywood and U.S. diplomats, the Spanish government proposed the Sustainable Economy Bill in November 2009.¹⁸⁰² This legislation came to be known as 'Ley Sinde.' Professor Corredoira argued that the Spanish government also implemented this law to pre-empt the then negotiated ACTA treaty, to allow the Spanish government to retain control over copyright enforcement.¹⁸⁰³ However, in the end ACTA was not adopted.

The bill introduced an anti-piracy provision to delete illegal content on Spanish servers or sites hosted on Spanish territory.¹⁸⁰⁴ The law was named after the Minister of Culture at the time: Angeles González Sinde.¹⁸⁰⁵

The law faced a lot of protests at the time. While some said it intended to save thousands of jobs, other parties argued that it did not allow for enough safeguards in its original form, and they wanted to include a judge.¹⁸⁰⁶ Interestingly, even the Spanish cinema body head criticized the law.¹⁸⁰⁷

At the end of 2010, after much protest, the Sustainable Economy bill was finally accepted but without the Ley Sinde amendment. After the initial rejection the US ambassador to Spain sent a warning letter pressuring the Spanish president to adopt the law. If not, Spain would be put on the trade blacklist, which would have left Spain open to a range of retaliatory options.¹⁸⁰⁸

However, few months later, the law was reinstated and approved by the Spanish congress (February 15, 2011). The SINDE part was reintroduced, but with minor changes.¹⁸⁰⁹ These main changes intended to create more judicial control.¹⁸¹⁰ The new government immediately put the law on the agenda, and adopted it within 10 days.¹⁸¹¹ First the Spanish executive refused to enact the law, but after more US pressure, the executive government passed the law, on December 30, 2011.¹⁸¹²

¹⁸⁰² Cory Doctorow, "Wikileaks cables reveal that the US wrote Spain's proposed copyright law," *Boingboing* (December 3, 2010), http://boingboing.net/2010/12/03/wikileaks-cables-rev.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A%20boingboing%2FiBag%20%28Boing%20Boing%29.

¹⁸⁰³ Corredoira, "Anti-piracy Laws and Censorship Governance," P.4

¹⁸⁰⁴ Oscar Montezuma Panez, "Spanish Court Rules That Linking to Potential Copyright Infringing Material Is Not Copyright Infringement," *Electronic Frontier Foundation* (August 5, 2011), <https://www.eff.org/deeplinks/2011/08/spanish-court-rules-linking-potential-copyright>.

¹⁸⁰⁵ Corredoira, "Anti-piracy Laws and Censorship Governance," P.4.

¹⁸⁰⁶ R. Muñoz and R.J. Cano, "Fracasa la 'ley Sinde' en el Congreso tras el último intento del PSOE de conseguir apoyo," *El País* (December 21, 2010), http://cultura.elpais.com/cultura/2010/12/21/actualidad/1292886001_850215.html.

¹⁸⁰⁷ Ernesto, "Law to shutdown P2P sites resurrected by Spanish coalition," *Torrentfreak* (January 25, 2011), <http://torrentfreak.com/law-to-shutdown-p2p-sites-resurrected-by-spanish-coalition-110125/>.

¹⁸⁰⁸ Antonio Fraguas, "EE UU afeó a Zapatero la decisión de no aprobar la 'ley Sinde'," *El País* (January 4, 2012), http://cultura.elpais.com/cultura/2012/01/03/actualidad/1325545206_850215.html.

¹⁸⁰⁹ Jesús Miguel Marcos, "La 'ley Sinde' se salva "sin cambios sustanciales"," *Público* (January 25, 2011), <http://www.publico.es/culturas/357997/la-ley-sinde-se-salva-sin-cambios-sustanciales>.

¹⁸¹⁰ Rocio Garcia, "Gobierno y PP pactan una 'ley Sinde' con más garantías judiciales," *El País* (January 24, 2011), http://cultura.elpais.com/cultura/2011/01/24/actualidad/1295823605_850215.html.

¹⁸¹¹ Pamela Rolf, "Spanish Government Tables Law to Fight Illegal Downloads," *The Hollywood Reporter* (12 March, 2011), <http://www.hollywoodreporter.com/news/sinde-law-illegal-downloads-269328>.

¹⁸¹² "Spain," *Global Censorship Chokepoints*, <https://globalchokepoints.org/countries/spain>.

The law on the sustainable economy amends the Information Society Services and Electronic Commerce Act ("The LSSI") and the Intellectual Property Law (the "LPI"). It creates a new administrative body, called the Intellectual Property Commission (Comisión de Propiedad Intelectual), as part of the Directorate General of Intellectual Property of the Ministry of Culture and Sport, with the authority to examine complaints of hosted copyright infringement from rights holders, and to notify the websites of the complaints."¹⁸¹³ It aims to facilitate the closure of websites that violate IP laws, and creates a new administrative authority, the Intellectual Property Commission, to be in charge of this.

This Commission began operation in March 2012. The Commission consisted of two divisions: the first division replaced the arbitration commission, which arbitrated and mediated conflicts between rights holders and collective rights organizations on the one side and distributing parties on the other side. The second division was in charge of the new enforcement capabilities and could remove web content at the request of copyright holders.¹⁸¹⁴

The law went into effect on the 1st of March 2012. It was immediately sabotaged by hackers.¹⁸¹⁵ The procedure was established by the law 2/2011 of March 4, 2011, on the Sustainable Economy and later implemented by Royal Decree 1889/2011 of December 30, 2011, which governed the functioning of the Intellectual Property Commission.¹⁸¹⁶ Chapters VI en VII of the Royal Decree described exactly how the procedure at the second section of the IP commission worked.¹⁸¹⁷

The procedure targeted infringements of copyright and related rights committed through information society services. The Spanish Consolidated Text of the Law on Intellectual Property governed the copyrights and neighboring or related rights.¹⁸¹⁸

The procedure intended to limit infringement by first pushing for the voluntary removal of illegally offered content or the disabling of access to that content by the party responsible for the infringement. If parties refused to voluntarily do this, provisions were included that would allow measures to suspend intermediary service to stop infringement (in the Spanish territory).¹⁸¹⁹

Procedures were aimed at providers of information society services through which infringement was committed. The concept information society service came from European Directive 1998/34/EC, amended by Directive 1998/48/EC and specified that service providers carried out an "economic activity" (which rules out personal blogs). The procedure was not targeted at file sharing on P2P networks by "ordinary users." "The infringing behavior it targets must be carried out for direct or indirect profit or must cause or be likely to cause financial damage."¹⁸²⁰ According to professor Correidora, this was also one of the big differences with the proposed US SOPA law. She claimed that having to prove that "the

¹⁸¹³ IIPA, *Special 301 Report on Copyright Enforcement and Protection* (2011), P.7.

¹⁸¹⁴ Corredoira, "Anti-piracy Laws and Censorship Governance," P.5.

¹⁸¹⁵ Glyn Moody, "Hacktivist Judo: Musician Exploits New Spanish Law To Overwhelm System With Legitimate Infringement Complaints," *Techdirt* (March 2, 2012), <http://www.techdirt.com/articles/20120302/09570417949/hacktivist-judo-musician-exploits-new-spanish-law-to-overwhelm-system-with-legitimate-infringement-complaints.shtml>.

¹⁸¹⁶ Meliá, "The administrative and judicial Procedure concerning Internet Infringements," P.2.

¹⁸¹⁷ Royal Decree 1889/2011

¹⁸¹⁸ Meliá, "The administrative and judicial Procedure concerning Internet Infringements," P.4.

¹⁸¹⁹ Meliá, "The administrative and judicial Procedure concerning Internet Infringements," P.5.

¹⁸²⁰ Meliá, "The administrative and judicial Procedure concerning Internet Infringements," P.7.

responsible party has, directly or indirectly, acted for purposes of monetary gain and/or has caused patrimonial damage to the owner of the rights” would be difficult to prove.¹⁸²¹

Other involved parties, like intermediary Internet service providers (access providers, caching services, storage services, search engines, linking sites) could be forced to cooperate with the commission as well.¹⁸²²

The procedure was carried out by the second section of the commission on intellectual property rights. This was attached to the Deputy Directorate General for Intellectual Property, which in turn was connected to the ministry of education, culture and sport). Various ministries appoint the members. The secretary of state for culture presided over the second section.¹⁸²³

12.3 The procedure in practice

Initiation

Rights holders and their representatives can initiate the procedure.¹⁸²⁴ A request made was subject to requirements, comparable to those required under the Notice and Takedown procedure in the US DMCA, and were put forward in the Royal Decree.¹⁸²⁵

The request needed to have: a) the identification of the work or other subject of the application; b) Some sort of evidence that proved ownership of the intellectual property rights claimed or the representation of the owner; c) Some form of evidence that showed that the work was being exploited, for profit or not, through the service of the society of information covered by the application, identifying, describing and locating that activity; d) A statement that the service has not been granted permission to operate the content; e) Some evidence that showed that this operation would damage the owner; f) The data available on the service to identify the “perpetrator”; g) Any other relevant circumstances in the process.¹⁸²⁶

Administrative phase

Afterwards the procedure moved to an administrative phase, which verified whether infringement had taken place. This was done by identifying the service provider infringing, as well as identifying the owners of those services. Identification took place through other service providers, which maintained contact with the allegedly infringing service provider (this includes advertising services and privacy protection services). This identification required judicial authorization. This verification led to a report of preliminary proceeding, which according to the Spanish government was enough to serve as evidence. If no infringement was found, the proceedings would be discontinued.¹⁸²⁷ To identify someone,

¹⁸²¹ Corredoira, "Anti-piracy Laws and Censorship Governance," P.6.

¹⁸²² Meliá, "The administrative and judicial Procedure concerning Internet Infringements," P.8.

¹⁸²³ Meliá, "The administrative and judicial Procedure concerning Internet Infringements," P.9.

¹⁸²⁴ Article 15(2) of the royal decree.

¹⁸²⁵ Meliá, "The administrative and judicial Procedure concerning Internet Infringements," P.10.

¹⁸²⁶ Article 17(2) of the Royal decree

¹⁸²⁷ Meliá, "The administrative and judicial Procedure concerning Internet Infringements," P.11-13.

the commission sent the relevant documents, reasons, and evidence to the judge.¹⁸²⁸ The ISP has 48 hours to provide the commission with identifying information.¹⁸²⁹

If infringement was found, the Second Section of the Commission would issue an initial decision to formally open the procedure. This decision contained: (a) identification of the infringing services, (b) reference to the allegedly infringing content and its location, (c) a request to the identified manager of the infringing services to remove the infringing content within a period of 48 hours or to provide counter arguments in his defense. All stakeholders were notified of this.¹⁸³⁰ Respondents are asked to voluntarily take the infringing content down.¹⁸³¹

After 48 hours expire, additional checks were carried out whether the infringement stopped, which got into an additional proceedings report. If removed, the second section would discontinue the procedure. If not removed, the second section would draft a final ruling proposal in which it would respond to statements of all parties, propose a decision, and make a provision for cooperation measures concerning intermediary services. This could become compulsory if the infringer continued the infringement.¹⁸³²

Parties were notified of this proposal and had five days to propose “closing submissions” or final arguments.¹⁸³³ The second section would then issue a final ruling on the case, in which it could order the removal of infringing content. The owner of the infringing services then had 24 hours to remove the content. If they did not, the ISP had 72 hours to remove the content.¹⁸³⁴ After that period, the commission checked if the infringement had been removed. If it was, the report was added to the case file and archived.¹⁸³⁵

If the content had not been removed, the commission would seek judicial authorization (the case would be brought before the Court of Contentious Administrative Proceedings¹⁸³⁶) for the cooperation measures in the final decision. The Court would check whether the resolution was within the limits of the law, and would issue a declaration for all the parties involved.¹⁸³⁷ This declaration could be “disconnection of the storage service provided to the infringing web site; blocking of the infringing web site by the Internet access operators established in Spain; the de-activation of the links to the infringing content or the removal from the index, by search engine services, of the URLs hosting the infringing content.”¹⁸³⁸

Parties had 72 hours to comply with this order. This suspension could last one year, but could also be shortened if the provider of the infringing service had ceased the infringement.¹⁸³⁹ According to professor Correidora, when the commission had discovered a crime, it would inform the criminal courts, “who would act in accordance with the

¹⁸²⁸ Article 18(2) of the Royal Decree.

¹⁸²⁹ Article 18(1) of the Royal Decree.

¹⁸³⁰ Meliá, “The administrative and judicial Procedure concerning Internet Infringements,” P.14-15.

¹⁸³¹ Article 20 of the Royal Decree.

¹⁸³² Meliá, “The administrative and judicial Procedure concerning Internet Infringements,” P.16-17.

¹⁸³³ Article 21 of the Royal Decree.

¹⁸³⁴ Article 22 of the Royal Decree.

¹⁸³⁵ Meliá, “The administrative and judicial Procedure concerning Internet Infringements,” P.18-20.

¹⁸³⁶ “Spain’s latest ‘Ley Sinde’ revision,” *Tumbit.spain* (April 14, 2011), <http://www.tumbit.com/news/articles/3047-spains-latest-ley-sinde-revision.html>.

¹⁸³⁷ Article 23 of the Royal Decree.

¹⁸³⁸ Meliá, “The administrative and judicial Procedure concerning Internet Infringements,” P. 21.

¹⁸³⁹ Meliá, “The administrative and judicial Procedure concerning Internet Infringements,” P.22.

commission's recommendations." In most of such cases, further investigation would be carried out by the criminal court.¹⁸⁴⁰

An interesting side note is that these verdicts could not lead to DNS blocking or locking out domestic or foreign visitors. The commission could also not request traffic documentation. This was also a difference from the in the U.S. proposed and much protested SOPA law.¹⁸⁴¹

12.4 Scale, severity and procedural safeguards

Scale

The government report for WIPO said that between March 2012 (the starting date of the operation) and December 2013 there were 400 requests for initiation submitted to the commission.¹⁸⁴²

Up until December 2013, of those 400 requests, more than 80 per cent were processed and finalized (around 335). The remaining 20% remained in the preliminary phase.¹⁸⁴³

Around 50 per cent of the requests were discontinued. In some cases they were deliberately flawed: an attempt to hinder the Commission's work.¹⁸⁴⁴ This trouble mainly happened at the start, because a hacktivist sabotage campaign was launched, intended to overload the commission with claims on legitimate content.¹⁸⁴⁵

In other cases, requests were made that fell outside of the scope of the Commission's powers, like the identification of P2P users. In other cases requests were made that applied to fair use cases, which made the Commission discontinue those cases as well.¹⁸⁴⁶

More than 20 cases were discontinued because infringement stopped, and in 60 cases content was voluntarily removed when the procedure was formally initiated. The latter involved over 90 web sites, of which 18 were shut down completely.¹⁸⁴⁷ A dozen cases were finalized through definitive rulings.¹⁸⁴⁸

Rights holders were not happy with the scale. In the beginning of 2013, the IIPA said the IP commission had been "extremely slow in response to rights holders' complaints." They said that only two websites were closed down, but voluntarily, and that the IP commission had not made use of its authority to request a judicial writ from the administrative court to close a website or service. IIPA pointed towards "at least 80 complaints outstanding." They argued for more resources to allow complaints to move forward faster.¹⁸⁴⁹

¹⁸⁴⁰ Corredoira, "Anti-piracy Laws and Censorship Governance," P.6.

¹⁸⁴¹ Corredoira, "Anti-piracy Laws and Censorship Governance," P.6.

¹⁸⁴² Meliá, "The administrative and judicial Procedure concerning Internet Infringements," P.32.

¹⁸⁴³ Meliá, "The administrative and judicial Procedure concerning Internet Infringements," P.31.

¹⁸⁴⁴ Enigmax, "Spanish 'SOPA': 79 site takedown requests in first month," *Torrentfreak* (April 4, 2012), <http://torrentfreak.com/spanish-sopa-79-site-takedown-requests-in-first-month-120404/>.

¹⁸⁴⁵ "Casi 80 solicitudes telemáticas de cierre de sitios el primer mes de la Ley Sinde," *El mundo.es* (April 1, 2012), <http://www.elmundo.es/elmundo/2012/04/01/navegante/1333276914.html>.

¹⁸⁴⁶ Meliá, "The administrative and judicial Procedure concerning Internet Infringements," P.32.

¹⁸⁴⁷ Meliá, "The administrative and judicial Procedure concerning Internet Infringements," P.33.

¹⁸⁴⁸ Meliá, "The administrative and judicial Procedure concerning Internet Infringements," P.34.

¹⁸⁴⁹ "Spain" International Intellectual Property Alliance (IIPA), *Special 301 Report on Copyright Enforcement and Protection*. (2013), <http://www.iipa.com/rbc/2013/2013SPEC301SPAIN.PDF>. P.1.

The numbers brought forward by the IIPA to support this position were that between March and December 2012, IIPA partners filed 87 complaints at the IP Commission, of which 16 had been initiated into cases under the commission, and none of which resulted in a website taken down. They called the process “agonizingly slow,” saying “all 16 of the initiated cases were initiated more than 30 days after their filing, 44% of them more than 90 days after their filing, and in two proceedings the delay exceeded 240 days.” They also said that these complaints were urgent and applied to repeat infringement. They complained that only seven cases had been solved.

During 2013, the Spanish government also released information in which it said that it had worked on investigation activities to spot infringement, sometimes in collaboration with the Secretariat of State for Security and the Secretary of State for Telecommunications and the Information Society. This, among other things, led to the cancelling of three domains. According to the government this was the result of collaboration with other bodies of the Central Government with responsibility for monitoring and surveillance of the Internet.¹⁸⁵⁰

This procedure could be divided into two subcases: voluntary removal and judge-mandated removal of infringing content. Requests for action initiated by rights holders were not considered sanctions so they were not included. For this case, voluntary removal scaled up to less than a hundred cases (which involved more than one website per case at times), while judge-mandated removal scaled up to “dozens.”

Severity

Content from websites was taken down, or complete websites. In some cases, access to websites could be blocked by access providers. The owners of infringing service providers could be punished individually as well.

According to Miguel Perez Subias of the Internet users association, these owners did not face consequences if they took the content down. But rights holders could still ask for monetary damages, which would be decided on by a judge.¹⁸⁵¹

Safeguards

Privacy

Whether or not this enforcement strategy interfered with privacy rights, depended on whether personal data was processed. This usually happens when infringement is found, and when enforcing parties have access to personal data.

Infringement was found by rights holders and their representatives, who could then initiate the procedure.¹⁸⁵² A request made would be subject to requirements, comparable to those required under the Notice and Takedown procedure in the US DMCA, and were put

¹⁸⁵⁰“La Policía y la Guardia Civil incautaron objetos que vulneraban derechos de propiedad intelectual por un valor superior a 6 millones de euros,” Press release, Spanish ministry of Education, Culture and Sports (June 11, 2013), <http://www.mecd.gob.es/prensa-mecd/actualidad/2013/06/20130611-propiedad-intelectual.html>

¹⁸⁵¹ Miguel Perez Subias (AUI), interviewed by author, February 2014.

¹⁸⁵² Article 15(2) of the royal decree.

forward in the Royal Decree.¹⁸⁵³ Usually these were made by collective rights organizations,¹⁸⁵⁴ using software to identify links to a song or a book.”¹⁸⁵⁵

The commission could then ask to identify the infringers. However, this required an order by a judge. Identification could run through other service providers, which maintained contact with the allegedly infringing service provider (this included advertising services and privacy protection services).¹⁸⁵⁶ To identify someone, the commission sent the relevant documents, reasons, and evidence to the judge.¹⁸⁵⁷ The ISP has 48 hours to provide the commission with identifying information.¹⁸⁵⁸

When treating the data afterwards, the commission would be legally obligated to stay within the limits of the Spanish data protection laws.¹⁸⁵⁹ The commission could not request traffic documentation.¹⁸⁶⁰ Only the commission would know the identity of the alleged infringer.¹⁸⁶¹

Impartial, competent and independent judge

Whether there was infringement would be judged by the Second Section of the Intellectual Property Commission, and in two phases by someone from the judiciary.

“The Second Section of the Intellectual Property Committee is composed by the head of the Ministry of Culture or person to which it delegates, who will chair the Section; and four members of the Ministries of Education, Culture and sport, Industry, Energy and Tourism, Presidency, Economy and Competitiveness respectively, designated by those departments, between government personnel belonging to groups or categories for which higher qualification is required, and who possess specific knowledge certified in intellectual property. Subject to compliance with the above requirement, the appointment by each department further assesses the legal training in the areas of procedural law, the Contentious-Administrative Jurisdiction and electronic communications.”¹⁸⁶²

In my interviews, worries were raised about the background of the members of this commission. Although candidates seemed to be selected also for their competence, it was interesting to note they represented the governmental side only. Although this suggested a more general perspective, there was no one to represent civil rights.¹⁸⁶³

There was no reason to doubt the impartiality, competence, and independence of the judiciary involved in the other two stages of the process. However, the extent to which this judge actually was involved in the process was difficult to determine.

¹⁸⁵³ Meliá, “The administrative and judicial Procedure concerning Internet Infringements,” P.10.

¹⁸⁵⁴ Miguel Perez Subias (AUI), interviewed by author, February 2014

¹⁸⁵⁵ Miguel Perez Subias (AUI), interviewed by author, February 2014

¹⁸⁵⁶ “Spain,” *Global Censorship Chokepoints*, <https://globalchokepoints.org/countries/spain>.

¹⁸⁵⁷ Article 18(2) of the Royal Decree.

¹⁸⁵⁸ Article 18(1) of the Royal Decree.

¹⁸⁵⁹ Article 13(5) of the Royal Decree.

¹⁸⁶⁰ Corredoira, “Anti-piracy Laws and Censorship Governance,” P.6.

¹⁸⁶¹ Miguel Perez Subias (AUI), interviewed by author, February 2014.

¹⁸⁶² Article 14 Royal Decree.

¹⁸⁶³ Miguel Perez Subias (AUI), interviewed by author, February 2014.

Presumption of innocence

The burden of proof was on the rights holders. As the section on the procedure in practice described, requests made by rights holders were subject to requirements of evidence. These documents were then evaluated by the commission.¹⁸⁶⁴

If infringement was found, the Second Section of the Commission would issue an initial decision to formally open the procedure. As mentioned in the section on the procedure in practice, this decision contained: (a) identification of the infringing services, (b) reference to the allegedly infringing content and its location, (c) a request to the identified manager of the infringing services to remove the infringing content within a period of 48 hours or to provide counter arguments in his defense. All stakeholders were notified of this.¹⁸⁶⁵ In other words, respondents are asked to voluntarily take the infringing content down,¹⁸⁶⁶ on the basis of evidence supplied by rights holders, and given the opportunity to appeal if they thought the assertions were unjustified.

If infringing content was not removed, the second section of the commission would propose a decision, and parties were notified of this proposal and had five days to propose “closing submissions” or final arguments.¹⁸⁶⁷ The second section would then issue a final ruling on the case, in which it could order the removal of infringing content. The owner of the infringing services then had 24 hours to remove the content. If they did not, the ISP had 72 hours to remove the content.¹⁸⁶⁸ Afterwards a judge could be involved.

Some have criticized the limited role for judges in this procedure. One of the main criticisms was that an administrative commission was the party shutting down websites.¹⁸⁶⁹ The judge only intervened in two stages of the procedure: to authorize the transfer of data by an access provider, so that the commission could identify the owner of a website against which it was acting (otherwise this would be a breach of data protection law), and to enforce the decision to shut down or block access to websites.

To identify infringers, the Commission sent the relevant documents, reasons, and evidence to the judge, so here too the burden of proof seemed to be on rights holders.¹⁸⁷⁰

If the Commission ordered the site blocked, the decision required a judge’s formal ratification. However, the court was only allowed to rule on whether there was a constitutional violation in the ruling, not on the actual merits of the case. It would not review the copyright decision.¹⁸⁷¹

According to Spanish newspaper *El País*, the law was curious for two reasons: it made the ministry of culture the main protector of IP rights controlled by the courts, and because the state could act not just against people who caused harm, but also against those “likely to

¹⁸⁶⁴ Article 17(2) of the Royal decree.

¹⁸⁶⁵ Meliá, “The administrative and judicial Procedure concerning Internet Infringements,” P.14-15.

¹⁸⁶⁶ Article 20 of the Royal Decree.

¹⁸⁶⁷ Article 21 of the Royal Decree.

¹⁸⁶⁸ Article 22 of the Royal Decree.

¹⁸⁶⁹ @Wicho, “El papel de los jueces en la Ley Sinde-Wert: básicamente ninguno,” *Microsiervos* (January 5, 2012), <http://www.microsiervos.com/archivo/mundoreal/papel-jueces-ley-sinde-wert-basicamente-ninguno.html>.

¹⁸⁷⁰ Article 18(2) of the Royal Decree.

¹⁸⁷¹ “Procedimiento de salvaguarda de derechos de propiedad intelectual de acuerdo con la Ley Sinde,” *Javier Prenafeta* (January 2, 2012), <http://www.jprenafeta.com/2012/01/02/procedimiento-salvaguarda-propiedad-intelectual-ley-sinde/#>.

cause property damage”, which was more vague and preventive.¹⁸⁷² El Pais feared that this would lead to the closure of 95% of Spanish websites.¹⁸⁷³

In the interviews, Victor Domingo said something similar. The system was intended to be faster than the “always tedious” legal procedures.¹⁸⁷⁴ He called it a complete shift in intellectual property policy. According to him, originally only judges could intervene when rights were infringed upon. “Although rights holders say it is fast, and has “alleged judicial intervention”, it is now different. It is now also about possible violations and possible damages to creators. It’s also an administrative intervention, the judge’s role is limited, and more like a messenger.”¹⁸⁷⁵

Although these claims were made, the low numbers of closed websites seemed to suggest that these claims were overstated.

Notice, right to be heard (prior to conviction), defenses and appeal

Before the alleged infringer would be punished, he or she would be sent a notice, which contained the request to remove the content and the evidence supplied by rights holders. The second section of the Commission would send a request to the identified manager of the infringing services to remove the infringing content within a period of 48 hours or to provide counter arguments in his defense. All stakeholders were notified of this, including the infringing party.¹⁸⁷⁶ In other words, there was a right to be heard.

Afterwards, if infringing content was not removed, the second section of the commission would propose a decision, and parties were notified of this proposal and had five days to propose “closing submissions” or final arguments.¹⁸⁷⁷ This again allowed them a chance to be heard. The second section would then issue a final ruling on the case.¹⁸⁷⁸

After that period, the commission checked if the infringement had been removed. If the content had not been removed, the commission would seek judicial authorization (the case would be brought before the Court of Contentious Administrative Proceedings.)¹⁸⁷⁹ For the cooperation measures in the final decision, the Court would check whether the resolution was within the limits of the law, and would issue a declaration for all the parties involved.¹⁸⁸⁰ It was unclear to what extent this decision could be appealed.

¹⁸⁷² Sergio Rodríguez, “‘Ley Sinde’ for dummies,” *El Mundo* (January 24, 2011), <http://www.elmundo.es/blogs/elmundo/catalejo/2011/01/24/ley-sinde-for-dummies.html>.

¹⁸⁷³ Sergio Rodríguez, “‘Ley Sinde’ for dummies.”

¹⁸⁷⁴ Victor Domingo (Internautas), email to author, April 2014.

¹⁸⁷⁵ Victor Domingo (Internautas), email to author, April 2014.

¹⁸⁷⁶ Meliá, “The administrative and judicial Procedure concerning Internet Infringements,” P.14-15.

¹⁸⁷⁷ Article 21 of the Royal Decree.

¹⁸⁷⁸ Article 22 of the Royal Decree.

¹⁸⁷⁹ “Spain’s latest ‘Ley Sinde’ revision,” *Tumbit.spain* (April 14, 2011), <http://www.tumbit.com/news/articles/3047-spains-latest-ley-sinde-revision.html>.

¹⁸⁸⁰ Article 23 of the Royal Decree.

Transparency

The second section of the commission released its composition after the procedure was already in place. The government relied on data protection laws to keep this anonymous, which caused much protest by legal scholars.¹⁸⁸¹

According to Miguel Perez Subias of AUI, some people discovered a document and found the names. He also said the decisions of the commission were not made public.¹⁸⁸²

Proportionality

Rights holders deemed the measure necessary because of the high piracy numbers. As it aimed for websites that offer infringing services, it seemed suitable as well. On whether it was an excessive burden, user rights organizations seemed to think it was. However, their comments on the proportionality seemed to focus on the lack of safeguards.

Victor Domingo said that “anyone with a website, that links to whatever the Intellectual Property Commission might want to consider allegedly violating the LPI, perhaps causing alleged and hypothetically financial loss and hypothetically alleged profiting from this, you must close.”¹⁸⁸³

He considered it a threat to free speech that the intellectual property law had to defend private interests, with such indeterminate legal concepts.¹⁸⁸⁴ Miguel Perez Subias from AUI also thought there were too little guarantees and that the role of the judge should be bigger, because the people making the judgment were only people with a particular vision of Internet rights.¹⁸⁸⁵

12.5 Impact on infringement levels

To implement Ley Sinde, Spain faced heavy lobbying. Of all the countries in the EU, Spain had been accused of having a relatively high amount of file sharing.¹⁸⁸⁶ According to La Coalición, an industry lobby group (and therefore biased), 50% of all people shared files illegally. Nielsen estimated around 45% of all Spanish people visited websites that offered links to pirated material.¹⁸⁸⁷ The Business Software Alliance estimated piracy levels at around 42-43% between 2007 and 2011.¹⁸⁸⁸ According to the European Observatory on infringements of intellectual property rights, 18% of all Spaniards reported having downloaded illegal content.¹⁸⁸⁹

¹⁸⁸¹ Pablo Romero, “Ésta es la 'Comisión Sinde',” *El Mundo.es* (February 11, 2013), <http://www.elmundo.es/elmundo/2013/02/11/navegante/1360581254.html>.

¹⁸⁸² Miguel Perez Subias (AUI), interviewed by author, February 2014.

¹⁸⁸³ Victor Domingo (Internautas), email to author, April 2014.

¹⁸⁸⁴ Victor Domingo (Internautas), email to author, April 2014.

¹⁸⁸⁵ Miguel Perez Subias (AUI), interviewed by author, February 2014.

¹⁸⁸⁶ Giles Tremlett, “Spain finds that film piracy is a hard habit to break,” *The Guardian* (March 31, 2010), <http://www.guardian.co.uk/world/2010/mar/31/spain-film-piracy-downloading-dvds>.

¹⁸⁸⁷ “Half of Spain's Internet users download illegally,” *The Local es* (April 9, 2014), <http://www.thelocal.es/20140409/spain-failing-in-fight-against-Internet-piracy>.

¹⁸⁸⁸ “Shadow Market,” *Business Software Alliance* (May 2012), http://globalstudy.bsa.org/2011/downloads/study_pdf/2011_BSA_Piracy_Study-Standard.pdf.

¹⁸⁸⁹ “IP in Europe,” *European Observatory on Infringements of Intellectual Property Rights*, <https://oami.europa.eu/ohimportal/nl/web/observatory/ip-in-Europe>.

The industry lobby group IIPA talked about “sky-high Internet piracy levels in Spain” due to a “de facto decriminalization of illegal downloading of content distributed via P2P file sharing.”¹⁸⁹⁰ What they were referring to was that Spanish copyright law made distributing unlicensed content illegal, but allowed for the downloading of it.¹⁸⁹¹ Spain was therefore one of the few countries where courts had declared that peer-to-peer sites could operate legally.¹⁸⁹²

According to the Spanish anti-piracy federation (“FAP”), which included film and videogame groups in Spain, 55% of digital piracy in Spain occurred via P2P networks, 32% via hosted websites, and 11% by streaming sites.¹⁸⁹³ IIPA said that with regard to movies, Spain consistently ranked in the top five countries for absolute downloads, and was “nearly always” the top country on the exchange per capita of illegal copies of films. They said it also had the worst online music piracy among major EU markets, with 45% of all Spanish Internet users using services that distributed music illegally (the EU average is 23%).¹⁸⁹⁴

IIPA also pointed to a study done by the International Data Cooperation (IDC) in 2010, which revealed that the Internet music piracy rate in Spain was 98.8%.¹⁸⁹⁵ In that same study, almost 70% of Spanish Internet users admitted to downloading illegal copyright content through P2P (85% of people under 24) and that almost 50% of users downloaded from direct download sites (75% of people under 24).¹⁸⁹⁶

These figures were used in the strong international lobby for more stringent legislation in Spain. When Wikileaks gave an intimate insight into U.S. diplomacy in 2010, they also revealed that Hollywood and U.S. diplomats had pressured Spain into adopting legislation that would target piracy.¹⁸⁹⁷

The U.S. had planned to put Spain on the special 301 Watch list. This annual 301 report reflected the U.S. Administration’s “continued resolve to encourage and maintain adequate and effective IPR protection and enforcement worldwide.”¹⁸⁹⁸ Countries put on the list could be subject to trade sanctions. Therefore in 2009, the Spanish government proposed the Sustainable Economy Bill. It took until the end of 2011 for the law to be approved in full form.

During the discussions on the new law, many warned that its effects on infringement would be small. In an interview with IEEE spectrum, professor Rosa Maria Sanz warned that it would only encourage people to use P2P. She also predicted that the law would be difficult

¹⁸⁹⁰ IIPA, *Special 301 Report on Copyright Enforcement and Protection* (2011), P. 1.

¹⁸⁹¹ Andrés Cala, “Push grows to blacklist Spain over digital pirating,” *The Christian Science Monitor* (March 4, 2013), [http://www.csmonitor.com/World/Europe/2013/0304/Push-grows-to-blacklist-Spain-over-digital-pirating/\(page\)/2](http://www.csmonitor.com/World/Europe/2013/0304/Push-grows-to-blacklist-Spain-over-digital-pirating/(page)/2).

¹⁸⁹² Jose Elias Rodriguez, “Spain's anti-piracy law may already be obsolete,” *Reuters* (March 26, 2012), <http://www.reuters.com/article/2012/03/26/net-us-spain-piracy-idUSBRE82P0JV20120326>.

¹⁸⁹³ IIPA, *Special 301 Report on Copyright Enforcement and Protection* (2011), P.2.

¹⁸⁹⁴ IIPA, *Special 301 Report on Copyright Enforcement and Protection* (2011), P.2.

¹⁸⁹⁵ IIPA, *Special 301 Report on Copyright Enforcement and Protection* (2011), P.2.

¹⁸⁹⁶ IIPA, *Special 301 Report on Copyright Enforcement and Protection* (2011), P.3.

¹⁸⁹⁷ Cory Doctorow, “Wikileaks cables reveal that the US wrote Spain's proposed copyright law,” *Boingboing* (December 3, 2010), http://boingboing.net/2010/12/03/wikileaks-cables-rev.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A%20boingboing%2FiBag%20%28Boing%20Boing%29.

¹⁸⁹⁸ “2013 Special 301 Report,” The Office of the United States Trade Representative (USTR) (January 5, 2013), <https://ustr.gov/sites/default/files/05012013%202013%20Special%20301%20Report.pdf>

to enforce. "There is a real problem of applying the law because it's so easy to circumvent the technical barriers used to block users from reaching the websites."¹⁸⁹⁹

This is similar to the reactions to SOPA, a similar law proposed in the US, as security analysts at Sandia National Laboratories warned for DNS hijacking, and called it a "whack-a-mole" approach that would only encourage users and owners of websites to resort to low cost workarounds.¹⁹⁰⁰

But there was other criticism on its functioning. Economists called the law useless. They said it would benefit only major labels and artists "at the expense of users and lesser-known artists."¹⁹⁰¹

Effect

As predicted, after coming into force, a lot of Internet traffic switched away from websites that offered links to copyright protected material and towards P2P sharing services instead.¹⁹⁰² However, that trend was also attributable to the closure of Megaupload, which at the time was the largest global file-sharing website (It was shut down by the U.S. government).¹⁹⁰³

This was one of the reasons the IIPA reacted furiously at the end of 2012. They issued a report saying that piracy continued to grow.¹⁹⁰⁴

The IIPA on the other hand thought that the procedure as introduced was "unnecessarily complicated for what should be a straightforward procedure."¹⁹⁰⁵ During the discussion on the law they had already said: "However, rights holders await the eventual implementation of such a procedure to determine whether its multiple layers of court review will undermine the law's efforts to encourage swift removal of infringing content."¹⁹⁰⁶

After this implementation, IIPA said the IP commission had been "extremely slow in response to rights holders' complaints." They also said: "whatever deterrent effect against online infringement the initial introduction of the measures had has now been halted by government inaction, as the LES procedures in practice have proven to be ineffectual. More than ever, websites providing or linking to illegal content can be secure in the knowledge that takedown measures are nonexistent and result in no consequences."¹⁹⁰⁷ Later, the IIPA report said that "there is very little to deter the average consumer from participating in an online free-for-all for unauthorized copyrighted content."¹⁹⁰⁸

¹⁸⁹⁹ Morgen Peck, "Spain's SOPA Law: How It Works And Why It Won't," *IEEE Spectrum* (January 9, 2012), <http://spectrum.ieee.org/tech-talk/telecom/Internet/spains-sopa-law-how-it-works-and-why-it-wont-work>.

¹⁹⁰⁰ Morgen Peck, "Spain's SOPA Law: How It Works And Why It Won't."

¹⁹⁰¹ Ernesto, "Economists urge government to stop war on piracy," *Torrentfreak* (March 27, 2010), <http://torrentfreak.com/economists-urge-government-to-stop-war-on-piracy-100327/>

¹⁹⁰² Jose Elias Rodriguez, "Spain's anti-piracy law may already be obsolete."

¹⁹⁰³ Jose Elias Rodriguez, "Spain's anti-piracy law may already be obsolete," *Reuters* (March 26, 2012), <http://www.reuters.com/article/2012/03/26/net-us-spain-piracy-idUSBRE82P0JV20120326>.

¹⁹⁰⁴ Andrés Cala, "Push grows to blacklist Spain over digital pirating."

¹⁹⁰⁵ IIPA, *Special 301 Report on Copyright Enforcement and Protection* (2011), P.1.

¹⁹⁰⁶ IIPA, *Special 301 Report on Copyright Enforcement and Protection* (2011), P.7.

¹⁹⁰⁷ "Spain" International Intellectual Property Alliance (IIPA), *Special 301 Report on Copyright Enforcement and Protection*. (2013), <http://www.iipa.com/rbc/2013/2013SPEC301SPAIN.PDF>. P.1.

¹⁹⁰⁸ IIPA, *Special 301 Report on Copyright Enforcement and Protection* (2013), P.2.

Although Spain implemented the law, the copyright industries claimed piracy expanded. Online streaming grew and became a more important form of piracy.¹⁹⁰⁹ According to FAP there were nearly 400 websites offering to Spanish consumers unauthorized access to movies and videogames.¹⁹¹⁰ Illegal music downloads remained high. According to SOLUS, 52% of music piracy happened through P2P, but other sources like cyber locker (55% of all non-P2P activity), hosted webpages (31%) and streaming (14%) accounted for a large percentage of piracy as well.¹⁹¹¹

For the IIPA speedy takedowns were important, and they saw failure in this regard. They also complained that the commission treated linking sites as intermediaries, which they considered bad, because this way they claimed “linking sites (in practice the more dynamic and harmful actor in these circumstances) are not held accountable for immediate takedowns as responsible parties.” The procedure was also ineffective against cyber lockers, they said, because these were “frequently, if not always, located in foreign jurisdictions.”¹⁹¹²

Governmental reaction to results

The governmental report on the procedure said that the procedure was not sufficient on its own to solve piracy, but had “added value.”¹⁹¹³

It said that to fight piracy, one should promote legal offers, offer education and awareness training, and as a third pillar ensure rights protection. This ‘Sinde procedure’ did not attempt to replace the other rights action to protect rights (like self regulation, notice and takedown and civil and criminal actions, but rather served as an additional way to protect copyrights.¹⁹¹⁴

Although the procedure appeared to be similar to a Notice and takedown procedure, it offered added value according to the presentation because it identified infringers and other stakeholders. This was good, because according to the report Internet anonymity of the owners of infringing web sites was one of their best means of “protection” against legal reprisals.¹⁹¹⁵

Another added value, according to the report, was the intervention of a public authority within the framework of an adversarial procedure, which would fully respect due process principles. This also involved the determination by a “competent public authority of the existence of an infringement of intellectual property rights, through a detailed, reasoned and justified ruling.”¹⁹¹⁶

Another added value according to the report was that after a takedown or disabled access was ordered, the owner of the service had to abstain from making the same content available in the future. Plus there would be interruption or suspension measures by intermediary services if the infringer did not comply. This would create more effective knowledge among third party intermediary services of infringing behavior of their clients.¹⁹¹⁷

¹⁹⁰⁹ IIPA, *Special 301 Report on Copyright Enforcement and Protection* (2013), P.2.

¹⁹¹⁰ IIPA, *Special 301 Report on Copyright Enforcement and Protection* (2013), P.3.

¹⁹¹¹ IIPA, *Special 301 Report on Copyright Enforcement and Protection* (2013), P.7.

¹⁹¹² IIPA, *Special 301 Report on Copyright Enforcement and Protection* (2013), P.7.

¹⁹¹³ Meliá, “The administrative and judicial Procedure concerning Internet Infringements,” P.23 -30.

¹⁹¹⁴ Meliá, “The administrative and judicial Procedure concerning Internet Infringements,” P.23-26.

¹⁹¹⁵ Meliá, “The administrative and judicial Procedure concerning Internet Infringements,” P.27-29.

¹⁹¹⁶ Meliá, “The administrative and judicial Procedure concerning Internet Infringements,” P.29.

¹⁹¹⁷ Meliá, “The administrative and judicial Procedure concerning Internet Infringements,” P.29.

The government did see obstacles connected to this procedure. Amongst them, they highlighted the lack of accurate registration data for Internet domain names, which made it difficult to identify owners, and the “massive use of privacy protection or identification data masking services concerning generic Internet domains.” They also wanted more collaboration with intermediaries like online payment or advertising services.¹⁹¹⁸

Reaction civil society

Miguel from the Internet users association said the procedure has not been effective. Mostly he blamed the cultural shift in user behaviour. “We have changed. We use information in a different way than before. Before, the industry sold copies. Now, on the Internet the value of a copy is nothing. The cost for a megabyte is near zero, and the ability to make copies is infinite. To make money selling copies is not possible in the Internet era.”¹⁹¹⁹

He argued that industry needed to change their business model. He said that it was of no use to prosecute users, because there would always be P2P. “They can move to the Kayman islands.”¹⁹²⁰

Victor Domingo, of Asociacion de Internautas, a digital rights organization, said the system was intended to be faster than the “always tedious” legal procedures.¹⁹²¹

Aftermath

In 2012, IIPA applauded swift action to implement law, but pressed Spain for more action, as P2P infringement remained largely unaffected. The Spanish government reacted to IPPA that they planned more ambitious legislation.¹⁹²²

In the 2013 special 301 report, Spain “escaped” the list, and received some congratulatory remarks: “MPAA welcomes the efforts of the Spanish government to enforce copyright protection and looks forward to concrete results in the months ahead.”¹⁹²³ However, because piracy numbers remained high, the Intellectual Property Alliance pushed for Spain to be put on the list again. They issued a report saying that piracy continued to grow. The Spanish government reacted that they planned more ambitious legislation.¹⁹²⁴

In other words, pressure resurfaced. On January 22, 2013, Chris Dodd of the MPAA met with Spanish prime minister to discuss more stringent legislation. Later, the US ambassador also criticized the Spanish track record. Later, the US ambassador to Spain also criticized the Spanish track record on copyright enforcement.¹⁹²⁵

To avoid being placed on the list for 2014, the Spanish government approved more stringent amendments to its penal code, making linking to pirated content a crime, punishable to up to 6 years in prison. However, the new law still did not affect link hosting

¹⁹¹⁸ Meliá, “The administrative and judicial Procedure concerning Internet Infringements,” P.36.

¹⁹¹⁹ Miguel Perez Subias (AUI), interviewed by author, February 2014

¹⁹²⁰ Miguel Perez Subias (AUI), interviewed by author, February 2014

¹⁹²¹ Victor Domingo (Internautas), email to author, April 2014.

¹⁹²² Andrés Cala, “Push grows to blacklist Spain over digital pirating.”

¹⁹²³ Eriq Gardner, “Spain Escapes U.S. Trade Rep's Piracy 'Watch List',” *The Hollywood Reporter* (May 1, 2013), <http://www.hollywoodreporter.com/thr-esq/spain-escapes-us-trade-reps-450185>.

¹⁹²⁴ Andrés Cala, “Push grows to blacklist Spain over digital pirating,” *The Christian Science Monitor* (March 4, 2013), [http://www.csmonitor.com/World/Europe/2013/0304/Push-grows-to-blacklist-Spain-over-digital-pirating/\(page\)/2](http://www.csmonitor.com/World/Europe/2013/0304/Push-grows-to-blacklist-Spain-over-digital-pirating/(page)/2).

¹⁹²⁵ Andrés Cala, “Push grows to blacklist Spain over digital pirating.”

sites and P2P sites.¹⁹²⁶ The new laws also aimed to make those facilitating, or third players profiting directly or indirectly from infringement, liable.¹⁹²⁷ This new law would take effect in the start of 2014.¹⁹²⁸

Miguel Perez Subias of the Internet users association called it a “modification of this law” and a “step in the wrong way.”¹⁹²⁹

In a report presented at WIPO, a representative of the Spanish government said that Spain would promote new reforms to fight piracy, like:

“(a) promoting a project to amend the Law on copyright and related rights, which will involve the introduction of the following improvements: -clarification that sophisticated linked web sites are involved in the economic exploitation of works localized by them whenever those sites display certain characteristics; -the empowerment of the CPI to broaden the range of works or subject matters to be protected in each case file; -the establishment of minimum requirements concerning the prior reporting of infringements and prior efforts in terms of self-protection; the broadening of the scope of the range of cooperation measures to cover advertising and electronic payment service providers – at the same time promoting self-regulatory solutions in said spheres; -the establishment of administrative sanctions for repeat infringers; -the promotion of self-regulation for technical intermediaries in the spheres of payment and advertising; -the improvement of civil procedural measures concerning the identification of large-scale infringers. (b) promoting reforms of the Criminal Code that will close the gap represented by the lack of criminal prosecution of behavior involving the sophisticated localization on the Internet of infringing content for profit and to the detriment of third parties.”¹⁹³⁰

12.6 The costs of the system

Because of the lack of transparency surrounding the procedure, it was unknown what the economic costs were connected to this procedure. Rights holders had costs, because they had to spot infringement, while governmental funds were allocated to the commission to function. For rights holders this allocation was not enough. The IIPA argued that the government of Spain needed to give more resources to the commission to allow complaints to move forward toward a speedy resolution.¹⁹³¹

According to Miguel of the Spanish Users Association, the commission was paid by the Spanish government, but it was unknown how much they earned or whether they earned money for this work specifically and for example how much time they spent on this work. Little was known about the inside functioning of the commission.¹⁹³²

¹⁹²⁶ “Spain readies hefty jail terms over Internet piracy,” *Reuters* (September 20, 2013), <http://www.reuters.com/article/2013/09/20/net-us-spain-piracy-idUSBRE98JORD20130920>.

¹⁹²⁷ Thomas Campbell, “Spanish government to come down harder on those benefiting from online piracy,” *IP&TV news* (September 23, 2013), <http://www.iptv-news.com/2013/09/spanish-government-to-come-down-harder-on-those-benefiting-from-online-piracy/>.

¹⁹²⁸ “Spain readies hefty jail terms over Internet piracy,” *Reuters*.

¹⁹²⁹ Miguel Perez Subias (AUI), interviewed by author, February 2014.

¹⁹³⁰ Meliá, “The administrative and judicial Procedure concerning Internet Infringements,” P.37.

¹⁹³¹ “Spain” International Intellectual Property Alliance (IIPA), *Special 301 Report on Copyright Enforcement and Protection*. (2013), <http://www.iipa.com/rbc/2013/2013SPEC301SPAIN.PDF>. P.1.

¹⁹³² Miguel Perez Subias (AUI), interviewed by author, February 2014.

12.7 Conclusion

Rights holders and their representatives could initiate the procedure by making a request similar to a DMCA notice and takedown request. The second session of the Spanish intellectual property commission would verify whether infringement had taken place. They could ask to identify the allegedly infringing service. This identification required judicial authorization.

If infringement was found, the Second Section of the Commission would issue decisions following an extensive time plan. During these decision rounds parties were asked to present their views. If after multiple times content was not removed the commission would seek judicial authorization (the case will be brought before the Court of Contentious Administrative Proceedings) for the cooperation measures in the final decision. In case of criminal behavior, additional proceedings could be launched.

This procedure has been divided into two subcases: voluntary removal and judge-mandated removal of infringing content. Requests for action initiated by rights holders were not considered sanctions so they were not included. For this case, voluntary removal scaled up to less than a hundred cases (which involved more than one website per case at times), while judge-mandated removal scaled up to “dozens.”

Regarding safeguards, there appeared to be privacy protection because contact details could be requested for additional proceedings, but this was protected by a judge. It was not clear if the commission that verified claims was completely impartial or independent because it had no members with a consumer rights background. There was a judge in a later phase, but its role was limited. Regarding a presumption of innocence, the procedure allowed website owners to submit their views and placed the burden of evidence on rights holders. Alleged infringers were notified, and had the right to be heard repeatedly and access to defenses and appeal. The procedure was not transparent, and user rights organizations thought it was disproportional.

Many complained that there was hardly an effect on infringement. The costs of the procedure were unknown, although rights holders seemed to think that more resources had to be allocated to this procedure. These outcomes will be highlighted again in the conclusion and compared with the outcomes of the other cases.

PART III: ANALYSIS AND CONCLUSION

13. FINDINGS AND ANALYSIS

13.1 Introduction

This research introduced the main research question: *“How does large-scale copyright enforcement on the Internet influence procedural safeguards like due process and fair trial, what are its costs and its effectiveness, and what do these findings imply for public policy?”*

Chapter 2 showed that new Internet-based technologies have facilitated large-scale copyright infringement in different ways. It also showed that many different actors are involved in infringement, in one way or another, and thus potentially relevant to enforcement actions. By specifying what constitutes a large scale, the chapter showed that infringement has remained high throughout the years: depending on the region, 15% to 70% of the population has infringed on copyrights. Although infringement happens on a large scale, the exact effect on the entertainment market is unclear. A segment on the economic impact of infringement showed that the market is adapting to these changes. It seems to be doing well in some areas, worse in others. Findings suggest that the losses are concentrated in a certain sector of the entertainment economy.

Chapter 3 showed that one way in which rights holders have responded is by trying to increase enforcement and control over the technologies through which their content is distributed. This led to different legislative changes. The two most important ways to enforce copyrights are through civil remedies and through criminal sanctions. The latter is associated with large-scale and profit-driven infringement. Civil remedies are intended to compensate economic injury suffered as a result of infringement and as a deterrent to further infringement. Criminal sanctions are intended to punish and deter further infringement.

A key problem that rights holders have been trying to solve is scale. While copyright infringement happens on a large scale, enforcement would have to impact on a large scale as well to be an effective deterrent. Dealing with infringement on a case-by-case basis is too costly in terms of time and money, especially when judicial procedures have to be followed, so new procedures had to be created. The chapter also discussed the difficulties of enforcement. Discovery of infringement is not a trivial problem. P2P networks operate pseudonymously, so to discover users for enforcement purposes, enforcers are dependent on linking IP addresses to users. The help of ISPs is required to link IP addresses to subscriber information. Furthermore, quite some errors and complexities have emerged in the effort to connect IP address to the actual users committing the infringement.

Rights holders have adopted new strategies to scale up enforcement, which can be categorized into four groups: (1) they target the demand for infringing content (end-users) directly on a large scale by aiming for settlements instead of actual lawsuits. (2) They target end-users indirectly through intermediaries, such as ISPs, that apply graduated response procedures. These procedures use a system of increasingly severe sanctions for each infringement to deter users, often starting with a warning letter and ending with Internet disconnection or fines as the ultimate sanction if infringement keeps happening. These procedures require intermediaries in the administration of sanctions. (3) They target the supply side directly by taking down or filtering websites that offer infringing content. Governmental parties often carry out these procedures. (4) They target the supply side indirectly by asking intermediaries, such as hosting companies or video sharing platforms, to

take action against infringing content. Notice and takedown procedures allow rights holders to notify websites of infringement and require them to take this content down.

These strategies are seen as a threat to human rights and procedural safeguards by technologists, academics and civil society organizations. Procedural safeguards, such as due process and fair trial, have been defined as the safeguards that aim to protect individuals from arbitrary power and from wrongful punishment, when they face deprivation of property or liberty as a result of enforcement or some form of arbitration, like in a court of law. They are important in the copyright context, because they protect the rule of law, free speech and other important values.

Proponents of more enforcement however claim there are large societal costs of infringement, and that massive investment in enforcement is therefore justified. Rights holders, White House and EU representatives also claim intensified enforcement can be done in accordance with human rights.¹⁹³³ For recent proposals like SOPA and ACTA, rights holders like the Movie Picture Association and the US Chamber of Commerce claim they follow the same rules of civil procedure you would find in an ordinary trial. According to them, copyright enforcement targets illegal sites and people that infringe on copyright only and does nothing to harm legal uses of content and Internet users who are not sharing protected content.

Chapter 4 showed that theoretically, large-scale enforcement can be understood through the lense of legal economics. Legal economics predicts a certain level of effectiveness of enforcement: effective deterrence requires large-scale enforcement and more severe sanctions in order to increase the costs of breaking the law. Increasing the scale of enforcement, hence increasing the chance of getting caught, is particularly effective. These theories also describe that scaling up enforcement is costly and that it is often associated with reduced procedural safeguards, because legal procedures are time consuming and expensive. When this tradeoff between scale and safeguards also applies to copyright enforcement, then the consequences can be serious for human rights and public values.

Next to increasing scale, effectiveness could also be increased through more severe sanctions. How is severity associated with procedural safeguards? If consequences of punishments are more severe, then the lack of procedural safeguards is more likely to lead to more severe wrongful sanctions and a more negative societal impact.

To empirically study the relationship between scale, severity and safeguards in online copyright enforcement, we analyzed 22 sanctioning mechanisms that belong to eight enforcement strategies in six countries between 2004 and 2014. Each enforcement strategy is a case study. We looked at what is known about its impact on infringement levels and its costs. Within each strategy, there can be multiple sanctioning mechanisms. We study these as subcases, where we identified the scale at which they were executed, the severity of the sanctions, and the safeguards provided to the actors on which the sanctions are imposed.

We first summarize the main results of the case and subcase studies. We qualitatively compare them to each other in terms of scale, severity and safeguards. This comparative analysis allows us to reconstruct the overall pattern across the 22 subcases, which allows us to answer the main research question. We then turn to the findings in terms of the cost of the strategies and their effectiveness in terms of reducing infringement. Afterwards, we

¹⁹³³ Declan McCullagh, "SOPA's most aggressive defender: U.S. Chamber of Commerce," *CNET* (November 30, 2011), <http://www.cnet.com/news/sopas-most-aggressive-defender-u-s-chamber-of-commerce/>.

highlight the possible limitations of this study. We end by reflecting on the implications of all these findings for the policy debate around online copyright enforcement.

13.2 Summary of case results

The first part of this chapter will summarize the case results and justify their subsequent categorization on the variables of scale, safeguards and severity. For each variable, the findings are summarized in a table and then combined into a graph that provides a comparative analysis of the cases.

Scale

This research qualifies scale in the number of people or entities to which a sanctioning mechanism is applied. To measure, qualify and compare scale is a bit more straightforward than the other variables in my study. After all, scale is in essence quantitative already. However, there are constraints and complexities here as well. Scale can be related to a regional or national legal district and can be limited to the organization(s) using the enforcement procedure. This makes the comparison more difficult. Similarly, the cases cover different time periods. For example, pre-settlement letters in the US were sent on a large scale (hundreds of thousands) by multiple law firms, whereas the French HADOPI sent out warning letters as one organization. Also, the amount of people living in a region can be taken into account. Targeting a thousand users in the US would not be the same scale as it would be in the Netherlands. For these reasons, we will compare the scale of sanctioning mechanisms in terms of orders of magnitude. Our categories range from very small to very large (the results are in table 13.1).

We start at the very large end of the spectrum. Enforcement took place on the largest scale at Google, when it applied its notice and takedown to its search engine, and at the French HADOPI authority, when it sent out the warnings. They both took place on a scale that ranged in the millions. HADOPI's warning system particularly large, in light of the fact that it only targeted French citizens. For Google, the trusted removal program allowed for millions of delistings in search, while manual takedowns allowed for a smaller amount of takedowns, but it still ranged into the millions of delistings. There was no precise data on ContentID, another mechanism used by Google, but the company reported that the program covered more than 200 million videos until 2013 (which means they were either blocked, monetized or tracked), which would testify to its incredible scale. For YouTube, manual takedowns consisted of only a fraction of the total amount of takedowns. This number was still estimated to range in the millions, however.

Next in line – i.e., going from very large to large scale – are the settlement letters sent by law firms in the US and the UK and the warnings sent out by Eircom. Multiple law firms have targeted hundreds of thousands of people in the US and two law firms have targeted tens of thousands of people in the UK. Eircom sent out tens of thousands of warning letters. This makes Eircoms' system scale in the same order of magnitude as the settlement letters, as this system reached thousands of people in only a year, whereas the settlement requests were sent in a longer period.

The qualification medium is for the thousands of websites seized by ICE in the US through 'Operation in Our Sites.' Each year, ICE seized almost a thousand websites. About half of those websites were forfeited, which is why this mechanism is also categorized as

medium. Notice and takedown in the Netherlands is more difficult to measure, as organizations have used it in different ways: they have used the procedure to takedown content from websites, but also to takedown websites at hosting providers or by getting contact details and writing to the website owner. Furthermore, there was no data on the total amount of takedowns in the Netherlands. What we do know, is that Brein, a leading rights holder enforcement organization, consistently targeted hundreds of websites each year. I have grouped those applications of the Dutch NTD procedure together and qualified them as medium. Similarly, I added the trusted removal program as applied by Leaseweb under medium, because they also receive hundreds of requests each year. Although the application of this procedure was done by Leaseweb alone and could have scaled to allow for more takedowns, it was only open to a limited group of complainants.

The SINDE procedure has been applied on a smaller scale than ‘Operation in Our Sites,’ where less than a hundred websites were voluntarily taken down. This is why it is qualified as small scale. Similarly, Eircom disconnected people for seven days on a small scale. This affected around one hundred users in the first year of its application.

On a very small scale, Eircom disconnected 12 people for a longer period. Similarly, very few of RIAA court cases actually made it to trial. I have categorized HADOPI criminal cases also as very small scale, because it was only applied to 51 people. The other strategies that involved court cases also occurred on a very small scale. For example, the SINDE procedure required judge mandated removal in only a “handful” of cases.

Case	Subcase	Scale	Qualification
Targeting end users directly (US)			
	Settlement letter	Hundreds of thousands	Large
	Court case	Few	Very small
Targeting end users directly (UK)			
	Settlement letter	Tens of thousands	Large
	Court case	Less than ten	Very small
HADOPI graduated response (France)			
	1 st warning	Millions	Very large
	2 nd warning	Hundreds of thousands	Large
	Court case	51 people	Very small
Eircom graduated response (Ireland)			
	1 st warning	Tens of thousands	Large
	2 nd warning	Thousands	Large
	7-day suspension	Around a hundred	Small
	12-month suspension	Less than hundred	Very small
NTD at Google/YouTube			
	NTD Google Search	Millions	Very large

	TCRP	Millions	Very large
	NTD YouTube	Millions	Very large
	Content ID	Millions	Very large
NTD in the Netherlands			
	NTD NL ISPs	Hundreds	Medium
	NTD Leaseweb trusted removal program	Hundreds	Medium
Operation 'In Our Sites' (USA)			
	Seizure	Thousands	Medium
	Forfeiture	Thousands	Medium
	Personal trial	Hundreds	Small
Ley SINDE (Spain)			
	Voluntary removal	Less than a hundred	Small
	Judge mandated removal	"a dozen"	Very small

Table 13.1: *qualifying the cases for scale.*

Severity

Severity is qualified on an ordinal scale of 3 scales of magnitude, ranging from low to high. Impact is a difficult thing to measure, because sanctions can impact businesses or individuals at various times and in varying ways. We also have limited data on the real effects of the sanction on the affected parties. For this reason, it make no sense to strive for higher granularity in the categories.

Most cases qualify as 'medium'. There is quite some diversity within this category, though. For some, a fine of thousands of dollars can be a higher punishment than the loss of a website. For others, losing a website can mean shutting down an entire business. Although these differences exist, we cannot rank them more precisely in terms of impact in the absence of more data on the effects. However, some of these differences will be taken into account in the further evaluation of the variables, later in this chapter. The results are in table 13.2.

Delisting a Google search result and the warnings sent by HADOPI and Eircom are qualified as low severity, because of their limited impact on the people involved. It also includes the videos claimed through Content ID on YouTube, especially because the majority of the videos were monetized, rather than removed. General YouTube takedowns are also in this category, because those takedowns typically only concerned one expression of audiovisual content within Google's own network.

Mechanisms with medium severity have a more substantial impact on people, from the removal of a website (through the SINDE procedure in Spain, Notice and takedown in the Netherlands, or 'Operation in Our Sites' in the US) to disconnections by Eircom. Although the second disconnection is a more severe sanction, the impact is not as high as heavy fines. I have qualified the pre-settlement letters as medium too, because they range up to a thousand dollars or pounds. The HADOPI court case could have been rated as high severity, but in practice the penalties have been very modest.

High severity covers the most impactful sanctions. The only penalties that qualify for this are the very high fines in the court cases against individual file sharers, which ranged in the hundreds of thousands of dollars in the US to the tens of thousands of pounds in the UK, and the criminal cases associated with ICE operation 'In Our Sites', because site operators ended up in prison. The impact of those fines and sentences was much greater than taking down a website or the disconnection of a broadband service.

Case	Subcase	Severity	Qualification
Targeting end users directly (US)			
	Settlement letter	Law firms asked for sums between the hundreds and thousands of dollars.	Medium
	Court case	The severity of the RIAA trials ranged into the hundreds of thousands of dollars.	High
Targeting end users directly (UK)			
	Settlement letter	The law firms asked for settlements between 300 and 700 pounds.	Medium
	Court case	The default judgements by court would lead to sums between 2,750 and 16,000 pounds.	High
HADOPI graduated response (France)			
	1 st warning	A warning.	Low
	2 nd warning	A warning.	Low
	Court case	The resulting penalty was supposed to be disconnection. However, the penalties have been fines between 50 and 600 Euros.	Medium
Eircom graduated response (Ireland)			
	1 st warning	A warning.	Low
	2 nd warning	A warning.	Low
	7-day suspension	A 7-day suspension.	Medium
	12-month suspension	A longer suspension, ranging to 12 months.	Medium
NTD at Google/YouTube			
	NTD Google Search	Delisting a search result.	Low
	TCRP	Delisting search results.	Low
	NTD YouTube	A YouTube video was taken down.	Low
	Content ID	A YouTube video was either blocked, monetized or tracked.	Low
NTD in the Netherlands			
	NTD NL ISPs	Websites are taken down and expressions of content on websites.	Medium

	NTD Leaseweb trusted removal program	Websites are taken down and expressions of content on websites.	Medium
Operation 'In Our Sites' (USA)			
	Seizure	Website was blocked	Medium
	Forfeiture	Website was forfeited	Medium
	Personal trial	Criminal trial	High
Ley SINDE (Spain)			
	Voluntary removal	Website was blocked	Medium
	Judge mandated removal	Website was blocked	Medium

Table 13.2: *qualifying the cases for severity.*

Safeguards

It should not come as a surprise that it is very challenging to compare across sanctioning mechanisms the degree of procedural safeguards in place. Safeguards aim to prevent mistrial and abuse, but it is difficult to assess how much particular safeguards contribute to these objectives. For example, proportionality is a safeguard related to the fairness of punishment, but it is less important to prevent mistrial. Another problem is that some sanctions have different focal points, which has consequences for the relevant safeguards. Notice and takedown, for example, aims to take content down. Because it is aimed at content, personal data are hardly processed. This means it often respects privacy. That does not mean, however, that it respects safeguards, in the sense that mistrial and abuse are more effectively avoided.

This ordinal scale has 5 points of magnitude, ranging from a very small to a very high, where comparatively speaking many safeguards are in place. What qualifies as very high is the level of safeguards offered in legal trials. The results are summarized in table 13.3.

As said, very high is the standard of actual court cases. They are present in several cases, for example in the final stage of HADOPI and in the court cases in the US (when targeting end users directly or associated with 'Operation in Our Sites'). Similarly, in Spain a judge could mandate the removal of websites, through the Ley Sinde procedure.

A high level of safeguards was offered in those procedures that still had a large amount of legal review in their process. For example, the Ley Sinde procedure allowed for 'voluntary takedowns' after a commission on intellectual property was involved. Although this was not a judge, the parties were notified and heard before a decision was taken. In the UK, judges could be involved in the final stage when users were targeted directly. Default judgements have been issued against end users, which did not allow for an actual hearing. These judgements were issues because defendants had not responded to the settlement request.

A medium level of safeguards was offered in the seizures of 'Operation in Our Sites': a magistrate judge was involved before websites were seized. The party whose website was seized was not heard or notified directly, however. A similar level of safeguards was offered in the Eircom disconnections. There was no judicial review in the process. The review takes place by Eircom employees and it is unclear how they apply the law. A similar level is offered

in Notice and takedown in the Netherlands: no judge is involved. The ISPs implementing the procedure are incentivized, via liability assignment, to judge in the favor of notifiers.

A low level of safeguards was offered in the settlement letters in the US and the UK. A judge was involved in the process, but only to guarantee some level of privacy. Most other safeguards were missing.

A very low level of safeguards is offered in the Google search delisting requests and the warnings by Eircom and HADOPI. There are hardly any safeguards, especially in the case of the warnings. Google search has introduced some limited safeguards through the transparency report and by using market force as a way to stimulate safe reporting. Similarly, YouTube employs a Content ID program that functions as an automated system.

Case	Subcase	Safeguards	Qualification
Targeting end users directly (US)			
	Settlement letter	Some ISPs forwarded the settlement requests to users, without the interference of a judge, while in other cases the judge was involved only in the process of early discovery and joinder. That remained the only involvement, unless the procedure led to a trial. Settlement requests were however designed in a way to discourage court cases. The burden of proof therefore rested heavily on the accused. Although users were sent a notice, this was already the settlement request. Technically there was a right to be heard or appeal, but that was discouraged because it could lead to high costs. Accused parties had unequal access to defenses. There was little transparency and the punishments were not proportional.	Low
	Court case	This is an adversarial trial with a judge and a hearing. The punishments were not proportional.	Very high
Targeting end users directly (UK)			
	Settlement letter	The judge is only involved to grant the Norwich Pharmacal order to allow law firms to get contact details. The judge was only involved to grant the Norwich Pharmacal order to get contact details. This involvement was limited. The burden of proof therefore rested heavily on the accused. The letters were phrased in a way to push defendants to settle. Although users were sent a notice,	Low

		this was already the settlement request. Technically there was a right to be heard or appeal, but that was made very unattractive. Accused parties had unequal access to defenses. Regarding transparency, there was little to none. The punishments were not proportional.	
	Court case	In the default judgements, no hearing was held.	High
HADOPI graduated response (France)			
	1 st warning	Regarding privacy, infringement was only found through over the top surveillance: by joining P2P networks. Although there was a rights protection committee that administered the warning phase, accusations were hardly checked for accuracy. Users were further found to be infringing by negligence, which also undermined the presumption of innocence. The warning was a first notice but it already had consequences. There was a right to be heard and appeal after this notice, however it was unclear how well these defenses were evaluated by the rights protection committee, considering their sheer number. Transparency happened through public reports, although it is unclear how HADOPI applied the law.	Very low
	2 nd warning	Similar to the above	Very low
	Court case	This is an adversarial trial with a judge and a hearing. Regarding proportionality, the disconnection penalty was eventually removed in favor of smaller fines.	Very high
Eircom graduated response (Ireland)			
	1 st warning	Regarding privacy, infringement was only found through over the top surveillance: by joining P2P networks. It was a privately administered sanctioning procedure, so there appeared to be no judge and it was unclear how accusations were checked or how the system is further applied. For the first two phases, the procedure was automated. The	Very low

		warning was a first notice but it already had consequences. There was a right to be heard and appeal. However, it was how well these defenses were evaluated by the Eircom employees. There was no transparency.	
	2 nd warning	Similar to the above	Very low
	7-day suspension	It is a privately administered sanctioning procedure, so there appears to be no judge and it is unclear how accusations are checked or how the system is further applied. There is a right to be heard and appeal. However, it remains unclear how well these defenses are evaluated by the Eircom employees. There is no transparency.	Medium
	12-month suspension	It is a privately administered sanctioning procedure, so there appears to be no judge and it is unclear how accusations are checked or how the system is further applied. There is a right to be heard and appeal. However, it remains unclear how well these defenses are evaluated by the Eircom employees. There is no transparency. The disconnection penalty was considered disproportional by multiple parties.	Medium
NTD at Google/YouTube			
	NTD Google Search	Spotting infringement in the program at Google required web crawling and taking the content down, and no processing of personal data. The system was privately administered, and parties did not take responsibility for takedowns. Accusations were hardly checked and biased towards the complainant. There was appeal but it took place after the delisting. There was no right to be heard. Regarding transparency, Google released a report that described some of the links which have been delisted, all the complainants and additional data. It was proportional.	Very low
	TCRP	In addition to the above, Google had introduced a separate large-scale	Very low

		takedown program for trusted complainants, who would be able to submit more notices that were not reviewed for accuracy but created additional safeguards by rewarding reputation: parties could lose their status of trusted complainant if they made too many mistakes.	
	NTD YouTube	For YouTube personal data was processed as infringement related back to an individual Google account. The takedown system was privately administered and biased towards the complainant. There was no chance to be heard, and appeal was possible only after the takedown. There was little transparency. Some have argued that it was disproportional.	Very low
	Content ID	For YouTube personal data was processed as infringement related back to an individual Google account. The takedown system was privately administered and biased towards the complainant. There was no chance to be heard, and appeal was possible only after the takedown. There was little transparency. Some have argued that it was disproportional.	Very low
NTD in the Netherlands			
	NTD NL ISPs	<p>Although it was difficult to evaluate the performance of different ISPs, ISPs claimed to check the accusations individually, and to ask notifiers to contact the alleged infringer. This would allow alleged infringers to be notified and to present their views. Some ISPs also offered the possibility of appeal. Regarding transparency, some providers lacked clear information about how they applied notice and takedown. There was also limited information on how it had been applied in the past. Regarding proportionality, there could have been some burden on free speech.</p> <p>Previously done experiments suggested that safeguards were less present in smaller providers. This research could not verify those claims,</p>	Medium

		although some of those experiments were done in a similar timeframe. They highlighted a lack of competence, no clear privacy protection and little transparency.	
	NTD Leaseweb trusted removal program	In addition to the above, Leaseweb had introduced a separate large-scale takedown program for trusted complainants, who would be able to submit more notices that were not reviewed for accuracy but created additional safeguards by rewarding reputation: parties could lose their status of trusted complainant if they made too many mistakes.	Medium
Operation 'In Our Sites' (USA)			
	Seizure	These websites were found through web crawling and research. A magistrate judge checked probable cause and there could be a trial after the sanction. Although the burden of proof was on the government, for seizures only probable cause had to be established. There were defenses and a right to be heard only after the seizure. Transparency was difficult in some cases, but the affidavit could be made public afterwards. Many argued that because the seizures lacked safeguards and affected entire domains, this strategy was disproportional.	Medium
	Forfeiture	This is an adversarial trial with a judge and a hearing.	Very high
	Personal trial	This is an adversarial trial with a judge and a hearing.	Very high
Ley SINDE (Spain)			
	Voluntary removal	Regarding safeguards, there appeared to be privacy protection because infringement was found through web crawling and research, but sometimes contact details could be requested for additional proceedings. This was protected by a judge. It was not clear if the commission that verified claims was completely impartial or independent because it had no members with a consumer rights background. Regarding a presumption	High

		of innocence, the procedure allowed website owners to submit their views. They were notified, and had the right to be heard and access to defenses and appeal. The procedure was not transparent, and appeared to be proportional.	
	Judge mandated removal	In addition to the above, there was a judge in a later phase.	Very high

Table 13.3: *qualifying the cases for safeguards.*

Comparison

In order to discuss the overall patterns in the variables across the 22 sanctioning mechanisms, we visually plot all mechanisms along the three dimensions: scale, severity and safeguards. Of course, plotting qualitative data in a graph is rather tricky. As none of the measures can be exact, I use an ordinal scale to display the variables for all sanctioning mechanisms, i.e., subcases. The graph has been divided into cells to make it more readable. Placement of the subcases in each cell in the graph is just for space purposes. Each bubble is to be read as simply belonging to that cell. The exact position in a cell, to the left or to the right, has no meaning. Also, some subcases score similarly on the variables. At times, two subcases have been represented by a single bubble, their names separated by a slash. Figure 13.1 displays the final result.

As the figure shows, there is a clear pattern in the relation between scale and safeguards. The subcases that scale up better have fewer safeguards. Think of the HADOPI warning letters and notice and takedown applied by Google. Similarly, for the sanctioning mechanisms that did not scale up well we found more safeguards, like court cases. The figure also suggests a relation between severe sanctions and scale: more severe sanctions did not scale up.

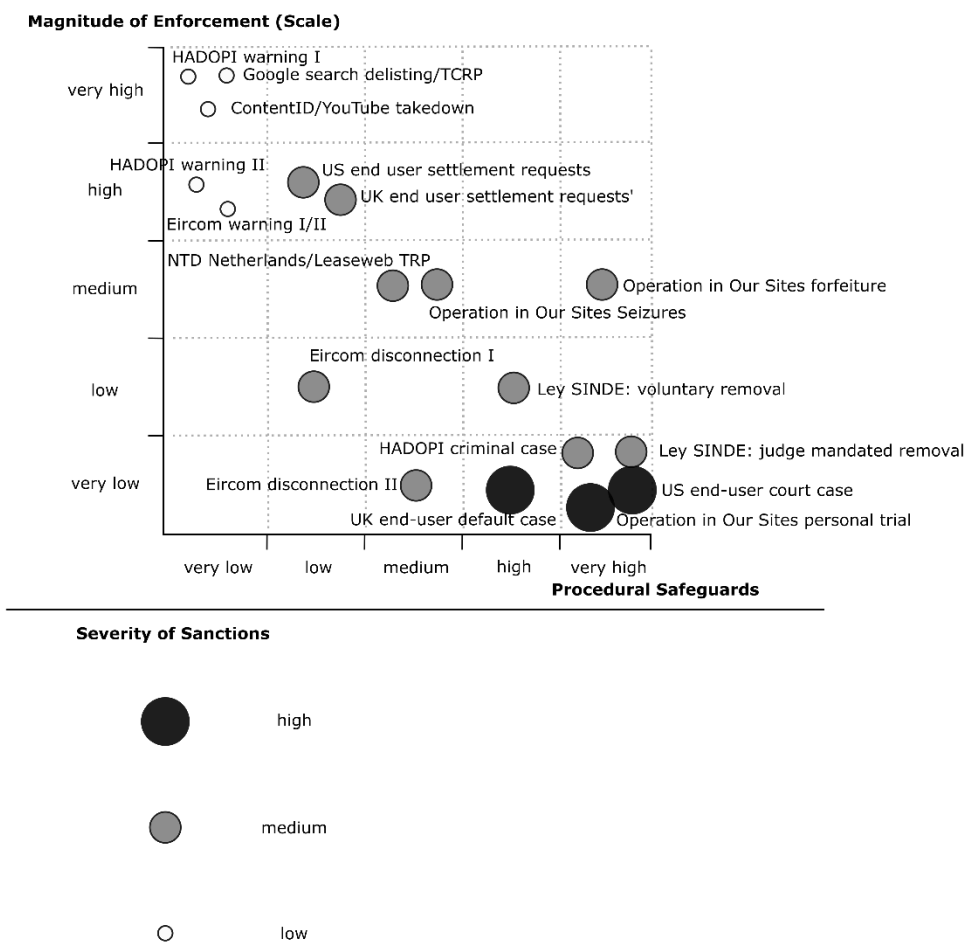


Figure 13.1: Graph that presents scale, severity and procedural safeguards for each subcase. For space purposes, some subcases are represented as one bubble, their names separated by a slash.

13.3 Scale comes at the cost of safeguards

The comparison of the 22 sanctioning mechanisms (Figure 13.1) shows a clear negative relationship: the larger the scale of the enforcement, the fewer the procedural safeguards. This relation is also visible within the cases. This is consistent with the economic model of enforcement proposed by Becker. Having more safeguards prevents innocent persons from being punished. However, the theory predicted that those rules of the game make the cost of apprehending and convicting a given percentage of offenders much higher and that therefore, in enforcement procedures that do scale up, safeguards will be reduced. In the case studies, this trade-off is already visible in the cases where enforcement does not even scale up that much.

In the cases where rights holders target demand directly for example, fewer safeguards were provided. In both the US and the UK, scaling up enforcement was only possible through a procedure that relied on settlement requests. Lawyers and rights holders found cheaper ways to target multiple people at once, without actually going through trial. Scaling up was achieved, by taking judges out of the procedure for most of the process. With them, most of the safeguards were also removed. However, this scale was still bounded by constraints: it was limited to infringement of the specific source material they represented, and by jurisdictional issues.

In the US, over 200,000 people in total have been targeted with copyright claims by only a small number of firms. Cases rarely made it to court and were designed to make people settle for smaller amounts of money, often hundreds to thousands of dollars. Although judges checked the discovery process, their review did not extend to the merits of the copyright claim. This meant there was little to no presumption of innocence, and rights holders and their representatives were the judges of their own cause, without a hearing. There was hardly an equality of parties, as citizens are incentivized to settle to prevent legal costs or a higher sanction. Although there was a possibility of appeal, it was made unattractive because it is in many cases more expensive than settling. The procedures were also not transparent. For some law firms it was impossible to determine how many letters have been sent to citizens.

In the interviews, the direct relation between scale and safeguards was also apparent. One lawyer said that sending large-scale settlement letters was a way to keep litigation costs low. He also said that when judges started preventing cases from being joined, this strategy became economically unfeasible. He added that providing more evidence than is done in the discovery phase was possible and could prove infringement, but was economically unfeasible.

One judge mentioned that she put separate mechanisms in place to guarantee safeguards, but that they were voluntary and put a severe burden on her office. This also confirms the link between safeguards and scale.

In the UK, law firms sent out thousands of settlement requests to end users. The law firms sent letters asking for a relatively small amount of money, usually hundreds of pounds. Although a judge checked the application to get personal details on infringers, he or she made no decision on the merits of the case. There was little presumption of innocence, and rights holders and their representatives were the judges of their own cause, without a hearing. Although there was a possibility of appeal, it was made unattractive because it was in many cases more expensive than settling. There was also no transparency – in fact, the lawyers tried to prevent transparency. Lawyers explicitly mention in their letters that due to the number of people they wrote, they cannot get into evidence. They also stated that they wanted to make sure it was more like an expensive parking ticket to maximize recovery of funds.

In these two cases, where rights holders targeted the demand side directly, the scale already showed a tradeoff between scale and safeguards. This tradeoff is even more apparent in the cases where demand and supply are targeted indirectly. For example, in both studied graduated response procedures, scaling up was mainly achieved through automation and by taking the judges out of the process in the first two stages of the procedure. Both procedures took place on an enormous scale: for example 9% of the total population has received a warning in France. HADOPI sent out millions of first warnings. Thousands of second warnings were sent out. They were automated, so there was no judge

or manual review involved. This meant that complaints by rights holders were taken at face value and there was no neutral adjudication of those complaints, no presumption of innocence and no hearing. The CNIL also confirmed that it would be impossible to check the accuracy of the first strikes, because of their high number. Subscribers could however appeal. There was some transparency as the HADOPI authority sent out reports on its functioning.

For Eircom, the procedure was kept much more in the dark. It was privately administered and it was unclear how sanctions are applied. Thousands of subscribers were warned. Like in the case of HADOPI, the first phases were automated, so accuracy checks, if any, were limited. This meant that complaints by rights holders were also mostly taken at face value, without neutral adjudication of those complaints and without a presumption of innocence or hearing. Subscribers could however appeal, but because the procedure was not transparent, it is unclear how this appeal worked and whether the later phases in the process allowed for safeguards.

Both cases showed a clear link between scale and safeguards. This link was also apparent in the way DtecNet finds infringement. They stated to only use human validation in high profile cases or in a high profile environment, while they automate all other cases.

One could argue that these graduated response procedures focus their attention on P2P platforms, which were predominantly used for infringement. The question remains whether this is enough to prevent mistrial or abuse.

The other indirect enforcement procedure that scaled up targeted supply. Procedures like notice and takedown allowed rights holders to take down millions of links from Google search, but offered no judicial scrutiny. To handle a scale that allows millions of search results removed, Google created a trusted removal system, which was largely automated. The majority of takedowns came from these trusted complainants. As a new safeguard, they based this system on the reputation of the complainant. If trusted complainants failed to perform well, they would be removed from the program. As those complainants had a financial incentive to stay in, this system rewarded a certain diligence on their part. Within the system, the rights holders did not have to go through the entire process that requires them to provide specific evidence of their claim. This made it scale efficiently for those enforcement vendors. One of those enforcement vendors is DtecNet. As mentioned before, they only use human validation in high profile cases or high profile environments.

Although this procedure involved many different actors, it was interesting that no party took responsibility for takedowns. Google said the responsibility was with rights holders, while the parties reporting the infringement all said they themselves did not take anything down.

In the procedure, there were incentives for Google to judge in favor of a claimant, because they could otherwise lose safe harbor protection. It is questionable whether there was a presumption of innocence, and there was no notice sent to the content provider, or a hearing before the sanction was applied. Only at the initiative and costs of sanctioned parties, could there be judicial checking and only after the sanction. Google introduced a bit of transparency by releasing a transparency report each year which detailed the amount of takedowns and different parties involved.

At YouTube, there was also an automated system called Content ID, which applied to millions of videos. The safeguards offered were similar to those at Google Search: partners allowed Google to scan for their content. Also, YouTube did not have a transparency report.

In the Netherlands, rights holders complained that notice and takedown was too burdensome because of the evidence requirements. Leaseweb used a trusted complainants system for notice and takedown comparable to what Google did with search. Notice and takedown took place on a moderate scale, especially for hosting providers.

Both cases show that for notice and takedown scaling up was achieved, but at the cost of procedural safeguards. It is interesting that parties have created new forms of safeguards in these procedures. Google has chosen to provide some level of transparency through their transparency reports in relation to search, while both Google and Leaseweb have created a takedown system with ‘trusted complainants’. This system also rewarded reputation to discourage mistrial and abuse.

Because scaling up was achieved more easily in those indirect procedures, it also shows that rights holders have been able to avoid procedural safeguards by making non-judicial players, like intermediaries, the sanctioning party. Traditionally, due process, fair trial, and other provisions that safeguard judicial performance and prevent wrongful punishments, are codified in laws and human rights. So relaxing them through private procedures creates a tension with the formal law.

In the cases where users were targeted directly, judges still played a minor role, but in the case of notice and takedown, intermediaries were notified of infringement and legally pressured to enforce. They faced liability if they did not. Instead of a judge, it was the intermediary evaluating the claims of infringement. In the cases of graduated response, the cooperation of intermediaries was required. In France this required governmental pressure, and in Ireland the ISP Eircom was initially sued to get them to cooperate with the system.

Although targeting demand directly (‘Operation in Our Sites’ and the SINDE procedure) did not scale up that well, those cases already showed tradeoffs with procedural safeguards.

This means the cases confirm the theoretical predictions – and also the warnings of the opponents of increased online copyright enforcement. When the number of sanctions is scaled up, this comes at the cost of procedural safeguards. Meanwhile, some actors have created new safeguards for large-scale procedures, but it is uncertain to what extent they suffice to prevent mistrial or abuse.

13.4 Severity and scale do not mix

Some strategies also increase the severity of the sanctions involved. The research shows, however, that when sanctions got more severe, the sanctioning mechanism never achieved scale. For example, taking down websites with the SINDE procedure in Spain or through ‘Operation in Our Sites’ in the US led to a more severe sanction -- taking down a complete website and business – but it was only executed against limited numbers of websites.

One could call this a reassuring finding. The pattern is consistent with the relationship between safeguards and scale. In other words, severity and safeguards have remained closely related: high severity sanctions are only found in sanctioning mechanisms with a high level of safeguards.

Research by Mathur revealed that the more severe the punishment is for a particular crime, the lesser it is probable that the criminal will be punished. This might be based on the fact that for harsher crimes, judges might be more hesitant to award severe punishments,

for example in cases of the death penalty.¹⁹³⁴ Severe penalties are more sensitive. Errors would bring about higher social costs, so it would make sense that society would invest more to prevent those social costs for higher penalties, and create more safeguards for more severe crimes.

In the US, 'Operation in Our Sites' led to the seizure of thousands of sites. They required a criminal investigation, but those seizures in first instance only required probable cause, which meant sanctioning could take place before trial with lower standards of evidence than would be the case in an ordinary court. During the Superbowl, for example, the procedure required scale and speed to make sure people would not stream the event. This could explain why some safeguards were stripped, like the right to challenge the seizure before it took place.

The reports submitted for the investigation were quite extensive, but the procedure still seems tilted towards the government side, in terms of safeguards. Site owners were notified, but after some time. They had little means to challenge the seizure, and had to prove their innocence only after already being sanctioned. Also, the US government has not been particularly transparent about the procedure, shrouding some of it in secrecy. The site owners had their entire business confiscated by the Federal government and a criminal investigation against their business, which is a severe sanction.

In Spain, the procedure created by the Sinde law allowed for similar severe sanctions, because complete websites were taken down or blocked. Apart from that, additional sanctions were possible, like criminally investigating the website owner. However, just as theory predicts, it has only been applied on a limited scale, reaching only a couple of hundred cases in two years. This procedure did allow for a lot of safeguards: there was a commission adjudicating (although it was not as independent as the judiciary), and some role for the judiciary too. The burden of proof was on the rights holders, and alleged infringers had the right to be heard and protest. There was little transparency.

The links between severity and scale were even clearer in the interviews and the reports by different actors. Although faster than regular lawsuits, IIPA blames government inaction and calls the process agonizingly slow. One reason for the small number of sanctions is that every more severe sanction is accompanied by more safeguards. 'Operation in Our Sites' required a complete criminal investigation. The SINDE procedure required an investigation, and allowed suspected infringers the chance to comment on allegations. The other cases confirm this relation between safeguards and severity. For example, in the cases where users were targeted directly, the relatively few times that cases actually made it to court, the sanctions were very severe. In the US, they ranged in the hundreds of thousands of dollars.¹⁹³⁵

Similarly, in France, the public authority HADOPI sent out millions of warnings to citizens, but only got a handful of sanctions (fines or a suspension of Internet access) ruled upon by the courts. This third phase took place on a much smaller scale, but guaranteed the full safeguards through a trial. The constitutional court said the procedure required safeguards in the disconnection phase because of the severity of the penalty. The sanction in that phase was much more severe than the disconnection phase at Eircom: originally it was disconnection coupled with the subscription fee, but has recently been lowered to fines of a

¹⁹³⁴ Vijay Mathur, "Economics of crime: an investigation of the deterrent hypothesis for urban areas," *the review of economics and statistics* 60.3 (1978), 459-466. P.465.

¹⁹³⁵ Electronic Frontier Foundation, *RIAA v The People: Five years later* (2008). 5. and: Eric Bangeman, "RIAA Trial Verdict Is In: Jury Finds Thomas Liable for Infringement," *Ars Technica* (October 4, 2007).

maximum of 1.500 Euros. One wonders how the legal system would handle more third strikes.

This means the cases confirmed the theoretical predictions. The enforcement strategies either scale up the probability of sanctions, or increase the severity of penalties, but not both.

13.5 Economic costs of increased enforcement

The cost of enforcement strategies is an important consideration to evaluate the policy options. Theoretically, Becker makes two observations with regard to enforcement policy and criminal activities: obedience is not taken for granted, and public and private resources are spent to prevent offenses and apprehend offenders. The main question in Becker's article is "how many resources and how much punishment should be used to enforce different kinds of legislation?"¹⁹³⁶

The goal of enforcement is to achieve a degree of compliance with a rule or prescribed behavior that society believes it can afford. Enforcement can be costly. The extent to which laws are enforced depends on resources devoted to that task. Because of this cost limitation, it is impossible to detect and punish all offenders. Offenders are deterred by expected punishments, which are (broadly speaking) the probability times the severity of the punishment.¹⁹³⁷ The more significant the offense, the more likely society will want to use resources to prevent the offense. This does not necessarily mean that more resources will make punishment more severe, but it means that the offender will be pursued more 'tenaciously' to increase the probability of apprehension.¹⁹³⁸

This research showed that there are different costs to take into consideration for copyright enforcement. First of all, there were costs borne by the rights holders themselves. In principle, this is a private decision based on private cost and benefits, not an issue of public policy. Rights holders have the freedom to spend what they deem sufficient to enforce their rights.

Second, there are the institutional costs on courts. When private rights are infringed, there is an institutional infrastructure to correct this. This is part of the rule of law. That being said, it still is relevant to consider the magnitude of these costs. Copyright enforcement competes for the resources of the court system with other transgressions and disputes. The burden on courts affects the whole of society.

Third, there are the costs for law enforcement by public institutions, such as criminal investigations by police units or administrative sanctioning mechanisms like HADOPI. If we as a society decide that violating certain norms and laws should not go unpunished, it has consequences for the allocation of public resources. This, too, is part of the rule of law.

Fourth, there are cost borne by those who need to defend themselves against the threat or application of a sanction. This can range from the cost of legal defense in a court case all the way to the cost of having to protect online speech or business from unwarranted takedown actions.

¹⁹³⁶ Gary Becker, "Crime and Punishment: an Economic approach," *The Journal of Political Economy* 76.2 (1968), 169-217. P.169.

¹⁹³⁷ George Stigler, "The Optimum Enforcement of Laws," in: *Essays in the Economics of Crime and Punishment*, ed. Gary Becker and William Landes, (1974), 55-67. P.56.

¹⁹³⁸ Stigler, "The Optimum Enforcement of Laws," P.57-58.

Fifth, and last, there are costs imposed on third parties. The large-scale enforcement efforts that rely on intermediaries, such as ISPs, de facto externalize part of the enforcement cost to those intermediaries. One could argue that this is simply the cost of doing business. ISPs are shielded from liability only when they do act if they are notified of infringement. Irrespective of whether these costs are seen as legitimate, it is relevant to include these costs into the overall picture and to realize that some of the enforcement costs are not borne by the rights holders nor the public institutions.

The case studies have found that cost has been a critical consideration for the enforcement strategies of rights holders. For example, targeting users directly in the US (and in the UK) have been expensive for rights holders. The earlier lawsuits as enacted by the RIAA were expensive and litigation was not able to recover the costs through the fines awarded by courts and the settlements paid by infringing users.

However, smaller firms were able to actually create economic returns. They sought efficiency through joinder and early discovery, which means defendants were grouped at court first and that the remaining costs were simply sending out letters and building an infrastructure for collection. Putting cases together also saved the courts money. Discovery required lower standards of evidence, which was also cheaper for rights holders. However, because courts later became more opposed to joining too many defendants at once and granting discovery, the litigation became more economically difficult.

In the UK, costs were a major driver for this enforcement strategy to focus on achieving early settlements. The lawyers referred to it as a cost effective method because most cases would settle early on and that it needed to be an expensive parking ticket to maximize recovery. They also mentioned that they needed to send enough letters to make the strategy economically viable. However, one law firm stopped for financial reasons, since not enough people were reached and those that were settled less often. Another firm did make money but was forced to shut down. The procedure relied on grouping defendants in one case at one court to be economically viable, and this ran into resistance at the courts.

Other strategies relied on law enforcement. The cases that target supply directly for example required extra investment. In the US, the FBI and Customs department worked together on seizing websites. Several judges were involved, as were lawyers representing the government interest.

Similarly, the SINDE law procedure required tax payer money, the exact amount is unknown, to finance an administrative authority tasked with fighting infringement. It also burdened, to a small extent, the judicial system. Rights holders still faced costs, they had to spot infringement themselves, and presumably hired private agencies to do this. The IIPA however thought that the government needed to allocate more resources to this procedure to make it more effective.

The graduated response procedure in France also relied on a new administrative authority financed by tax payers. When people cite the HADOPI procedure as a relatively cheap way to enforce copyrights, they mean cheap for rights holders.¹⁹³⁹ There were still high costs. Rights holders hired TMG to monitor Internet traffic and notify HADOPI. HADOPI itself had a budget ranging in the millions funded by the state, ISPs needed systems to identify subscribers and send them infringement notices. Subscribers might end up paying

¹⁹³⁹ Alain Strowel, "The 'Graduated Response' in France: Is It the Good Reply to Online Copyright Infringement." in: *Copyright Enforcement and the Internet*, ed. Stamatoudi (Kluwer Law International, The Netherlands, 2010). P. 153.

these costs. Furthermore there were judicial and administrative costs.¹⁹⁴⁰ Another potential cost that could be taken into account is that subscribers could be forced to pay by installing means to secure their connections.

There has been debate on whether the procedure was too expensive for taxpayers to fund. Most notably, the Lescure report that evaluated the HADOPI law mentioned that “the focus of public funds on the prevention of P2P downloading is the result of a bad prioritization and an inadequate allocation of resources.”¹⁹⁴¹ It concluded “that it does not appear desirable to maintain an independent administrative authority whose activity is limited to combating illegal downloading. This would contribute neither to the lawfulness of the provision, nor to the coherence of state activity, nor to the saving of public funds.”¹⁹⁴² This would be especially pressing if the system would only marginally benefit authors, as some academics argued.¹⁹⁴³

Similar to HADOPI, other cases also showed how rights holders distributed costs to third parties. Notice and takedown, for example, placed part of the enforcement burden on platform owners, because they had to establish procedures and thus absorb some of the costs of enforcement. In this case, it meant that Google had to invest in enforcement as well.¹⁹⁴⁴

According to Google, they had hundreds of people working on what they referred to as “anti-piracy.” They say it is “not a trivial cost.” These costs stem from developing innovative technology, as well as from the people hired to work on this. They also thought that for cost reasons, smaller ISPs had no choice but to simply accept notices.¹⁹⁴⁵ Rights holders had substantial costs as well. They have to hire or finance anti-piracy organizations or independent enforcement vendors, with specific business models tailored to the needs of rights holders. Other researchers confirmed that there was some burden on ISPs, and that enforcement costs were especially burdensome for smaller providers.¹⁹⁴⁶

IRMA specifically opted for the graduated response procedure at Eircom as opposed to lawsuits, calling those a “waste of resources.” Because there was no administrative or judicial authority involved, costs in this procedure were much lower. IRMA paid DtecNet to scan Internet traffic for infringement. IRMA in turn needed an enforcement department to build dossiers on IP addresses, and to send notices to Eircom. Eircom needed an infrastructure to identify IP addresses, and to send out warnings. However, they themselves said that technology was already in place for things like child pornography. Another cost could be the potential competitive disadvantage of having to enforce this against their own subscribers, who might flock to other ISPs, but this effect could not be confirmed.

¹⁹⁴⁰ Internet Society, Perspectives on Policy Responses to Online Copyright Infringement, an Evolving Policy Landscape," *Internet Society website* (Feb 20, 2011) P.47, <http://www.Internetsociety.org/perspectives-policy-responses-online-copyright-infringement-evolving-policy-landscape>

¹⁹⁴¹ Pierre Lescure, *Mission « Acte II de l'exception culturelle » Contribution aux politiques culturelles à l'ère numérique*, Ministère de la Culture et de la Communication (May 2013) P.33., www.culturecommunication.gouv.fr/var/culture/storage/culture_mag/rapport_lescure/index.htm#/1

¹⁹⁴² Pierre Lescure, *Mission « Acte II de l'exception culturelle » Contribution aux politiques culturelles à l'ère numérique*, Ministère de la Culture et de la Communication (May 2013) P.33., www.culturecommunication.gouv.fr/var/culture/storage/culture_mag/rapport_lescure/index.htm#/1

¹⁹⁴³ Geiger, "Challenges for the Enforcement of Copyright in the Online World," P.10.

¹⁹⁴⁴ Jennifer Urban and Laura Quilter, "Efficient Process or 'Chilling Effects'? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act," *Santa Clara Computer and High Technology Law Journal* 22 (2006): 621. P. 636.

¹⁹⁴⁵ Fred von Lohmann (Intellectual Property Director Google) interviewed by author, August 2013.

¹⁹⁴⁶ Urban and Quilter, "Efficient Process or 'Chilling Effects'?" P. 636.

All in all, the findings show that the total costs of enforcement have risen. This should be no surprise, as infringement has risen as well. This means that more cost are borne by society as a whole, since the large-scale strategies allocate a significant portion of the cost to public entities (by increasing the role of the state), third parties (by getting them to enforce against infringers) and the recipients of the sanctions (who might have to defend themselves against claims of infringement).

This allocation of cost points to an incentive problem caused by the misalignment of private and social cost and benefits. The benefits of enforcement of their private rights flow to the rights holders, but a significant portion of the costs are carried by others. This provides an incentive to rights holders to initiate or demand more enforcement than would be the case if they carried most of the costs themselves.

One could argue that tax payers should carry these costs, as it does for law enforcement in general. This is a fair point, but it does not solve the incentive problem and it does not tell us anything about how high the cost to taxpayers, or third parties, should be. Clearly there is a limit, as there is for enforcement of any crime. This is not an empirical question, but a normative and political one. Part of any such evaluation of the appropriate level of cost on society is to look at what public values are being advanced by these enforcement strategies: the protection of cultural production. This brings us to the next question: did it actually work? Was infringement reduced or cultural production stimulated by the large-scale enforcement strategies.

13.6 Enforcement has had little impact at its current scale

The available studies on the different enforcement initiatives show that, overall, large-scale copyright enforcement has had little impact on infringement levels. Although rights holders and governments intensified enforcement, few of the strategies examined in the cases have had an observable and lasting deterrent effect on large-scale infringement.

The graduated response procedures suggest that there were some deterrent effects on a particular type of infringement (see chapters 7 and 8), while targeted end users directly had no observable effect (see chapters 5 and 6). The notice and takedown procedures are deemed successful, but it is unsure if they have a lasting deterrent effect on infringement (see chapters 9 and 10). There is no evidence that the strategies that target supply directly had an observable effect (chapters 11 and 12). A more in depth description will now follow.

Strategies that mainly relied on increasing scale had some effects, but only in limited ways. Graduated response procedure combine warnings applied on an incredible scale with potentially more severe sanctions later on a very small scale, which could explain their limited success. In France HADOPI scaled up enforcement massively. As the first graduated response procedure and partly funded by the French taxpayers, it was the subject of a lot of discussion and studies with contradicting conclusions. Those studies have been discussed in chapter 7. Overall, it seems that HADOPI has had some deterrent effects on P2P file sharing. The strongest indicator seems to be the ever decreasing amount of warnings sent out, although Giblin points out that this might be for other reasons. At the same time, other forms of file sharing rose up, and there has been no increase in sales. Also, it is uncertain whether file sharers moved towards ways to hide their P2P file sharing. There is also a lot of variation in figures cited by the authority itself.

Graduated response in Ireland is difficult to evaluate. After its implementation, things have remained quiet on the effect of Eircom's graduated response procedure on

infringement. As the procedure is privately administered, the relevant stakeholders were able to shroud the procedure and its effects in relative mystery. In an interview, IRMA suggested that the amount of notifications decreased with each phase (few people receive a second warning, even fewer receive a third warning). This would suggest the procedure is effective. However, just like in the case of HADOPI, it might simply reflect the fact that users deploy encryption and proxies to better hide their actions or that they move to non-P2P alternatives for downloading infringing content.

For the other strategies that managed to scale up, there is little evidence to suggest that infringement levels have gone down in response. After a period of targeting users directly in the US, P2P related infringement remained relatively stable. Also, it appeared these procedures were slowly being abandoned. They not only faced heavy resistance by the public, but have also received repeated criticism and opposition from judges who made it more difficult for rights holders and law firms to engage in these practices. At first there seemed to be some deterrent effect, but decreased file sharing bounced back after some time.

The UK paints a similar picture: targeting end users directly has not been an effective deterrent. Although it appeared to have been intended as a profitable business for smaller, more specific rights holders, infringement numbers were not affected, and remained relatively high. Here too, the procedure came under close scrutiny of the courts, and the public eye. Three lawyers were suspended from practicing law and ordered to pay a fine for breaching the solicitors code of conduct. Although other law firms have since picked up the process, it appears as if courts have since created more requirements before those firms can start sending letters.

Targeting supply indirectly scaled up massively, but it remains questionable to what extent it was a real deterrent. According to the anti piracy authority Brein, notice and takedown in the Netherlands “works.” They however suggest that they have not been able to bring down infringement in the Netherlands enough, because a lot of content is currently hosted on foreign servers.

In the case of Google search, the question remains whether fewer users found their way to infringing content because of removed search results. The company itself claims that the engine does not seem to be a major driver of infringement, and provides some evidence for this.

In the case of YouTube, notice and takedown does not play a big role as rights holders have moved to agreements with Google to monetize their content through the ContentID system. Under this system rights holders have been paid large amounts of money, but it remains unclear to what extent it has worked as a deterrent.

Strategies that mainly relied on increasing severity have not reduced infringement. Although qualified as medium in the summary of the case results, targeting supply directly was done with increased severity, as opposed to the strategies that scaled up massively. The Immigrations and Customs Enforcement (ICE) of the US government targeted sites directly through that offered pirated products. The majority of enforcement focused on trademarks. With regards to copyright, it is difficult to determine whether or not this had a substantial effect on infringement. The enforcement actions intended to fight live streaming, and links sites. For those types of sites, research suggests that effects were limited to none.

The SINDE law in Spain too has had limited effects on infringement, and seems to have worked as a slower notice and takedown procedure, with more safeguards. The IIPA said that the agonizingly slow procedure offered little to deter the infringement. After

repeated criticism from rights holders, Spain moved forward with additional enforcement procedures that further increases severity to make up for this perceived inadequacy.

In sum, the case studies found little visible deterrent effect. I will briefly touch on several other initiatives of rights holders, though strictly speaking outside of the scope of this study. Even there, no demonstrable proof can be found that enforcement has a deterrent effect on infringement.

In the US, larger rights holders, like the RIAA, abandoned targeting users directly and have since moved towards a graduated response system. They themselves claimed it was an effective deterrent.¹⁹⁴⁷ However, a film consortium spoke out against the system, saying it was ineffective as a deterrent.¹⁹⁴⁸ Research suggested that 45% of Americans still actively pirated media.¹⁹⁴⁹ Also, this system does not include the pornography industry, one of the biggest drivers of targeting users directly. For smaller firms, it might therefore still be interesting to use this procedure, not as a deterrent, but as a way to retrieve funds. One wonders however, to what extent judges will thwart this process.

Some authors suggest that there have been better results in other countries. For example, some say enforcement of the EU IPRED directive in Sweden in 2009, caused a 27% increase in CD sales, and a 48% increase in digital music sales in Sweden.¹⁹⁵⁰ In Germany, each year hundreds of thousands of file sharers were sent letters by law firms requesting copyright payments for illegal downloading. In 2011 half a million of those letters were sent, in 2012 about 250,000 were sent out. Although the internet is abundant with warnings not to share files in Germany,¹⁹⁵¹ no research has confirmed that it has been an effective deterrent. Research suggests that 46% of Germans still actively pirate media.¹⁹⁵² A new law has dramatically lowered the possible maximum fines that law firms can ask for copyright infringement.¹⁹⁵³ The idea behind that legislative change is to protect consumers.¹⁹⁵⁴

Enforcement actions aimed at cyber lockers have not been very effective, research suggests. The researchers claim the supply is too distributed to take down, located too globally, and that taking down a specific service is not enough to disrupt the piracy ecosystem.¹⁹⁵⁵ In Germany, taking down streaming sites had little effect. "The existence of alternative sources of unlicensed consumption, coupled with the rapid emergence of new

¹⁹⁴⁷ "CCI Provides First Copyright Alert System Progress Report Highlighting Initial Accomplishments," Press release, Center for Copyright Information (May 28, 2014), <http://www.copyrightinformation.org/press-release/cci-provides-first-copyright-alert-system-progress-report-highlighting-initial-accomplishments/>

¹⁹⁴⁸ Martin Anderson, "Film consortium urges ISPs to abandon ineffective 'six strikes' policy for pirates," *The Stack* (May 13, 2015), <http://thestack.com/Internet-security-task-force-six-strikes-130515>.

¹⁹⁴⁹ Joe Karaganis and Lennart Renkema, "Copy culture in the US & Germany," *the American Assembly* (2013)

¹⁹⁵⁰ Brett Danaher, Michael D. Smith, and Rahul Telang, "Piracy and Copyright Enforcement Mechanisms" (May 2013), forthcoming in: *Innovation Policy and the Economy*, volume 14, ed. Lerner and Stern, (University of Chicago Press, Chicago, Illinois). P. 29.

¹⁹⁵¹ A simple Google search on "file sharing in Germany" suffices to see that it is actively discouraged for fear of consequences.

¹⁹⁵² Joe Karaganis and Lennart Renkema, "Copy culture in the US & Germany," *the American Assembly* (2013).

¹⁹⁵³ Michael Filtz, "File-sharing in Germany: Could the cost of getting caught be about to come down?," *ZDNet* (August 9, 2013), <http://www.zdnet.com/file-sharing-in-germany-could-the-cost-of-getting-caught-be-about-to-come-down-7000018915/>.

¹⁹⁵⁴ Andy, "Germany passes law to mitigate copyright trolling 'fines'," *Torrentfreak* (July 3, 2013), <https://torrentfreak.com/germany-passes-law-to-mitigate-copyright-trolling-fines-130703/>.

¹⁹⁵⁵ Tobias Lauinger et al., "Clickonomics: Determining the Effect of Anti-Piracy Measures for One-Click Hosting," Presentation at the NDSS Symposium (2013), http://www.Internetsociety.org/sites/default/files/07_1_0.pdf

platforms, led the streaming piracy market to quickly recover from the intervention and to limited substitution into licensed consumption.”¹⁹⁵⁶

In short: in chapter 2, we discussed that the levels of infringement have remained stable worldwide, and that the case studies show enforcement procedures have limited effects on infringement, if any. For some enforcement procedures, there may have been a limited effect. Graduated response procedures seemed to impact P2P infringement. This might be because the system combines a large scale in the first phase with a severe sanction in a later phase, or it might just be a false signal and merely express the shift of users to encryption and file sharing outside of P2P.

The research shows that scaling up enforcement directed to end users directly or indirectly could have some effect at bringing infringement down. However, bringing it down further, would mean that scale should be increased further, possibly in combination with severity. Before concluding with the discussion on the implications of these results, the following section will highlight the limitations of this study.

13.7 Limitations

Research is always subject to certain limitations that have to be taken into account when evaluating the findings. This study is no exception.

First, there are limitations inherent in the empirical scope of the study. Data collection was performed within a specific timeframe in a limited number of countries. Information has been collected for 22 sanctioning mechanisms related to 8 enforcement strategies in 6 countries implemented between 2004 and 2014. We found clear patterns in the dataset, but we should also be modest when generalizing beyond the dataset. Our findings seem to reflect general mechanisms that are likely also present in other countries where the rule of law provides similar protections and safeguards to citizens and businesses. Countries where the rule of law is institutionalized differently are likely to display different patterns.

A related limitation in scope is time. The data was collected until 2014. It is hard to evaluate to what extent the relationships that were found will remain to hold over time. New technologies are likely to emerge that impact the variables of this study. Perhaps they enable new enforcement procedures that reduce the painful tradeoff between scale, severity and safeguards. Think of algorithmic decision making and the rise of ‘Big Data’. Future research could explore whether procedural values could be implemented in a technological way, as some scholars are doing.¹⁹⁵⁷ This also means studying the effectiveness and ethics of algorithmic governance. While the future might hold many surprises, we should also note that the relationships found in this study, as theorized by legal economics, have held up in many domains over many decades.

Second, there are limitations in data collection because of the politicized nature of copyright enforcement. The study had to deal with the fact that some stakeholders saw it in their best interest to decline to be interviewed. Chapter 4 shows how this issue of selection bias was mitigated. It seems very unlikely that rights holders possess evidence that would

¹⁹⁵⁶ Luis Aguiar, Jörg Claussen, Christian Peukert, “Online Copyright Enforcement, Consumer Behavior, and Market Structure”, *European Commission joint research centre* (2015), see: <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/online-copyright-enforcement-consumer-behavior-and-market-structure>

¹⁹⁵⁷ Danielle Keats Citron, “Technological Due Process,” *Washington University Law Review* 85 (2008): 1249.

substantially change the findings of this study, since they would have a strong incentive to make that evidence public. That being said, it would have been better if their views would have been more directly represented.

Third, there are the inevitable limitations of condensing complex realities into a single comparative framework. This can be clearly seen in measuring the variables. They are qualitative in nature and therefore subject to interpretation and to limitations. For example, the problem with effectiveness is that for most of the studies on enforcement it is unclear how high infringement levels would be without those specific enforcement procedures. There is also no telling what the situation will be in years. Programs might work out in the long term or might erode, as many are now based on observing Torrent users, and Torrent is diminishing in importance as a facilitating technology for infringement. It is also unclear to what extent infringement has flocked to private channels. For scale there are some other problems. It is not just limited to the nature of the procedure. It also is tied to who are actually enforcing, and the money they are willing to spend on enforcement. Regarding costs, some of the costs are not known, because the private companies refused to provide insight. This means that some of the cases and variables were difficult to isolate and ascertain, while for some it is unclear how they influence the conclusions.

A fourth limitation is that the study cannot neatly separate and isolate the many interacting factors. It remains difficult to isolate specific enforcement procedures from others, so as to measure their specific effects. Countries do not enact just one copyright enforcement procedure, but multiple strategies at the same time. In the US for example, there are lawsuits, notice and takedown procedures, criminal investigations and more taking place. It is difficult to make an isolated evaluation of the deterrent effect of each procedure without considering some spillover effects. One way to extend research in this field is to isolate effects via policy and natural experiments, and by having country-specific studies of the combined effect of enforcement procedures.

Fifth, there are limitations related to the theoretical framework. The study has employed a specific framework from legal economics. Of course, there are other valuable perspectives. For example, there has been research into the swiftness of responses. Davis writes that there is a temporal factor to deterrence. Lowering the expected time until detection increases the benefits of crime. That is more than just scale.¹⁹⁵⁸ Other factors not taken into account are differences in wealth between individuals. People with more wealth might not be deterred quickly by fines. They also have more safeguards, as it will be easier for them to carry the burden of extensive legal representation. This was left out of this study to retain a feasible scope, but also because none of the enforcement procedures specifically aim for a timely response, except for 'Operation in Our Sites.' In that case, no additional effectiveness was observed. This study also does not include theories about the moral choices of people. For example, in research it was revealed that people that go to church are less likely to commit crimes,¹⁹⁵⁹ and that people whose peers commit crimes are more likely to do so.¹⁹⁶⁰ The study also does not take into account non-rational models of infringement behavior, such as rules of thumb, rules of information, habitual behavior, behavior that is emotionally motivated or impulsive behavior, etc. One could argue that all these behaviors

¹⁹⁵⁸ Michael Davis, "Time and Punishment: An Intertemporal Model of Crime," *Journal of Political Economy*, 96.21 (1988), 383-390.

¹⁹⁵⁹ See for example: Byron Johnson, *More God, Less Crime* (Templeton Press, 2011).

¹⁹⁶⁰ Anne Case and Lawrence F. Katz, "The company you keep: The effects of family and neighborhood on disadvantaged youths," *National Bureau of Economic Research* No. w3705. (1991).

may still be influenced by rational calculations. The rational actor approach has argued that the consequences of a change of policy may still be best predicted by sticking to the rational actor methodology. In other words: "the average aggregate behavior changes as if people were rational."¹⁹⁶¹ That being said, it might very well be that strategies using those theories from social psychology or the increasingly popular behavioral economics could help improve deterrence. For example, in the current study the perception of risk is not taken into account. People can download from the comfort of their own home, which might influence the way they perceive their risk of getting caught. On the other hand, sending warnings might influence risk perception and explain why graduated response procedures show some effects. Similarly, this study does not look at the role of social norms in legal compliance. A study by Svensson and Larsson researched the perceived gap between those social norms and copyright law. They conducted a survey on the attitudes of respondents between 15 and 25 to file sharing before and after the implementation of the IPRED law which aimed to increase enforcement in Sweden. The authors concluded that although file sharing behaviour had decreased in frequency after implementation of the law, social norms remained unaffected. The limited effect was attributed to some deterrence. The authors write that people more generally abide by informal social control than the law, and that the law has little chance of bringing about legal compliance without the support of social norms. They said people largely ignored the new copyright law, in similar ways like they did with traffic laws or tax laws. The authors also wrote that if compliance was only based on deterrence, and not on social norms, there could be negative consequences, like a lack of public confidence in the law and that counter measures may arise, like increased anonymization. Although the authors said that it did not necessarily have to be the case that there had to be a complete correspondence between social norms and the law, there should be some foothold in the public debate. They showed that since the implementation of the law, the gap between norms and the law had not diminished.¹⁹⁶² Because my study focuses on deterrence, the research by Svensson and Larsson could supplement this. It might explain why there have been little deterrent effects found in copyright enforcement thus far.

A final limitation is that the study has focused only one one path – copyright enforcement – to achieve two incredibly complex public policy goals: to stimulate cultural production and guarantee access to culture by the public. To fully understand the policy ramifications of the findings, one also needs to look at alternative paths. Future studies should look towards the effectiveness and costs (both social and economic) of other ways to attain those similar public policy goals, without necessarily favoring copyright in its current form as the legal instrument. The last part of the previous section, on the policy implications of this study, already hinted at relevant alternatives.

In sum, there are practical, empirical and theoretical limitations that have to be taken into account when interpreting the findings of this study. Future work will be able to overcome some of these limitations. This should not prevent anyone from taking seriously the robust empirical patterns that have been uncovered in the course of this research.

¹⁹⁶¹ Stephan Panther, "The economics of crime and criminal law: An antithesis to sociological theories?." *European Journal of Law and Economics* 2.4 (1995): 365-378. P.367.

¹⁹⁶² Måns Svensson and Stefan Larsson, "Intellectual property law compliance in Europe: Illegal file sharing and the role of social norms," *New media & society* 14.7 (2012): 1147-1163.

13.8 Implications for policy

This research has set out to determine whether an empirical relationship exists between scale, severity and safeguards. These insights can guide policymakers by more clearly showing the policy choices they face in this domain.

We have empirically corroborated the prediction of legal economics: copyright enforcement procedures were able to scale-up only by offering fewer procedural safeguards to sanctioned parties. Similarly, procedures that impacted on a larger scale provided less severe sanctions. The research has also shown that infringement levels remained by and large unchanged, and that enforcement procedures created substantial costs, a significant portion of which were externalized to the state and to third parties.

What do these findings imply for public policy on copyright enforcement? Thinking about enforcement from within the legal economics framework, we can boil down the discussion on policy implications to three key questions.

1. How can we make enforcement more effective?
2. Can we mitigate the negative side effects of intensified enforcement?
3. Are there alternatives to intensified enforcement?

This research provides guidance to answer these questions, although many things remain unclear.

How could we make enforcement more effective?

The status quo turned out to be rather disappointing for everyone: society bore significant cost and side-effects of more large-scale enforcement, without getting much in return in terms of effectiveness. The strategies have not been very successful at bringing down infringement levels. In most cases, even the rights holders expressed their discontent about the current situation.

In response, the discussion has shifted towards defining what “effective” means exactly. In the Netherlands, for example, Brein has said that they wanted to bring infringement down to 25%. RIAA has stated that it appreciates the “educational” aspect of graduated response, since hardcore downloaders might never be deterred.

Others argue that “effective” could also mean that, even when infringement levels are undeterred, enforcement benefits new business models or stimulates a vibrant entertainment market. It is unclear whether this effect occurs in practice. Assuming that HADOPI, for example, effectively reduces illegal P2P sharing, has this created a better market for the entertainment and cultural sector? If settlement letters would work, would they stimulate the movie industry?

As was noted in the Introduction of this dissertation, it remains unclear how copyright infringement has impacted the market for entertainment. Critics and academics argue and demonstrate that the revenue streams have merely shifted, for example from recordings to live performances, and that overall the market is still vibrant. Others claim that infringement threatens diversity. This empirical question is outside the scope of this dissertation. Future work will have to create more clarity on these impacts.

When we return to the original, and still dominant, enforcement goal of bringing infringement levels down, our theory and empirical evidence point to two basic options: further increase scale and further increase severity.

For each of the new enforcement strategies, achieving scale was accompanied by fewer safeguards, especially when compared to the safeguards offered in a conventional civil

court case. This strongly suggests that scaling up further will be possible only by removing even more safeguards. This can generate serious societal costs, as safeguards protect the rule of law, human rights like free speech and privacy, innovation and the careful balance copyright strikes between protected content and other content or content available for fair use. Countless examples show mistrial and abuse happen in the field of copyright. This is exactly what makes copyright enforcement procedures controversial.

The second option is to increase the severity of the sanction imposed on infringers. Some enforcement procedures are controversial because in comparison to the perceived damage done by infringement, the sanctions are perceived as disproportionate. A classic example, here, is the case of Capitol Records vs. Jammie Thomas-Rasset. The woman was ordered to pay \$220,000 for sharing 24 songs via KaZaA. Such sanctions caused resistance by the general public. Rights holders already face a difficult situation because there is little public support for enforcement, and more severity will exacerbate this problem.

Apart from the societal impacts associated with larger scale and higher severity, any intensification of enforcement will also impose further economic costs on the state, a.k.a., the tax payers, and third parties.

What does this mean for policy makers? The large-scale enforcement efforts of the past decade have led to a problematic status quo. If the cases we studied are any guide then further intensifying enforcement strategies—i.e., increasing scale, severity, or both—would very likely increase the negative impacts of enforcement, with uncertain results in terms of reduced infringement. Is that worth it?

To some extent, this question is already being answered in practice. Some of the strategies that have been proposed to increase severity and scale up further have already become highly controversial. Politics has intervened and stopped SOPA and the judiciary put limits on speculative invoicing in the UK. In Germany large-scale lawsuits without judicial interference were corrected by the legislator by lowering the penalties involved. Also, the ultimate sanction in HADOPI has been reduced. Meanwhile, judges and lawmakers aim to put an end to the large-scale targeting of end-users through settlement requests in the US.

Can we mitigate the negative side effects of more enforcement?

Would there be any way to increase scale and severity of sanctioning while also retaining or even increasing the procedural safeguards? Our comparative analysis of 22 sanctioning mechanisms suggest that this is extremely difficult. The only countervailing examples are the modest new safeguards that some of the new procedures have introduced. Think of Google's transparency report, for example. Systems based on reputation and increased transparency might improve the balance. It is questionable, however, whether these safeguards are sufficient to prevent mistrial and abuse. The question for policy makers is then whether we should accept these negative impacts.

Where safeguards are protected and their cost are borne by the rights holders, the rights holders themselves have been unwilling to scale up because they find it too costly. This is most visible in the court cases targeting end users directly. We found ample evidence that rights holders have largely abandoned these procedures because of their cost. In other words, the rights holders themselves were not willing to spend their money on scaling up enforcement while retaining safeguards. This raises the inevitable question: if rights holders, who reap the potential benefits of more effective enforcement, are not willing to shoulder these costs, then why should the state, tax payer or third parties be asked to carry them?

*Are there alternatives?*¹⁹⁶³

Legal economics suggest examining different legal regimes to attain economic objectives. Coase, who paved the way for legal economics, proposed what Hazlett, Porter, and Smith call a “symmetric evaluation of resource appropriation rules.” He argued that negative externalities or damaging spillovers (like copyright infringement) were not proof of market failure, but should be taken into account as regular input costs. That view allows us to see the problem from a viewpoint of institutional symmetry. Instead of assuming some theoretical ideal of a perfect functioning government and market failure, multiple approaches should be tested and evaluated in empirical and economic terms, to see which approach is the most efficient.¹⁹⁶⁴

If we view copyright infringement as an economic problem, what alternatives to deterrence exist? A number of authors have suggested alternative ways to regulate culture. Alternative approaches range from decriminalization of socially or economically less harmful practices, to legalization, and state regulated compensation schemes in the form of world licenses.¹⁹⁶⁵

Some suggest a tax. According to Landes and Lichtman, this could be a tax “applicable to particular tools, services, venues associated with copyright infringement. As long as the tax would non-trivially increase the incentive to create and disseminate copyrighted work, and the tax itself would not discourage legitimate behavior.”¹⁹⁶⁶

The central idea of these compensations is to reward rights holders for the unauthorized use of copyright works.¹⁹⁶⁷ Different scholars have argued for different ways to implement this. Some suggest levies on Internet subscription,¹⁹⁶⁸ which is similar to copying levies in European countries. Others suggest a tax.^{1969 1970} They are an extension of collective rights management, which is a longstanding practice in parts of the market for copyright works.¹⁹⁷¹

These levies are also under criticism. One of the problems is the concept of harm. Levies can lead to double payment, especially when tied to private copying. Some say the harms from private copying are too small.¹⁹⁷² Furthermore, levies restrict price setting and can lead to a misallocation of resources. They also require copyright management organizations. This is costly, they may be slow, or become incredibly powerful. They would also have to determine actual use.¹⁹⁷³

¹⁹⁶³ Part of this Section was previously published as Floris Kreiken & David Koepsell, “Coase and Copyright,” *University of Illinois Journal of Law, Technology and Policy* 1 (2013): 1-44.

¹⁹⁶⁴ Thomas W. Hazlett et al., “Radio Spectrum and the Disruptive Clarity of Ronald Coase,” *Journal of Law & Economics* 54.21 (2011): S125. S137.

¹⁹⁶⁵ Geiger, “Challenges for the Enforcement of Copyright in the Online World,” P.17.

¹⁹⁶⁶ Lichtman and Landes, “Indirect liability for copyright infringement: an economic perspective.” P.406.

¹⁹⁶⁷ Christian Handke, Bodo Balazs, Joan-Josep Vallbé, “The value of online licenses for recorded music,” *Paper presented at Annual Congress of the Society for Economic Research on Copyright Issues*, (2014). P.3, and: William Fisher, *Promises to keep: Technology, law, and the future of entertainment*, (Stanford University Press, 2004).

¹⁹⁶⁸ Neil Weinstock Netanel, “Impose a noncommercial use levy to allow free peer-to-peer file sharing.” As published in *Harvard Journal of Law & Technology* 17 (2003): 2-84.

¹⁹⁶⁹ William Fisher, *Promises to keep: Technology, law, and the future of entertainment*, (Stanford University Press, 2004).

¹⁹⁷⁰ Handke, Balazs, Vallbé, “The value of online licenses for recorded music,” *Paper*. P.3.

¹⁹⁷¹ Handke, Balazs, Vallbé, “The value of online licenses for recorded music,” *Paper*. P. 3.

¹⁹⁷² Joost Poort and João Pedro Quintais, “The Levy Runs Dry: A Legal and Economic Analysis of EU Private Copying Levies,” *4 Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 205 (2013). P. 205-206.

¹⁹⁷³ Handke, Balazs, Vallbé, “The value of online licenses for recorded music,” *Paper*. P. 3-4.

Some have evaluated a theoretical compensation system for recorded music. It would grant private Internet subscribers the right to download and use works in return for a fee. According to their model, this would be welfare increasing in the current market conditions. The fee is based on a (very low) price consumers are willing to pay, and would increase rights holders revenue as well. They would propose a mandatory fee that lies between 1.74 and 9.25 Euros.¹⁹⁷⁴

Some authors point towards new business models as an inspiration for new rights. One way would be to abandon the property model and move towards different models. This is more in line with business models currently on the rise, like Netflix and Spotify. This means that vendors would pay for the right to give access to culture to the public, and still compensate rights holders for their work.

These new business models allow for remuneration to creators, and are warmly embraced by the public.¹⁹⁷⁵ They demonstrate the growing power of a new form of intermediaries, like Apple and Amazon, which provide access to content for consumers.¹⁹⁷⁶ Those intermediaries themselves make agreements with rights holders to provide remuneration and access to consumers at the same time, through private contract law.¹⁹⁷⁷ These intermediaries reap the benefits of the new infrastructure economically, but do not rely on the exclusivity of their product to receive remuneration.¹⁹⁷⁸ They recognize that content is a *service* made possible through unique and valued forms of access, rather than relying on the exchange of tokens protected by state monopolies.¹⁹⁷⁹

In a changing market that revolves around access, intermediaries will compete over access rights by offering remuneration to creators. Recently, this can already be observed by the way Tidal has taken on Spotify by claiming to better deals for creators. At the same time, those intermediaries will compete with each other by offering content to consumers. Some intermediaries might be more popular by offering better quality to consumers, and some intermediaries might be more popular to creators by offering better marketing or a better price to creators.

For those access rights to work, copyrights should focus on limiting unfair competition or “competitive harm.”¹⁹⁸⁰ So intermediaries that have not bargained with other intermediaries for the spread of content and seek to benefit from it financially would potentially be liable for copyright infringement. This would make copyright as it was again: reserved for the big fish, not the little ones.

In summary, policymakers should give equal weight to legislative alternatives that might better guarantee economic incentives in the entertainment market and access to culture for the public.

¹⁹⁷⁴ Handke, Balazs, Vallbé, “The value of online licenses for recorded music,” *Paper*. P.1-2.

¹⁹⁷⁵ Wendy Bernfeld, “Brave New World: Digital Distribution Beyond the Old World,” *Sundance Institute* (Apr. 23, 2012, 9:04 PM), <http://www.sundance.org/artistservices/distribution/article/brave-new-world-digital-distribution-beyond-the-old-world/>

¹⁹⁷⁶ Bernfeld, “Brave New World: Digital Distribution Beyond the Old World.”

¹⁹⁷⁷ Bernfeld, “Brave New World: Digital Distribution Beyond the Old World.”

¹⁹⁷⁸ Bernfeld, “Brave New World: Digital Distribution Beyond the Old World.”

¹⁹⁷⁹ Bernfeld, “Brave New World: Digital Distribution Beyond the Old World.”

¹⁹⁸⁰ Stadler, “Copyright as Trade Regulation,” P.912.

SUMMARY

The Internet has been a disruptive force in many markets, among them the markets for entertainment and cultural products. New Internet-based technologies have undermined the protection of copyright on these products. Copyright is a legal tool which was devised to incentivize cultural production and to facilitate access to culture by the public. New information technologies have facilitated large-scale copyright infringement. The exact effect on the entertainment market is unclear. The market is adapting to these changes and seems to be doing well in some areas, and worse in others.

Rights holders, however, view infringement as unequivocally illegal, wrong and harmful. They have sought increased enforcement of copyright via gaining more control over the technologies through which their content is distributed. A key problem that rights holders are trying to solve is scale. Since infringement is widespread, enforcement efforts also need to impact at a large scale. Dealing with each case of infringement via the standard civil law procedures is very costly in terms of time and money. Therefore, rights holders have adopted new strategies to scale up enforcement online, which in some cases involve intermediaries or the government in their application.

To deal with these difficulties and with large-scale infringement, rights holders have adopted new strategies to scale up enforcement, which can be categorized into four groups: (1) they target the demand for infringing content (end-users) directly on a large scale by aiming for settlements instead of actual lawsuits. (2) They target end-users indirectly through intermediaries that apply graduated response procedures. These procedures use a system of increasingly severe sanctions for each infringement to deter users, often starting with a warning letter and ending with Internet disconnection or fines as the ultimate sanction if infringement keeps happening. These procedures require intermediaries in the administration of sanctions. (3) They target the supply side directly by taking down or filtering websites that offer infringing content. Governmental parties often carry out these procedures. (4) They target the supply side indirectly by asking intermediaries to take action against infringing content. Notice and takedown procedures allow rights holders to notify websites of infringement and require them to take this content down.

Few people defend infringement, but there are concerns that these new enforcement strategies are disproportionately costly to society. Technologists, academics and civil society organizations, like the Electronic Frontier Foundation, argue that that scaled-up enforcement will be bad for human rights and other public values because it erodes procedural safeguards, most notably due process and fair trial. Fewer safeguards would give too much control over Internet services, and even Internet access, to rights holders. In a nutshell, the argument is that if rights holders can unilaterally decide what is right or wrong because of lacking judicial scrutiny, then this will be bad for free speech, the rule of law, and innovation.

Proponents of intensified enforcement point to the cost of infringement, which they estimate to be in the billions. They claim this demands more effective enforcement. Rights holders, White House and EU representatives also claim large-scale enforcement can be done in accordance with human rights. According to representatives of the rights holders, such as the Movie Picture Association of America (MPAA) and the US Chamber of Commerce, SOPA and ACTA follow the same rules of civil procedure you would find in an

ordinary trial. In their view, copyright enforcement targets illegal sites and people that infringe on copyright only and does nothing to harm legal uses of content and Internet users who are not sharing protected content.

Who is right? What is the actual impact of the new enforcement strategies on legal safeguards and, more broadly, on public values? There has been a lack of empirical research to answer this question. This dissertation set out to overcome this gap by providing the first comparative empirical analysis of new enforcement strategies. Its core research question is: *“How does large-scale copyright enforcement on the Internet influence procedural safeguards like due process and fair trial, what are its costs and its effectiveness, and what do these findings imply for public policy?”*

Legal economics predicts a certain level of effectiveness of enforcement: effective deterrence requires large-scale enforcement and more severe sanctions in order to increase the costs of breaking the law. Increasing the scale of enforcement, hence increasing the chance of getting caught, is particularly effective. These theories also describe that scaling up enforcement is costly and that it is often associated with reduced procedural safeguards, because legal procedures are time consuming and expensive. When this tradeoff between scale and safeguards also applies to copyright enforcement, then the consequences can be serious for human rights and public values.

Next to increasing scale, effectiveness could also be increased through more severe sanctions. How is severity associated with procedural safeguards? If consequences of punishments are more severe, then the lack of procedural safeguards is more likely to lead to more severe wrongful sanctions and a more negative societal impact.

To empirically study the relationship between scale, severity and safeguards in online copyright enforcement, we analyzed 22 sanctioning mechanisms that belong to eight enforcement strategies in six countries between 2004 and 2014. Each enforcement strategy is a case study. We looked at what is known about its impact on infringement levels and its costs. Within each strategy, there can be multiple sanctioning mechanisms. We studied these as subcases, where we identified the scale at which they were executed, the severity of the sanctions, and the safeguards provided to the actors on which the sanctions are imposed.

The research shows that rights holders were able to scale up enforcement in some strategies, and that in these cases, scale came at the cost of procedural safeguards. Procedures like notice and takedown for example, allowed rights holders to take down millions of links from Google search, but only because judicial scrutiny had been removed. Only at the initiative and costs of sanctioned parties, could there be judicial checking and only after the sanction. Rightsholders have been able to avoid legal safeguards by making non-judicial players, like intermediaries, the sanctioning party. In the case of notice and takedown, intermediaries were notified of infringement and legally pressured to enforce: they faced high fines if they did not. This trade-off between safeguards and scale is visible in every enforcement strategy analyzed. This means the cases confirm the theoretical predictions – and also the warnings of the opponents of increased online copyright enforcement. When the number of sanctions is scaled up, this comes at the cost of procedural safeguards. Meanwhile, some actors have created new safeguards for large-scale procedures, but it is uncertain to what extent they suffice to prevent mistrial or abuse.

Some strategies also increased the severity of the sanctions involved. The research shows, however, that when sanctions got more severe, the sanctioning mechanism never achieved scale. For example, taking down websites with the SINDE procedure in Spain or

through 'Operation in Our Sites' in the US led to a more severe sanction -- taking down a complete website and business -- but it was only executed against limited numbers of websites. Similarly, in France, the public authority HADOPI sent out millions of warnings to citizens, but only got a handful of sanctions (fines or a suspension of Internet access) ruled upon by the courts. This means the cases confirmed the theoretical predictions. The enforcement strategies either scale up the probability of sanctions, or increase the severity of penalties, but not both.

Figure A illustrates that in the 22 subcases corresponding to 8 enforcement strategies researched, there was a connection between scale, severity and safeguards. The subcases that scale up better have fewer safeguards. Think of the HADOPI warning letters and notice and takedown applied by Google. Similarly, for the sanctioning mechanisms that did not scale up well we found more safeguards, like court cases. The figure also suggests a relation between severe sanctions and scale: more severe sanctions did not scale up.

Of course, plotting qualitative data in a graph is rather tricky. As none of the measures can be exact, I use an ordinal scale to display the variables for all sanctioning mechanisms, i.e., subcases. The graph has been divided into cells to make it more readable. Placement of the subcases in each cell in the graph is just for space purposes. Each bubble is to be read as simply belonging to that cell. The exact position in a cell, to the left or to the right, has no meaning. Also, some subcases score similarly on the variables. At times, two subcases have been represented by a single bubble, their names separated by a slash.

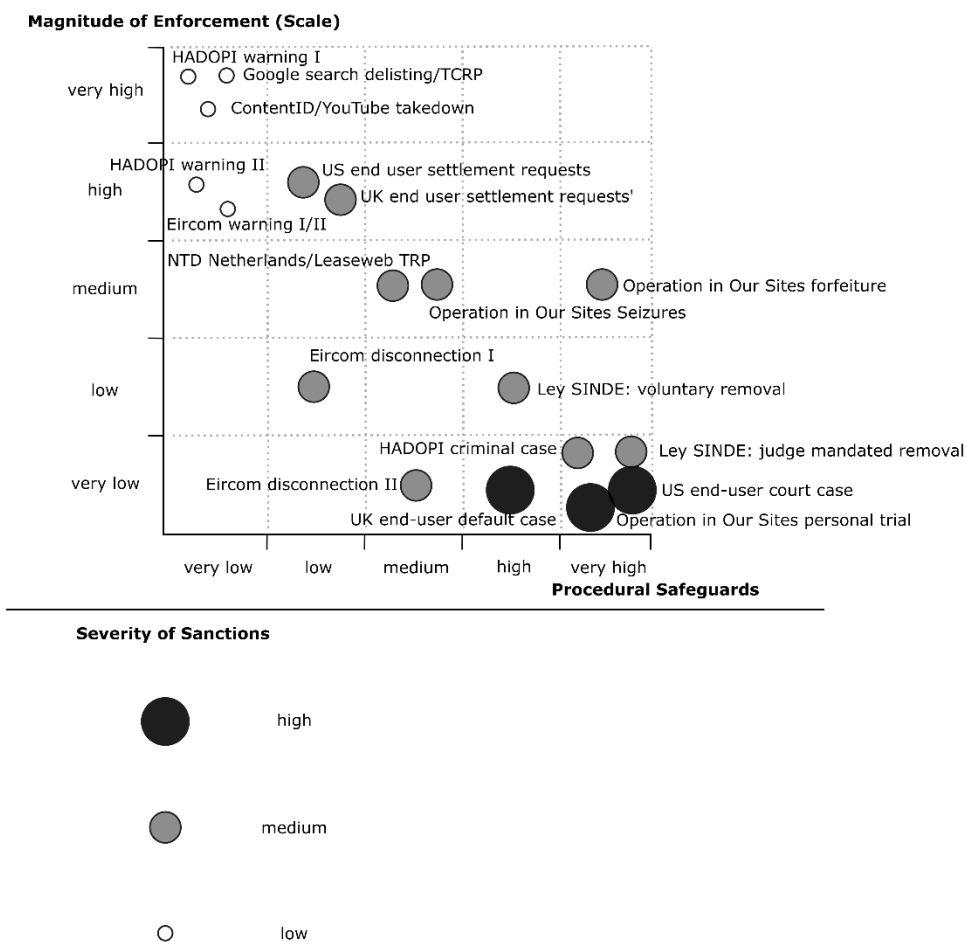


Figure A: Graph that presents scale, severity and procedural safeguards for each subcase. For space purposes, some subcases are represented as one bubble, their names separated by a slash.

This research showed that there are different costs to take into consideration for copyright enforcement: costs borne by the rights holders themselves, the institutional costs on courts, the costs for law enforcement by public institutions, costs borne by those who need to defend themselves against the threat or application of a sanction, and costs imposed on third parties.

All in all, the findings show that the total costs of enforcement have risen. This should be no surprise, as infringement has risen as well. This means that more cost are borne by society as a whole, since the large-scale strategies allocate a significant portion of the cost to public entities (by increasing the role of the state), third parties (by getting them to enforce against infringers) and the recipients of the sanctions (who might have to defend themselves against claims of infringement).

This allocation of cost points to an incentive problem caused by the misalignment of private and social cost and benefits. The benefits of enforcement of their private rights flow

to the rights holders, but a significant portion of the costs are carried by others. This provides an incentive to rights holders to initiate or demand more enforcement than would be the case if they carried most of the costs themselves.

The research also shows that almost none of the enforcement strategies brought infringement down permanently. The levels of infringement have remained stable worldwide, and the case studies show enforcement procedures have limited effects on infringement. Graduated response procedures seemed to impact P2P infringement. This might be because the system combines a large scale in the first phase with a severe sanction in a later phase, or it might just be a false signal and merely express the shift of users to encryption and file sharing outside of P2P.

This research has set out to determine whether an empirical relationship exists between scale, severity and safeguards. These insights can guide policymakers by more clearly showing the policy choices they face in this domain.

We have empirically corroborated the prediction of legal economics: copyright enforcement procedures are able to scale-up only by offering fewer procedural safeguards to sanctioned parties. Similarly, procedures that impact on a larger scale provide less severe sanctions. The research has also shown that infringement levels are by and large unchanged, and that enforcement procedures create substantial costs, a significant portion of which are externalized to the state and to third parties.

What do these findings imply for public policy on copyright enforcement? Thinking about enforcement from within the legal economics framework, we can boil down the discussion on policy implications to three key questions.

- (1) How can we make enforcement more effective?
- (2) Can we mitigate the negative side effects of intensified enforcement?
- (3) Are there alternatives to intensified enforcement?

This research provides guidance to answer these questions, although many things remain unclear.

How could we make enforcement more effective?

The status quo turned out to be rather disappointing for everyone: society bore significant costs and side-effects of more large-scale enforcement, without getting much in return in terms of effectiveness. The strategies have not been very successful at bringing down infringement levels. In most cases, even the rights holders expressed their discontent about the current situation.

Although there has been some discussion about what “effective” means, when we return to the original, and still dominant, enforcement goal of bringing infringement levels down, our theory and empirical evidence point to two basic options: further increase scale and further increase severity.

For each of the new enforcement strategies, achieving scale was accompanied by fewer safeguards, especially when compared to the safeguards offered in a conventional civil court case. This strongly suggests that scaling up further will be possible only by removing even more safeguards. This can generate serious societal costs, as safeguards protect the rule of law, human rights like free speech and privacy, innovation and the careful balance copyright strikes between protected content and unprotected content or content available for fair use. Countless examples show mistrial and abuse happen in the field of copyright. This is exactly what makes copyright enforcement procedures controversial.

The second option is to increase the severity of the sanction imposed on infringers. Some enforcement procedures are controversial because in comparison to the perceived damage done by infringement, the sanctions are perceived as disproportionate. A classic example, here, is the case of Capitol Records vs. Jammie Thomas-Rasset. The woman was ordered to pay \$220,000 for sharing 24 songs via KaZaA. Such sanctions caused resistance by the general public. Rights holders already face a difficult situation because there is little public support for enforcement, and more severity will exacerbate this problem.

Apart from the societal impacts associated with larger scale and higher severity, any intensification of enforcement will also impose further economic costs on the state, a.k.a., the tax payers, and third parties.

What does this mean for policy makers? The large-scale enforcement efforts of the past decade have led to a problematic status quo. If the cases we studied are any guide then further intensifying enforcement strategies—i.e., increasing scale, severity, or both—would very likely increase the negative impacts of enforcement, with uncertain results in terms of reduced infringement. Is that worth it?

To some extent, this question is already being answered in practice. Some of the strategies that have been proposed to increase severity and scale up further have already become highly controversial. Politics has intervened and stopped SOPA and the judiciary put limits on speculative invoicing in the UK. In Germany large-scale lawsuits without judicial interference were corrected by the legislator by lowering the penalties involved. Also, the ultimate sanction in HADOPI has been reduced. Meanwhile, judges and lawmakers aim to put an end to the large-scale targeting of end-users through settlement requests in the US.

Can we mitigate the negative side effects of more enforcement?

Would there be any way to increase scale and severity of sanctioning while also retaining or even increasing the procedural safeguards? Our comparative analysis of 22 sanctioning mechanisms suggest that this is extremely difficult. The only countervailing examples are the modest new safeguards that some of the new procedures have introduced. Think of Google's transparency report, for example. Systems based on reputation and increased transparency might improve the balance. It is questionable, however, whether these safeguards are sufficient to prevent mistrial and abuse. The question for policy makers is then whether we should accept these negative impacts.

Where safeguards are protected and their cost are borne by the rights holders, the rights holders themselves have been unwilling to scale up because they find it too costly. This is most visible in the court cases targeting end users directly. We found ample evidence that rights holders have largely abandoned these procedures because of their cost. In other words, the rights holders themselves were not willing to spend their money on scaling up enforcement while retaining safeguards. This raises the inevitable question: if rights holders, who reap the potential benefits of more effective enforcement, are not willing to shoulder these costs, then why should the state, tax payer or third parties be asked to carry them?

*Are there alternatives?*¹⁹⁸¹

So what is the alternative? We would have to reform copyright. Copyright is currently an exclusive property right, but large-scale infringement and the problems with enforcement show that this paradigm might be unfit for the information technology age. Using theories in

¹⁹⁸¹ Part of this Section was previously published as Floris Kreiken & David Koepsell, "Coase and Copyright," *University of Illinois Journal of Law, Technology and Policy* 1 (2013): 1-44.

legal economics, we can look for new ways to guarantee economic incentives in the entertainment market and access to culture for the public. One way would be to drop exclusivity and move towards an access right, which is more in line with business models currently on the rise (like Netflix and Spotify). This means that vendors would pay for the right to give access to culture to the public, and still compensate rights holders for their work. It would drastically drop the costs of enforcement, and the costs in the form of human rights violations.

SUMMARY IN DUTCH

Het internet is een ontwrichtende kracht geweest in vele markten, waaronder de markt voor entertainment en voor culturele producten. Nieuwe op het internet gebaseerde technologieën hebben de bescherming van het auteursrecht op deze producten ondermijnd. Auteursrecht is een juridisch instrument dat is ontwikkeld om culturele productie te stimuleren en om de toegang tot cultuur voor het publiek te verbeteren. Nieuwe informatietechnologieën hebben de grootschalige schending van het auteursrecht echter makkelijk gemaakt. Het precieze effect op de culturele markt is onduidelijk. De markt is zich aan deze veranderingen aan het aanpassen en lijkt het goed te doen op sommige gebieden, en slechter op andere.

Rechthebbenden zien inbreuken echter als onmiskenbaar illegaal, fout en schadelijk. Ze zochten daarom meer handhaving van het auteursrecht door meer controle te krijgen over de technologieën waarmee hun content wordt verspreid. Een belangrijk probleem dat rechthebbenden proberen op te lossen is schaal. Aangezien inbreuken op zo'n grote schaal plaats vinden, moet handhaving ook op een grote schaal toegepast worden. Het is echter zeer kostbaar in termen van tijd en geld om elke individuele inbreuk aan te pakken via de gebruikelijke civielrechtelijke procedures. Daarom hebben rechthebbenden nieuwe strategieën gevonden om handhaving online op te schalen, die in sommige gevallen voor hun toepassing afhankelijk zijn van tussenpersonen of de overheid.

Deze nieuwe strategieën kunnen worden onderverdeeld in vier groepen: (1) zij richten zich op grote schaal direct op de vraag naar inbreukmakende content (eindgebruikers) door zich met name te richten op schikkingen in plaats van daadwerkelijke rechtszaken. (2) Ze richten zich indirect op eindgebruikers via tussenpersonen die 'graduated response procedures' toepassen. Deze procedures maken gebruik van een systeem van steeds strengere sancties voor elke inbreuk om gebruikers af te schrikken, en beginnen vaak met een waarschuwingsbrief en eindigen met afsluiting van de internetconnectie of boetes als de ultieme sanctie indien inbreuken blijven plaats vinden. Deze procedures vereisen tussenpersonen in de toepassing van sancties. (3) Ze richten zich direct op de aanbodzijde door het afsluiten of het filteren van websites die inbreukmakende content aanbieden. Overheidspartijen voeren vaak deze procedures uit. (4) Ze richten zich indirect op de aanbodzijde door tussenpersonen te vragen op te treden tegen inbreukmakende content. 'Notice and takedown' procedures stellen rechthebbenden in staat websites op de hoogte te stellen van inbreuken en hen te verplichten om deze content neer te halen.

Weinig mensen verdedigen inbreuken, maar er zijn zorgen dat deze nieuwe handhaving strategieën onevenredig kostbaar zijn voor de samenleving. Technologen, wetenschappers en maatschappelijke organisaties, zoals de Electronic Frontier Foundation, beweren dat die opgeschaalde handhaving slecht zal zijn voor mensenrechten en andere publieke belangen, omdat het procedurele waarborgen als het recht op een eerlijk proces erodeert. Procedures met minder waarborgen zouden rechthebbenden te veel controle geven over internetdiensten en zelfs over toegang tot het internet. In een notendop is het argument dat als rechthebbenden eenzijdig kunnen beslissen wat goed of fout is omdat gerechtelijke controle ontbreekt, dat slecht zal zijn voor de vrijheid van meningsuiting, de rechtsstaat, en innovatie.

Voorstanders van intensievere handhaving wijzen op de kosten van al die inbreuken, die zij in de miljarden schatten. Ze beweren dat dit vraagt om effectievere handhaving. Rechthebbenden, het Witte Huis en EU-vertegenwoordigers beweren ook dat grootschalige handhaving kan worden toegepast in overeenstemming met de mensenrechten. Volgens vertegenwoordigers van de rechthebbenden, zoals de Movie Picture Association of America (MPAA) en de US Chamber of Commerce, hanteren handhavingsprocedures als SOPA en ACTA dezelfde procesregels als een reguliere rechtszaak. Naar hun mening richt handhaving van het auteursrecht zich op illegale sites en mensen die inbreuk maken op het auteursrecht, en doet zij niets om legaal gebruik van content of internet gebruikers die niets fout doen te schaden.

Wie heeft er gelijk? Wat is de werkelijke impact van de nieuwe handhaving strategieën op juridische waarborgen en, meer in het algemeen, op publieke belangen? Er is een gebrek aan empirisch onderzoek om deze vraag te beantwoorden. Dit proefschrift heeft tot doel deze leemte in onze kennis op te vullen met een eerste vergelijkende empirische analyse van nieuwe handhavingstrategieën. De onderzoeksvraag luidt: *"Hoe beïnvloed grootschalige handhaving van het auteursrecht op het internet procedurele waarborgen, zoals het recht op een eerlijk proces, wat zijn de kosten en de doeltreffendheid ervan, en wat betekenen deze bevindingen voor beleid?"*

Rechtseconomische theorieën voorspellen een zekere mate van effectiviteit van handhaving: effectieve afschrikking vereist grootschalige handhaving en strengere sancties om de kosten van het overtreden van de wet te vergroten. Het vergroten van de schaal van de handhaving, dus het verhogen van de pakkans, is in het bijzonder effectief. Deze theorieën beschrijven dat handhaving op grote schaal kostbaar is en dat het vaak samen gaat met verminderde procedurele waarborgen, omdat wettelijke procedures tijdrovend en duur zijn. Als deze uitruil tussen schaal en waarborgen ook geldt voor de handhaving van het auteursrecht, kunnen de gevolgen ernstig zijn voor de mensenrechten en publieke belangen.

Naast schaalvergroting, zou de effectiviteit ook kunnen worden verhoogd door zwaardere sancties. Wat is het verband tussen strafzwaarte en procedurele waarborgen? Als de gevolgen van straffen ernstiger zijn, kan het ontbreken van procedurele waarborgen leiden tot zwaardere onterechte sancties en een negatievere maatschappelijke impact.

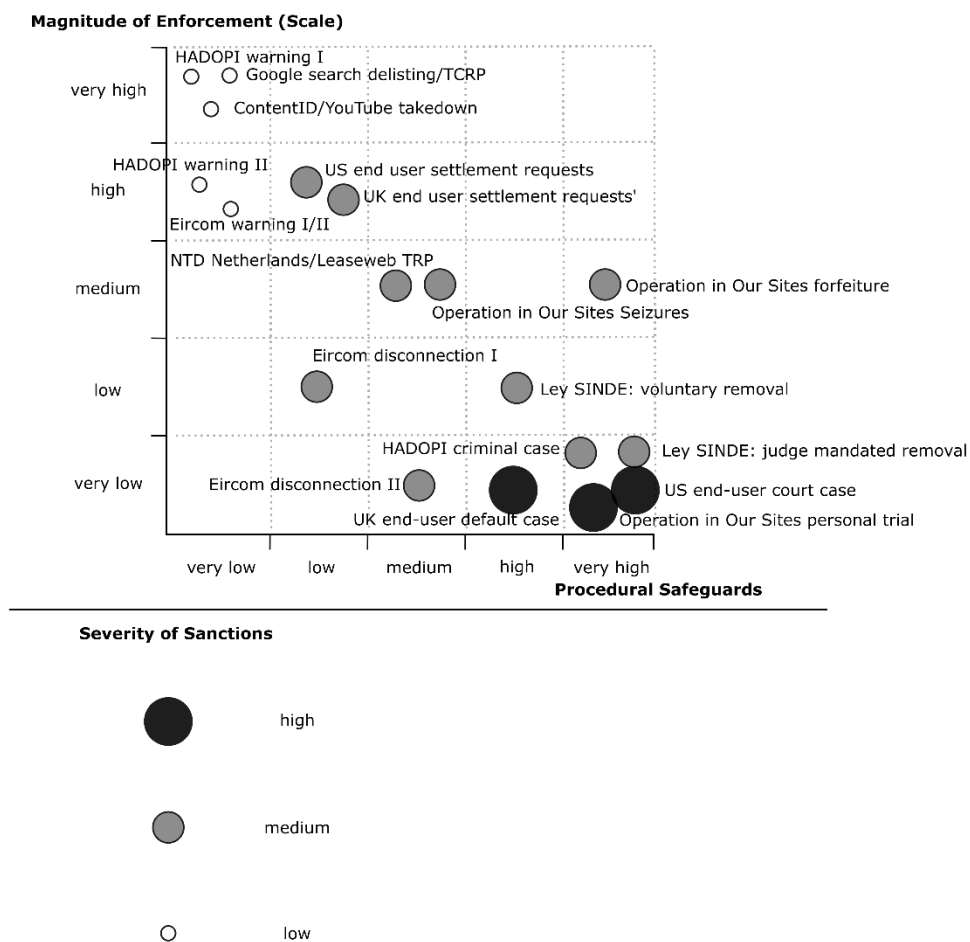
Om de relatie tussen de schaal, strafzwaarte en waarborgen in de online handhaving van het auteursrecht empirisch te onderzoeken, analyseerden we 22 sanctiemechanismen die behoren tot acht handhavingsstrategieën in zes landen tussen 2004 en 2014. Elke handhavingsstrategie is een casus. We hebben gekeken naar wat bekend is over het effect ervan op inbreuk niveaus en de kosten van de handhaving. Binnen elke strategie kunnen er meerdere sanctiemechanismen zijn. We bestudeerden deze als subcasussen, waarbij we keken naar de schaal waarop ze werden toegepast, de strafzwaarte, en de procedurele waarborgen die werden geboden aan de betrokkenen die een sanctie werd opgelegd.

Het onderzoek toont aan dat rechthebbenden handhaving in sommige strategieën hebben kunnen opschalen, en dat in deze gevallen schaal ten koste ging van procedurele waarborgen. Procedures zoals bijvoorbeeld 'notice and takedown' stelden rechthebbenden in staat om miljoenen zoekresultaten van Google te verwijderen, maar alleen omdat de gerechtelijke controle was weggehaald. Alleen op het initiatief en de kosten van de gesanctioneerde partijen, kon er gerechtelijke controle plaats vinden en pas na de sanctie. Rechthebbenden hebben waarborgen kunnen ontlopen door niet-gerechtigde spelers, zoals tussenpersonen, de sanctionerende partij te maken. In het geval van 'notice and takedown' worden tussenpersonen op de hoogte gebracht van de inbreuk en juridisch onder druk gezet

om te handhaven: zij worden geconfronteerd met hoge boetes als ze dat niet doen. Deze uitruil tussen waarborgen en schaal is zichtbaar in elk handhavingsstrategie die we hebben geanalyseerd. Dit betekent dat het casusonderzoek de theoretische voorspellingen bevestigt - en ook de waarschuwingen van de tegenstanders van toegenomen handhaving van het auteursrecht. Wanneer het aantal sancties toeneemt, gaat dit ten koste van de procedurele waarborgen. Inmiddels hebben een aantal partijen nieuwe waarborgen voor grootschalige procedures gecreëerd, maar het is onzeker in hoeverre zij volstaan om juridische fouten of misbruik te voorkomen.

Sommige strategieën verhogen de strafzwaarte. Het onderzoek laat echter zien dat zwaardere sancties niet op grote schaal werden toegepast. Zo leidden bijvoorbeeld het offline halen van een website via de Sinde procedure in Spanje of via 'Operation in Our Sites' in de VS tot een zware sanctie – het verwijderen van een gehele website of bedrijf - maar werden zij alleen toegepast op een beperkt aantal websites. Ook in Frankrijk heeft de overheidsinstantie HADOPI weliswaar miljoenen waarschuwingen aan burgers gestuurd, maar kreeg slechts een handvol de ultieme sancties (boetes of een opschorting van de toegang tot internet) op bevel van de rechter. Dit betekent dat het casusonderzoek de theoretische voorspellingen bevestigt. De handhaving strategieën vergroten ofwel de kans op sancties, of verhogen de zwaarte van de straf, maar niet allebei.

Figuur B toont dat in de 22 subcasussen en de daarbij horende 8 casussen die onderzocht zijn, er een verband is tussen schaal, strafzwaarte en waarborgen. De subcasussen die op grotere schaal worden toegepast hebben minder waarborgen. Denk aan de HADOPI waarschuwingsbrieven en 'notice and takedown' zoals het door Google wordt toegepast. Voor de sanctiemechanismen die niet goed opschaalden vonden we meer waarborgen, zoals in het geval van rechtszaken. De figuur suggereert ook een relatie tussen strenge straffen en schaal: zwaardere sancties schalen niet op.



Figuur B: Grafiek die schaal, strafzwaarte en waarborgen laat zien voor elke subcasus. Voor ruimtelijke doeleinden, zijn sommige subcasussen als één bol weer gegeven, van elkaar gescheiden door een schuine streep.

Het weergeven van kwalitatieve gegevens is in een grafiek lastig. Aangezien geen van de maatregelen precies kunnen zijn, gebruik ik een ordinale schaal om de variabelen weer te geven voor alle sanctiemechanismen (de subcasussen). De grafiek is verdeeld in cellen om het beter leesbaar te maken. Elke bol wordt gelezen als alleen die van die cel. De exacte positie in een cel, naar links of naar rechts, heeft verder geen betekenis en is zo weergegeven om meer ruimte te kunnen gebruiken. Daarnaast scoren sommige subcasussen hetzelfde op variabelen. Daarom zijn zij soms vertegenwoordigd door een enkele bol, hun namen gescheiden door een schuine streep.

Het onderzoek laat ook zien dat auteursrechthandhaving verschillende kosten met zich mee brengt: kosten voor de rechthebbenden, institutionele kosten voor rechtbanken, kosten voor de rechtshandhaving door publieke instellingen, kosten door degenen die zich willen verdedigen tegen de dreiging of de toepassing van een sanctie, en de kosten voor derde partijen.

Al met al, laten de bevindingen zien dat de totale kosten van de handhaving zijn gestegen. Dit is geen verrassing, aangezien het aantal inbreuken eveneens is gestegen. Dit betekent dat er meer kosten door de samenleving als geheel worden gedragen, omdat de grootschalige handhavingsstrategieën een aanzienlijk deel van de kosten toewijzen aan openbare instanties (door het vergroten van de rol van de staat), derden (door ze te betrekken in handhaving tegen eindgebruikers) en de ontvangers van de sancties (die zichzelf willen verdedigen tegen claims).

Deze verdeling van de kosten wijst op een problematische prikkel door een verkeerde afstemming van private en maatschappelijke kosten en baten. De voordelen van handhaving van hun privé-rechten stromen naar de rechthebbenden, maar een aanzienlijk deel van de kosten wordt gedragen door anderen. Dit biedt rechthebbenden een prikkel om meer handhaving te initiëren of vragen dan het geval zou zijn als ze het grootste deel van de kosten zelf zouden dragen.

Het onderzoek toont ook aan dat bijna geen enkele van de handhavingstrategieën inbreuken blijvend verminderden. Het niveau waarop inbreuken wereldwijd plaats vonden bleef nagenoeg stabiel, en het casusonderzoek toont aan dat handhavingsprocedures beperkte gevolgen hadden voor het aantal inbreuken dat plaats vond. 'Graduated response' procedures leken van invloed te zijn op door P2P gefaciliteerde inbreuken. Dit kan zijn omdat het systeem een grote schaal in de eerste fase combineert met een zware sanctie in een latere fase, maar het kan ook een vals signaal zijn en alleen maar wijzen op de verschuiving van eindgebruikers richting encryptie en het delen van bestanden buiten P2P.

Dit onderzoek was gericht op het aantonen van een empirische relatie tussen de schaal, strafwaarde en procedurele waarborgen. Deze inzichten kunnen beleidsmakers begeleiden door meer duidelijkheid te verschaffen over de beleidskeuzes waarmee zij worden geconfronteerd in dit domein.

We hebben empirisch de rechtseconomische theorieën bevestigd: procedures die auteursrecht op grote schaal handhaven kunnen dat door minder procedurele waarborgen te bieden aan gesanctioneerde partijen. Ook hebben procedures die op een grotere schaal worden toegepast minder strenge sancties. Het onderzoek heeft ook aangetoond dat het aantal inbreuken dat plaats vond wereldwijd in grote lijnen onveranderd bleef, en dat handhavingsprocedures aanzienlijke kosten creëren, waarvan een groot deel is uitbesteed aan de staat en aan derden.

Wat betekenen deze bevindingen voor de handhaving van het auteursrecht? Door binnen het rechtseconomisch kader over handhaving na te denken, kunnen we de discussie over beleidsimplicaties in drie kernvragen voeren:

(1) Hoe kunnen we handhaving effectiever maken?

(2) Kunnen we de negatieve bijwerkingen van intensievere handhaving beperken?

(3) Zijn er alternatieven voor intensievere handhaving?

Dit onderzoek biedt een leidraad om deze vragen te beantwoorden, hoewel veel dingen onduidelijk blijven.

Hoe kunnen we handhaving effectiever maken?

De status quo bleek nogal teleurstellend voor iedereen: de maatschappij draagt aanzienlijke kosten en neveneffecten van meer grootschalige handhaving, zonder dat daar veel tegenover staat in termen van effectiviteit. De strategieën zijn niet erg succesvol geweest in het terugdringen van het aantal inbreuken. In de meeste gevallen uitten zelfs de rechthebbenden hun onvrede over de huidige situatie. Hoewel er enige discussie bestaat

over wat "effectief" betekent, wees, als we terugkeren naar het oorspronkelijke, en nog steeds dominante doel van handhaving om het aantal inbreuken naar beneden te brengen, onze theorie en empirisch bewijs op twee fundamentele opties: verdere toename van de schaal waarop handhaving plaats vindt en een toename van de strafzwaarte.

Voor elk van de nieuwe handhaving strategieën is het bereiken van schaal gepaard gegaan met minder waarborgen, vooral in vergelijking met de waarborgen aangeboden in een gewone civiele rechtszaak. Dit suggereert sterk dat schaalvergroting verder alleen mogelijk zal zijn door nog meer waarborgen te verwijderen. Dit kan leiden tot ernstige maatschappelijke kosten, omdat waarborgen belangrijk zijn voor de bescherming van de rechtsstaat, mensenrechten zoals de vrijheid van meningsuiting en privacy, innovatie en de zorgvuldige balans die auteursrecht bewaakt tussen beschermde uitingen en niet beschermde uitingen of uitingen die onder de uitzonderingsregels vallen. Talloze voorbeelden laten zien dat misbruik en nietige gedingen voorkomen op het gebied van auteursrecht. Dit is precies wat handhavingsprocedures controversieel maakt.

De tweede optie is om de strafzwaarte te vergroten. Sommige handhavingsprocedures zijn omstreden omdat de sancties in vergelijking met de waargenomen schade van inbreuken als onevenredig worden ervaren. Een klassiek voorbeeld hiervan is de zaak van Capitol Records vs. Jammie Thomas-Rasset. De vrouw werd veroordeeld tot \$ 220.000 voor het delen van 24 liedjes via Kazaa. Dergelijke sancties veroorzaken veel weerstand bij het grote publiek. Rechthebbenden zijn al geconfronteerd met een moeilijke situatie, omdat er weinig draagvlak is voor handhaving, en een vergrote strafzwaarte zal dit probleem verergeren.

Afgezien van deze maatschappelijke effecten zal elke intensivering van handhaving ook verdere economische kosten opleggen aan de staat en aan derden.

Wat betekent dit voor beleidsmakers? De pogingen tot grootschalige handhaving van de afgelopen tien jaar hebben geleid tot een problematische status quo. Als het door ons verrichte casusonderzoek een goede leidraad is zou het verder intensiveren van handhaving - dat wil zeggen: meer schaal en een hogere strafzwaarte - zeer waarschijnlijk de negatieve effecten van handhaving vergroten met onzekere resultaten in termen van een afname van het aantal inbreuken. Is dat het waard?

Tot op zekere hoogte is deze vraag al beantwoord in de praktijk. Sommige van de strategieën die zijn voorgesteld om de strafzwaarte en schaal te vergroten zijn al erg omstreden. De politiek heeft ingegrepen en SOPA gestopt en in het Verenigd Koninkrijk heeft de rechterlijke macht het grote aantal schikkingsvoorstellen verstuurd door advocaten aan voorwaarden verbonden. In Duitsland werden dezelfde soort grootschalige schikkingsvoorstellen zonder rechterlijke tussenkomst gecorrigeerd door de wetgever door de mogelijke sanctie op het eind te verlagen. Ook is de uiteindelijke sanctie in HADOPI verminderd. Ondertussen streven rechters en wetgevers er in toenemende mate naar om een einde te maken aan het op grote schaal versturen van schikkingsvoorstellen in de VS.

Kunnen we de negatieve bijwerkingen van meer handhaving beperken?

Zou er een manier zijn om de schaal en de strafzwaarte van sanctionering te verhogen, terwijl we ook procedurele waarborgen kunnen behouden of kunnen laten toenemen? Onze vergelijkende analyse van 22 sanctiemechanismen suggereert dat dit uiterst moeilijk is. De enige compenserende voorbeelden zijn de bescheiden nieuwe waarborgen die in een aantal van de nieuwe procedures zijn toegevoegd. Denk aan het transparantie verslag van Google, bijvoorbeeld. Systemen op basis van reputatie en meer transparantie kunnen de balans

verbeteren. Het is echter de vraag of deze garanties toereikend zijn om juridische fouten of misbruik te voorkomen. De vraag voor beleidsmakers blijft dan of we deze negatieve neveneffecten moeten accepteren.

Rechthebbenden zijn niet bereid om de waarborgen te behouden en daarvoor de kosten te dragen, omdat die procedures te duur zijn. Dit is het meest zichtbaar in de rechtszaken tegen eindgebruikers. We hebben voldoende bewijs dat rechthebbenden deze procedures grotendeels hebben verlaten vanwege de kosten. Met andere woorden, de rechthebbenden zelf waren niet bereid om hun geld te besteden aan het opschalen van de handhaving, met behoud van waarborgen. Dit roept de onvermijdelijke vraag op: als rechthebbenden, die profiteren van de potentiële voordelen van een effectievere handhaving, niet bereid zijn om deze kosten te dragen, waarom zouden dan de staat, belasting betaler of derden moeten worden gevraagd om ze te dragen?

*Zijn er alternatieven?*¹⁹⁸²

Wat is het alternatief? We zouden het auteursrecht moeten hervormen. Auteursrecht is momenteel een exclusief eigendomsrecht, maar inbreuken op grote schaal en de problemen met handhaving laten zien dat dit paradigma misschien niet geschikt is voor het informatietechnologie tijdperk. Met behulp van rechtseconomische theorieën kunnen we kijken naar nieuwe manieren om de entertainment markt economisch te stimuleren en de toegang te garanderen tot cultuur voor het publiek. Een manier zou zijn om exclusiviteit te laten vallen en meer te bewegen in de richting van een toegangsrecht. Dat is meer in lijn met de business modellen die momenteel opkomen (zoals Netflix en Spotify). Dit betekent dat leveranciers zouden betalen voor het recht om toegang tot cultuur aan het publiek te geven, en nog steeds rechthebbenden compenseren voor hun werk. Het zou drastisch de kosten van de handhaving verlagen, en de kosten in de vorm van schendingen van de mensenrechten verlagen.

¹⁹⁸² Part of this Section was previously published as Floris Kreiken & David Koepsell, "Coase and Copyright," *University of Illinois Journal of Law, Technology and Policy* 1 (2013): 1-44.

BIBLIOGRAPHY

Articles, Books, News, Websites

- @Wicho. "El papel de los jueces en la Ley Sinde-Wert: básicamente ninguno." *Microsiervos*, January 5, 2012. <http://www.microsiervos.com/archivo/mundoreal/papel-jueces-ley-sinde-wert-basicamente-ninguno.html>
- Abelson, Sarah. "An Emerging Secondary Market for Digital Music: The Legality of ReDigi and the Extent of the First Sale Doctrine." *29 Ent. & Sports Law* 8 (2012).
- Adcock, Robert and David Collier. "Measurement validity: A shared standard for qualitative and quantitative research." *American Political Science Association*, 95.03 (2001). 529-546.
- Adermon, Adrian and Che-Yuan Liang. "Piracy, Music, and Movies: A Natural Experiment," *Working Paper Series* 13. Center for Fiscal Studies, Uppsala University (2010).
- Admin. "DirecTV prepares to sue." *Geek*, July 31, 2001. <http://www.geek.com/news/directv-prepares-to-sue-545136/>
- Aguiar, Luis and Bertin Martins. "Digital Music Consumption on the Internet: Evidence from Clickstream Data," *European Commission, Joint Research Centre, Institute for Prospective Technological Studies*, March, 2013. <http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=6084>
- Aguiar, Luis, Jörg Claussen, Christian Peukert. "Online Copyright Enforcement, Consumer Behavior, and Market Structure." *European Commission, Joint research centre*, 2015. <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/online-copyright-enforcement-consumer-behavior-and-market-structure>
- Albanesius, Chloe. "Megaupload Shutdown Fails to Slow File Sharing." *PCmag*, February 9, 2012. <http://www.pcmag.com/article2/0,2817,2400052,00.asp>
- Alexander, Lexi. "See No Evil, Hear No Evil...Definitely Don't Notice The MPAA." *Lexi Alexander*, October 2014. <http://www.lexi-alexander.com/blog/2014/10/5/see-no-evil-hear-no-evildefinitely-dont-notice-the-mpaa>
- Alge, Bradley. "Effects of computer surveillance on perceptions of privacy and procedural justice." *Journal of Applied Psychology* 86.4 (2001): 797.
- Allworth, James. "Why I'm Not Going Near Spotify (and Why You Shouldn't Either)." *Harvard Business Review*, July 22, 2011. http://blogs.hbr.org/cs/2011/07/why_im_not_going_near_spotify.html
- Ambassador Miriam Sapiro. "The Role of the Anti Counterfeiting Trade Agreement (ACTA)." *Official office of the U.S. Trade Representative response, We the People*, <https://petitions.whitehouse.gov/response/role-anti-counterfeiting-trade-agreement-acta>
- American Civil Liberties Union. "Citing Right to Anonymity Online. ACLU Asks Boston Court to Block Recording Industry Subpoena." *American Civil Liberties Union*, September 29, 2003. <http://www.aclu.org/technology-and-liberty/citing-right-anonymity-online-aclu-asks-boston-court-block-recording-industry>
- Anderson, Chris. "Free! Why \$0.00 Is the Future of Business." *Wired*, February 25, 2008. http://archive.wired.com/techbiz/it/magazine/16-03/ff_free?
- Anderson, Greg. "Statistics on Scandinavian Music Streamers." *Arcticstartup*, January 23, 2012. <http://www.arcticstartup.com/2012/01/23/statistics-on-scandinavian-music-streamers>

- Anderson, Martin. "Film consortium urges ISPs to abandon ineffective 'six strikes' policy for pirates." *The Stack*, May 13, 2015. <http://thestack.com/Internet-security-task-force-six-strikes-130515>
- Anderson, Nate. "US government finally admits most piracy estimates are bogus." *ArsTechnica*, April 13, 2010. <http://arstechnica.com/tech-policy/2010/04/us-government-finally-admits-most-piracy-estimates-are-bogus/>
- Anderson, Nate. "France halts 'three strikes' IP-address collection after data leak." *Wired*, May 17, 2011. <http://www.wired.com/threatlevel/2011/05/tmg/>
- Anderson, Nate. "Major ISPs agree to 'six strikes' copyright enforcement plan." *ArsTechnica*, July 7, 2011. <http://arstechnica.com/tech-policy/2011/07/major-isps-agree-to-six-strikes-copyright-enforcement-plan/>
- Anderson, Nate. "The 'legal blackmail' business: inside a P2P settlement factory." *Ars Technica*, September 29, 2010. <http://arstechnica.com/tech-policy/2010/09/amounts-to-blackmail-inside-a-p2p-settlement-letter-factory/>
- Anderson, Nate. "The RIAA? Amateurs, Here's how you sue 14,000+ P2P users." *Ars Technica*, June 2, 2010. <http://arstechnica.com/tech-policy/news/2010/06/the-riaa-amateurs-heres-how-you-sue-p2p-users.ars>
- Anderson, Nate. "US anti-P2P law firms sue more in 2010 than RIAA ever did." *Ars Technica*, October 7, 2010. <http://arstechnica.com/tech-policy/2010/10/us-anti-p2p-law-firms-sue-more-in-2010-than-riaa-ever-did/>
- Andy. "Germany passes law to mitigate copyright trolling 'fines'." *Torrentfreak*, July 3, 2013. <https://torrentfreak.com/germany-passes-law-to-mitigate-copyright-trolling-fines-130703/>
- Arnold, Michael, Eric Darmon, Sylvain Dejean and Thierry Pénard. "Graduated response policy and the behavior of digital pirates: Evidence from the french three-strike (hadopi) law." *Available at SSRN 2380522* (2014).
- Article 19. "European Commission: Freedom of Expression Needs Better Protection in Digital Communications." *Art 19 Press Release*, November 9, 2010. www.article19.org/pdfs/press/european-commission-freedom-of-expression-needs-better-protection-in-digital.pdf
- Asghari, Hadi, Michel Van Eeten, and Milton Mueller. "Unraveling the economic and political drivers of deep packet inspection." *GigaNet 7th Annual Symposium*. November. (Vol. 5. 2012).
- Austen, Ian. "RIM to Start a Music-Sharing Service." *Bits*, August 25, 2011. <http://bits.blogs.nytimes.com/2011/08/25/rim-to-start-a-music-sharing-service/>
- Ayres, Ian and John Braithwaite. *Responsive Regulation: Transcending the Deregulation Debate*. New York: Oxford University Press, 1992.
- Aziz, Riyadh Abdul. "Copyright piracy in Spain." *Muscatdaily.com*, September 22, 2013. <http://www.muscatdaily.com/Archive/Stories-Files/Copyright-Piracy-in-Spain-2kpm>
- BAE Systems Detica. "The six business models for copyright infringement." *Google & PRS for Music*, June 27, 2012. <http://www.prsformusic.com/aboutus/policyandresearch/researchandconomics/Documents/TheSixBusinessModelsofCopyrightInfringement.pdf>
- Bahrani, Mahmoud. "The economics of crime with Gary Becker." *The Chicago Maroon*, May 25, 2012. <http://chicagomaroon.com/2012/05/25/the-economics-of-crime-with-gary-becker/>

- Bakare, Lanre. "Illegal music filesharing is now mainstream." *the Guardian*, September 18, 2012. <http://www.theguardian.com/commentisfree/2012/sep/18/illegal-music-filesharing-mainstream-ed-sheeran>
- Bakker, Jasper. "'Afpersende' Britse piraterijbestrijder geschorst." *Webwereld*, January 19, 2012. <http://webwereld.nl/nieuws/109247/-afpersende--britse-piraterijbestrijder-geschorst.html>
- Balganesh, Shyamkrishna. "The Uneasy Case Against Copyright Trolls." *S. CAL. L. REV.* 86: 723 (2013).
- Band, Jonathan and Jonathan Gerafi. "Foreign Ownership of Firms in IP Intensive Industries" (March 13, 2013). Available at SSRN: <http://ssrn.com/abstract=2333839> or <http://dx.doi.org/10.2139/ssrn.2333839>
- Band, Jonathan and Jonathan Gerafi. "Infringement Risk in Copyright-Intensive Industries." *Infojustice.org*, January 6, 2014. <http://infojustice.org/archives/31827>
- Band, Jonathan. "New Study: The Profitability of Copyright-Intensive Industries." *Infojustice.org*, June 17, 2013. <http://infojustice.org/archives/29916>
- Band, Jonathan and Jonathan Gerafi. "CEO Compensation in the Copyright-Intensive Industries." *Infojustice.org*, August 14, 2013. <http://infojustice.org/archives/30466#more-30466>
- Bangeman, Eric. "MediaSentry site redesign drops references to litigation." *Ars Technica*, February 20, 2008. <http://arstechnica.com/tech-policy/2008/02/mediasentry-site-redesigned-loses-references-to-litigation/>
- Bangeman, Eric. "RIAA Trial Verdict Is In: Jury Finds Thomas Liable for Infringement." *Ars Technica*, October 4, 2007.
- Bangeman, Eric. "P2P Traffic Shifts Away From Music, Towards Movies." *Ars Technica*, July 5, 2007.
- Bangeman, Eric. "Pass or Fail? RIAA's College Litigation Campaign Turns One." *Ars Technica*, February 27, 2008.
- Bangeman, Eric. "RIAA Trial Verdict Is In: Jury Finds Thomas Liable for Infringement." *Ars Technica*, October 4, 2007.
- Barendt, Eric. *Freedom of speech*. Oxford University Press, 2005.
- BBC News. "Viacom will sue YouTube for \$1bn." *BBC News*, March 13, 2007. <http://news.bbc.co.uk/2/hi/business/6446193.stm>
- BBC. "Japan introduces piracy penalties for illegal downloads." *BBC*, October 1, 2012. <http://www.bbc.com/news/technology-19767970>
- Beadon, Leigh. "Infographic: People Will Pay To Support Creators When Free Is An Option." *Techdirt*, December 12, 2012. <https://www.techdirt.com/blog/casestudies/articles/20121210/12422821338/infographic-people-will-pay-to-support-creators-even-when-free-is-option.shtml>
- Beadon, Leigh. "NBC Universal Caught Using Infringing Graphic From Apple, Probably Won't Learn Anything." *Techdirt*, March 30, 2012. <http://www.techdirt.com/articles/20120330/08581418302/nbc-universal-caught-using-infringing-graphic-apple-probably-wont-learn-anything.shtml>
- Becker, Gary. "Crime and Punishment: an Economic approach." *The Journal of Political Economy* 76.2 (1968). 169-217.
- Beggs, Jodi. "The Coase Theorem." *Economics-About.com*. <http://economics.about.com/od/externalities/a/The-Coase-Theorem.htm> (last visited February 11, 2013).

- Benabou, VL.. "The Chase: The French Insight into the 'Three Strikes' System." in: *Copyright Enforcement and the Internet*. ed. Stamatoudi. Kluwer Law International. The Netherlands, 2010.
- Benkler, Yochai. "Seven Lessons from SOPA/PIPA/Megaupload and Four Proposals on Where We Go From Here." *Techpresident*, January 25, 2012. <http://techpresident.com/news/21680/seven-lessons-sopapipamegaupload-and-four-proposals-where-we-go-here>
- Benkler, Yochai. *The wealth of networks: How social production transforms markets and freedom*. Yale University Press, 2006.
- Berkow, Jameson. "Netflix Proclaimed 'King' of North American Internet Use." *Fin. Post*, May 17, 2011. <http://business.financialpost.com/2011/05/17/netflix-named-king-of-north-american-internet/>
- Bernfeld, Wendy. "Brave New World: Digital Distribution Beyond the Old World." *Sundance Institute*, April 23, 2012. <http://www.sundance.org/artistservices/distribution/article/brave-new-world-digital-distribution-beyond-the-old-world/>
- Biddle, Peter, Paul England, Marcus Peinado and Bryan Willman. "The Darknet and the Future of Content Distribution." in: *Proceedings of the 2002 ACM Workshop on Digital Rights Management* (2002). <http://crypto.stanford.edu/DRM2002/darknet5.doc>
- Billboard Staff. "Legitimate Streaming Services Cut Down on Piracy, Report Suggests." *Billboardbiz*, October 3, 2012. <http://www.billboard.biz/bbbiz/industry/digital-and-mobile/bittorrent-share-shrinks-in-countries-that-1007966012.story>
- Bits of Freedom. "Providers verwijderen tekst Multatuli." *Bits of Freedom website*, October 13, 2004. <https://www.bof.nl/2004/10/13/providers-verwijderen-tekst-multatuli/>
- Bits of Freedom. "Overgeleverd aan willekeur, onderzoek naar de verwijdering van rechtmatige informatie door hostingproviders." *Bits of Freedom website*, December 22, 2012. Dutch version can be found here: <https://www.bof.nl/live/wp-content/uploads/20120401-overgeleverd-aan-willekeur-rapport.pdf>
- Bjerkoe, Richard and Anders Sorbo. "The Norwegian Music Industry in the Age of Digitalization." *BI Norwegian School of Management - Thesis* (September 2010). <http://www.scribd.com/doc/37406039/Thesis-Bjerkoe-Sorbo>
- Bomsel, Olivier and Heritiana Ranaivoson. "Decreasing Copyright Enforcement Costs: The Scope of Graduated Response". *Review of Economic Research on Copyright Issues*. 6(2) (2009): 13-29.
- Borland, John. "Audiogalaxy hit by RIAA suit." *CNET News.com*, May 24, 2002.
- Borland, John. "Record Industry warns of new lawsuits." *CNET News.com*, October 17, 2003.
- Borland, John. "RIAA files 80 new file-swapping suits." *CNET News.com*, October 30, 2003.
- Borland, John. "RIAA Sues Aimster Over File-Swapping." *CNET News.com*, May 25, 2001.
- Borland, John. "RIAA sues iMesh file-trading firm." *CNET News.com*, September 19, 2003.
- Borland, John. "Suit Hits Popular Post-Napster Network." *CNET News.com*, October 3, 2001.
- Boswell, Wendy. "Google Search Statistics." *About Tech*. <http://websearch.about.com/od/focusongoogle/f/Google-Search-Statistics.htm> last viewed on April 16, 2014.
- Botero, Juan Carlos and Alejandro Ponce. "Measuring the rule of law." *Available at SSRN* 1966257 (2011).
- Boudreau, John. "Illegal file sharing showing no letup." *San Jose Mercury News*, July 3, 2006.

Boutin, Paul. "E-book piracy costs U.S. publishers \$3 billion, says study." *Venturebeat.com*, March 2, 2010. <http://venturebeat.com/2010/03/02/book-piracy-costs-u-s-publishers-3b-says-study/>

Bowman, Lisa. "Labels aim big guns at file swappers." *CNET News.com*, June 25, 2003.

Boyle, James. *The public domain: Enclosing the commons of the mind*. New Haven: Yale University Press, 2008.

Bradwell, Peter. "Can't Look Now: Finding Film Online." *Open Rights Group*, October 19, 2011. <http://www.openrightsgroup.org/blog/2011/cant-look-now:-finding-film-online>

Bradwell, Peter, "Evidence Please." *Open Rights Group*, October 13, 2011. <http://www.openrightsgroup.org/blog/2011/the-need-for-evidence>

Brandle, Lars. "France's 'Three-Strikes' Hadopi Law Gets the Guillotine." *Billboardbiz*, July 10, 2013. <http://www.billboard.com/biz/articles/news/global/1569397/frances-three-strikes-HADOPI-law-gets-the-guillotine>.

Brewster, Thomas. "Britain's Anti-Piracy Act Delayed By Cost Dispute." *TechWeek Europe*, April 26, 2012. <http://www.techweekeurope.co.uk/news/copyright-anti-piracy-act-delayed-75259>

Bridis, Ted. "Some strange twists in music piracy lawsuits." *Associated Press*, August 23, 2004.

Bridy, Annemarie. "Graduated Response American Style: 'Six Strikes' Measured Against Five Norms." *Fordham Intellectual Property, Media & Entertainment Law Journal* 23.1 (2012): 1-66.

Bridy, Annemarie. "Is Online Copyright Enforcement Scalable?" *Vanderbilt Journal of entertainment and technology law* 13 (2011): 695.

Bridy, Annemarie. "Why Pirates (Still) Won't Behave: Regulating P2P in the Decade after Napster." *Rutgers Law Journal* 40 (2009): 565.

Bright, Peter. "French 'three strikes' anti-piracy software riddled with flaws." *Ars Technica*, May 26, 2011. <http://arstechnica.com/tech-policy/2011/05/french-three-strikes-anti-piracy-software-riddled-with-flaws/>

Brink, Graham. "DirecTV turns to state courts for piracy suits." *St. Petersburg Times Online*, November 1, 2003. http://www.sptimes.com/2003/11/01/State/DirecTV_turns_to_stat.shtml

Broido, Andre, Nevil Brownlee, kc claffy, Thomas Karagiannis and Michalis Faloutsos. "Is P2P dying or just hiding?" *Global Internet and Next Generation Networks*. (November/December 2004).

Brustein, Joshua. "Netflix and YouTube Dominate Online Video. Can Amazon Catch Up?." *Bloomberg Business*, Nov 11, 2013. <http://www.businessweek.com/articles/2013-11-11/netflix-and-youtube-dominate-online-video-dot-can-amazon-catch-up>

Buist, Henk-Jan. "BREIN stuurt politie af op uploader." *Webwereld*, May 23, 2012. <http://webwereld.nl/nieuws/110601/brein-stuurt-politie-af-op-uploader.html>

Business Software Alliance. "2011 Piracy Study." <http://globalstudy.bsa.org/2011/>

Business Software Alliance. "Shadow Market." *Business Software Alliance*, May 2012. http://globalstudy.bsa.org/2011/downloads/study_pdf/2011_BSA_Piracy_Study-Standard.pdf

Butler, Susan. "Sixth Wave of RIAA Pre-Litigation Letters Sent to Colleges." *The Hollywood Reporter Esquire*, July 19, 2007.

Byford, Sam. "Megaupload takedown may have increased legal movie downloads, says study." *The Verge*, March 7, 2013. <http://www.theverge.com/2013/3/7/4077484/study-says-megaupload-shutdown-helped-movie-sales>

- Cala, Andrés. "Push grows to blacklist Spain over digital pirating." *The Christian Science Monitor*, March 4, 2013. [http://www.csmonitor.com/World/Europe/2013/0304/Push-grows-to-blacklist-Spain-over-digital-pirating/\(page\)/2](http://www.csmonitor.com/World/Europe/2013/0304/Push-grows-to-blacklist-Spain-over-digital-pirating/(page)/2)
- Cammaerts, Bart, Bingchun Meng and Robin Mansell. "Copyright & Creation". *Media Policy Brief, London School of Economics* (September 2013). <http://blogs.lse.ac.uk/mediapolicyproject/>
- Campbell, Colin. "Gabe Says Piracy Isn't About Price." *IGN*, November 25, 2011. <http://uk.games.ign.com/articles/121/1213357p1.html>
- Campbell, Thomas. "Spanish government to come down harder on those benefiting from online piracy." *IP&TV news*, September 23, 2013. <http://www.iptv-news.com/2013/09/spanish-government-to-come-down-harder-on-those-benefiting-from-online-piracy/>
- Canadian Intellectual Property Council. *The True Price of Peer to Peer File-Sharing* (2010). Available at: <http://musiccanada.com/wp-content/uploads/2015/06/The-True-Price-of-Peer-to-Peer-File-Sharing.pdf>
- Carolan, Mary. "Four Music Firms Dispute Data Chief's Notice to Eircom." *Irish Times*, March 1, 2012.
- Carolan, Mary. "Legal action to stop UPC users downloading illegally." *The Irish Times*, February 10, 2014. <http://www.irishtimes.com/news/crime-and-law/courts/legal-action-to-stop-upc-users-downloading-illegally-1.1686474>
- Carr, Paul. "Book Piracy: A Non-Issue." *TechCrunch*, August 23, 2011. <http://techcrunch.com/2011/08/23/book-piracy-a-non-issue/>
- Case, Anne and Lawrence F. Katz. "The company you keep: The effects of family and neighborhood on disadvantaged youths." *National Bureau of Economic Research* No. w3705. (1991).
- Castro, Daniel, Richard Bennett, and Scott Andes. "Steal these policies: strategies for reducing digital piracy." *Information Technology and Innovation Foundation* (Washington, DC: 2009). <http://www.itif.org/files/2009-digital-piracy.pdf>
- Center for Copyright Information. "CCI Provides First Copyright Alert System Progress Report Highlighting Initial Accomplishments." *Press release, Center for Copyright Information*, May 28, 2014. <http://www.copyrightinformation.org/press-release/cci-provides-first-copyright-alert-system-progress-report-highlighting-initial-accomplishments/>
- Center for Democracy and Governance. *Handbook of Democracy and Governance Program Indicators* (August 1998).
- Chaitovitz, Ann, Charisma Hampton, Kevin Rosenbaum, Aisha Salem, Tom Stoll and Albert Tramosch. "Responding to Online Piracy: Mapping the Legal and Policy Boundaries." 20 *COMmLAW CONSPECTUS* 1, 7 (2011).
- Champeau, Guillaume. "Devant l'Hadopi, le silence est la meilleure des defenses." *Numérama*, December 16, 2011. <http://www.numerama.com/magazine/20964-devant-l-HADOPI-le-silence-est-la-meilleure-des-defenses.html>
- Champeau, Guillaume. "Hadopi : le gouvernement refuse de payer la note." *Numérama*, August 12, 2010. <http://www.numerama.com/magazine/16492-HADOPI-le-gouvernement-refuse-de-payer-la-note.html>
- Champeau, Guillaume. "Hadopi : le vrai bilan négatif de la riposte graduée." *Numérama*, May 9, 2013. <http://www.numerama.com/magazine/25919-HADOPI-le-vrai-bilan-negatif-de-la-riposte-graduee.html>

- Champeau, Guillaume. "Hadopi affirme que le P2P est en baisse. Vraiment?." *Numerama*, March 27, 2012. <http://www.numerama.com/magazine/22146-HADOPI-affirme-que-le-p2p-est-en-baisse-vraiment.html>
- Champeau, Guillaume. "HADOPI: la CNIL avait dénoncé l'absence de contrôle de TMG!" *Numerama*, September 20, 2010. <http://www.numerama.com/magazine/16826-hadopi-la-cnil-avait-denonce-l-absence-de-contrôle-de-tmg.html>
- Cisco. "Cisco visual networking index: Forecast and methodology, 2009–2014." *CISCO White paper* (2010).
- Citron, Danielle Keats. "Technological Due Process." *Washington University Law Review* 85 (2008): 1249.
- Claburn, Thomas. "Fair Use Worth More to Economy Than Copyright, CCA Says." *InformationWeek*, Sept 12, 2007. <http://www.informationweek.com/fair-use-worth-more-to-economy-than-copyright-cca-says/d/d-id/1059122>
- Claburn, Thomas. "ICE Confirms Inadvertent Web Site Seizures." *InformationWeek*, Feb. 18, 2011. <http://commcns.org/ufeCLE>
- CNN. "Napster usage quadruples." *CNN.com*, September 11, 2000.
- CNN. "UPDATE: Mediaset Files EUR500 Million Suit Vs Google's YouTube." *CNN Money*, July 30, 2008. http://money.cnn.com/news/newsfeeds/articles/dif500/200807301025DOWJONESDJONLINE000654_FORTUNE5.htm
- Coase, Ronald H.. "The Federal Communications Commission." *Journal of Law & Economics* 2. (1959).
- Coase, Ronald H.. "The Institutional Structure of Production." *The American Economic Review* 82 (1992): 713.
- Coase, Ronald. "The Problem of Social Cost." *Journal of Law & Economics* (1960): 1-44.
- Cobia, Jeffrey. "The Digital Millennium Copyright Act Takedown Notice Procedure: Misuses, Abuses, and Shortcomings of the Process." *Minn. JL Sci. & Tech.* 10 (2008): 387.
- Cohen, Daniel J. and Roy Rosenzweig. "Owning the Past: A Brief History of Copyright." in *Digital History: A Guide to Gathering, Preserving, and Presenting the Past on the Web*. available at <http://chnm.gmu.edu/digitalhistory/copyright/1.php>
- Cohen, Julie E.. "Lochner in Cyberspace: The New Economic Orthodoxy of "Rights Management." *Michigan Law Review* 97 (1998): 462.
- Cohen, Julie. "Pervasively distributed copyright enforcement." *Georgetown Law Journal* 95 (2006).
- Cohn, Cindy. "Mass Copyright Litigation: New Challenge for the Federal Courts." *Electronic Frontier Foundation*. (Apr. 19, 2011). <https://www.eff.org/deeplinks/2011/04/masscopyright-litigation-new-challenge-federal>
- Collier, David, Henry Brady, and Jason Seawright. "Source of leverage in causal inference: toward an alternative view of methodology." In: *Rethinking social inquiry: diverse tools, shared standards*. ed. H.E.Brady and D.Collier. Berkely, California: Rowman & Littlefield and Berkeley Public Press, 2004.
- Collins, Barry. "Big six ISPs capitulate to music industry." *PC Pro*, July 24, 2008. <http://www.pcpro.co.uk/news/214620/big-six-isps-capitulate-to-music-industry>
- Collins, Barry. "ISPs exaggerate the cost of data." *PC Pro*, October 7, 2011. <http://www.pcpro.co.uk/news/broadband/370393/isps-exaggerate-the-cost-of-data>
- Collins, John. "Eircom to cut broadband over illegal downloads." *Irish Times*, May 24, 2010. <http://www.irishtimes.com/newspaper/frontpage/2010/0524/1224271013389.html>

- Collins, John. "Three strikes rule aims to knock out music sharing." *Irish Times*, June 4, 2010. Copyrights & Campaigns ((June 20, 2009).
<http://copyrightsandcampaigns.blogspot.com/2009/06/sony-bmg-attomey-we-were-shocked-by.html>
- Cornes, Richard and Todd Sandler. *The theory of externalities, public goods, and club goods*. (Cambridge University Press, 1996).
- Corredoira, Loreto. "Anti-piracy Laws and Censorship Governance." *Paper for the ECREA Conference* (2012).
http://mediagovernance.univie.ac.at/fileadmin/user_upload/p_mediagovernance_industriesresearchgroup/Papers/Paper_Anti-piracy_Laws_and_Censorship_Governance_Pfra_Loreto_CORREDOIRA_Istanbul_.pdf
- Cuevas, Ruben and others. "Is Content Publishing in BitTorrent Altruistic or Profit-Driven?" *Proceedings of ACM CoNext* (2010).
- Curshing, Tim. "Swedish Study Shows File Sharing and Music Buying Go Hand-in-Hand." *Techdirt*, November 18, 2011.
<http://www.techdirt.com/articles/20111118/02101616810/swedish-study-shows-file-sharing-music-buying-go-hand-in-hand.shtml>
- Cushing, Tim. "Starz, Netflix and How Industry Jealousies Strangle a Golden Goose." *Techdirt*, September 2, 2011. <http://www.techdirt.com/articles/20110901/20203315773/starz-netflix-how-industry-jealousies-strangle-golden-goose.shtml>
- d'Astous, Alain, Francois Colbert, and Daniel Montpetit. "Music Piracy on the Web – How effective are anti-piracy arguments? Evidence from the theory of planned behavior," 28 *Journal of Consumer Policy*(2005): 289.
- Danaher, Brett, Michael D. Smith and Rahul Telang. "Did HADOPI cause an increase in iTunes music sales in France?." *Infojustice.org*, March 14, 2012.
<http://infojustice.org/archives/8891>
- Danaher, Brett, Michael D. Smith, and Rahul Telang. "Piracy and Copyright Enforcement Mechanisms" (may 2013). forthcoming in: *Innovation Policy and the Economy*. volume 14. ed. Lerner and Stern. University of Chicago Press, Chicago, Illinois.
- Danaher, Brett, Michael D. Smith, Rahul Telang and Siwen Chen. "The effect of graduated response anti-piracy laws on music sales: evidence from an event study in France." *The Journal of Industrial Economics* 62.3 (2014): 541-553.
- Datoo, Siraj. "France drops controversial 'Hadopi law' after spending millions." *the Guardian*, July 9, 2013. <http://www.theguardian.com/technology/2013/jul/09/france-hadopi-law-anti-piracy>
- Davis, Michael. "Time and Punishment: An Intertemporal Model of Crime." *Journal of Political Economy*. 96.21 (1988). 383-390.
- Dayal, Geeta. "The Algorithmic Copyright Cops: streaming video's robotic overlords." *Wired*, June 9, 2012. <http://www.wired.com/threatlevel/2012/09/streaming-videos-robotic-overlords-algorithmic-copyright-cops/all/>
- De Beer, Jeremy and Christopher Clemmer. "Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?." *Jurimetrics* (2009): 375-409.
- De Bruijn, Hans. *Framing*. Atlas Uitgeverij, October 2011.
- de Gucht, Karel. "ACTA: Making the right choice." *speech for the European Commission* , June 20, 2012. http://europa.eu/rapid/press-release_SPEECH-12-477_en.htm

- de Haes, Andreas Udo "Downloaden toegenomen na Pirate Bay-blokkade – UPDATE." *Webwereld*, August 22, 2013. <http://webwereld.nl/e-commerce/78996-downloaden-toegenomen-na-pirate-bay-blokkade---update>
- de Haes, Andreas Udo. "UvA: Pirate Bay-blokkade heeft geen effect." *Webwereld*, April 13, 2012. <http://webwereld.nl/nieuws/110183/uva--pirate-bay-blokkade-heeft-geen-effect.html>
- de Haes, Andreas Udo. "XS4ALL: torrents toegenomen na Pirate Bay-blokkade." *Webwereld*, July 4, 2012. <http://webwereld.nl/nieuws/111053/xs4all--torrents-toegenomen-na-pirate-bay-blokkade.html>
- de Joode, Alex. "LeaseWeb first hosting provider worldwide to launch Law Enforcement Transparency Report." *Leaseweb blog*, April 11, 2013. <http://blog.leaseweb.com/2013/04/11/leaseweb-first-hosting-provider-worldwide-to-launch-law-enforcement-transparency-report/>
- Dean, Katie. "Senator takes a swing at RIAA." *Wired*, September 17, 2003.
- DeBriyn, James. "Shedding Light on Copyright Trolls: An Analysis of Mass Copyright Litigation in the Age of Statutory Damages." *UCLA Entertainment Law Review* 19.1 (2012).
- Delgado, Richard and Jean Stefancic. *Understanding words that wound*. Westview Press. 2004.
- Demsetz, Harold. "Toward a theory of property rights." *The American economic review* (1967): 347-359.
- Dent, Chris. "Copyright as (Decentered) Regulation: Digital Piracy as a Case Study." *Monash UL Rev.* 35 (2009): 348.
- Dickman, Joshua M. "Anonymity and the Demands of Civil Procedure in Music Downloading Lawsuits." *TUL. L. REv.* 82: 1049 (2008).
- DiCola, Peter. "Money from Music: Survey Evidence on Musicians' Revenue and Lessons About Copyright Incentives." *Arizona Law Review. Forthcoming; Northwestern Law & Econ Research Paper* No. 13-01 (January 9, 2013). Available at SSRN: <http://ssrn.com/abstract=2199058>
- DiepField blog. "The rise and fall of P2P." *DeepField blog*, April 10, 2012. <http://blog.deepfield.net/2012/04/10/the-rise-and-fall-and-rise-of-p2p/>, last viewed February 1, 2012.
- Digital Music News. "P2P Volume Climbs Again in June, User Levels Near 9 Million." *Digital Music News Blog*, July 8, 2005.
- Digital Rights Ireland. "Three unproven accusations and you're out - why the Eircom/IRMA deal is bad for Internet users." *Digital Rights Ireland*, January 29, 2009. <http://www.digitalrights.ie/three-unproven-allegations-and-youre-out/>
- Doctorow, Cory. "More incompetence revealed on the part of France's "three-strikes" copyright enforcer." *Boingboing*, May 26, 2011. <http://boingboing.net/2011/05/26/more-incompetence-re.html>
- Doctorow, Cory. "Wikileaks cables reveal that the US wrote Spain's proposed copyright law." *Boingboing*, December 3, 2010. http://boingboing.net/2010/12/03/wikileaks-cables-rev.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A%20boingboing%2FiBag%20%28Boing%20Boing%29
- Dommering, Egbert and others. *Informatierecht, fundamentele rechten voor de Informatiesamenleving*. Amsterdam: Otto Cramwinckel, 2000.
- Drajem, Mark. "Senator Warren Presses White House to Release Pacific Trade Text." *Bloomberg.com*, June 13, 2013. <http://www.bloomberg.com/news/articles/2013-06-13/senator-warren-presses-white-house-to-release-pacific-trade-text>

- Drechsler, C.T. Annotation. "Extent of Doctrine of "Fair Use" under Federal Copyright Act." 23 *A.L.R.3d* 139 (1969).
- Dregde, Stuart. "YouTube reveals \$1bn music payouts, but some labels still unhappy." *The Guardian*, February 3, 2014. <http://www.theguardian.com/technology/2014/feb/03/youtube-reveals-1bn-music-payouts-but-some-labels-still-unhappy>
- Dworkin, Ronald. *Principle, Policy, Procedure in A Matter of Principle*. Harvard University Press, 1985.
- Easley, David and Jon Kleinberg. *Networks, crowds, and markets: Reasoning about a highly connected world*. Cambridge University Press, 2010.
- Ebere Izuogu, Chukwuyere . "The Interim Digital Britain Report, File Sharing and the Emerging Role of Internet Service Providers "(May 30, 2009). Available at SSRN: <http://ssrn.com/abstract=1601787>
- Edwards, Lillian. *Role and responsibility of the Internet intermediaries in the field of copyright and related rights*. Geneva: World Intellectual Property Organisation, 2011.
- Ehrlich, Isaac. "Participation in Illegitimate Activities: A Theoretical and Empirical Investigation." *Journal of Political Economy* 81.3 (1973): 521-565.
- Eide, Erling. "Recent developments in Economics of Crime." *German Working Papers in Law and Economics* 1 (2004).
- El Mundo. "Casi 80 solicitudes telemáticas de cierre de sitios el primer mes de la Ley Sinde." *El mundo.es*, April 1, 2012. <http://www.elmundo.es/elmundo/2012/04/01/navegante/1333276914.html>
- Electronic Frontier Foundation. "DirectTV to Narrow Anti-Piracy Campaign." *The Electronic Frontier Foundation*, June 16, 2004. <https://www.eff.org/effector/17/22>
- Electronic Frontier Foundation. "In the Matter of the Seizure of the Internet Domain Name "Dajaz1.com"". *Electronic Frontier Foundation*. <https://www.eff.org/nl/cases/matter-seizure-Internet-domain-name-dajaz1com>
- Electronic Frontier Foundation. "EFF Calls Foul on Robo-Takedowns." *Electronic Frontier Foundation*, March 6, 2012. <https://www.eff.org/press/releases/eff-calls-foul-robotakedowns>
- Electronic Frontier Foundation. "Unsafe Harbors: Abusive DMCA Subpoenas and Takedown Demands." *Electronic Frontier Foundation*, September 25, 2003. <https://www.eff.org/wp/unsafe-harbors-abusive-dmca-subpoenas-and-takedown-demands>
- Electronic Frontier Foundation. "USCG v. The People." *Electronic Frontier Foundation*. <https://www.eff.org/uscg> (last visited October 28, 2010)
- Electronic Frontier Foundation. *RIAA v The People: Five years later*. 2008, <https://www.eff.org/wp/riaa-v-people-five-years-later>
- Elkin-Koren, Niva. "It's All About Control: Rethinking Copyright in the New Information Landscape." In: *The Commodification of Information*. ed. Niva Elkin-Koren, and Neil W. Netanel. The Hague: Kluwer Law international 2002.
- Elkin-Koren, Niva. "A democratic approach to copyright in cyberspace." *Cardozo arts & entertainment* 14 (1996): 215.
- Engstrom, Christian. "Copyright law turns kids into criminals - Reform will enrich artists and the public." *New Europe Online*, October 1, 2011. <http://www.neurope.eu/blog/copyright-law-turns-kids-criminals-reform-will-enrich-artists-and-public>

Enigmax. "Golden Eye Hit UK With Piracy Letters, First Innocent Step Forward." *Torrentfreak*, February 1, 2013. <http://torrentfreak.com/golden-eye-hit-uk-with-piracy-letters-first-innocents-step-forward-130201/>

Enigmax. "Pirate Bay enjoys 12 million traffic boost, shares unblocking tips." *Torrentfreak*, May 2, 2012. <http://torrentfreak.com/pirate-bay-enjoys-12-million-traffic-boost-shares-unblocking-tips-120502/>

Enigmax. "Spanish 'SOPA': 79 site takedown requests in first month." *Torrentfreak*, April 4, 2012. <http://torrentfreak.com/spanish-sopa-79-site-takedown-requests-in-first-month-120404/>

Enigmax. "Swedish Internet traffic recovers after initial IPRED scare." *Torrentfreak*, November 13, 2009. <http://torrentfreak.com/swedish-Internet-traffic-recovers-after-initial-ipred-scare-091113/>

Enigmax. "Three strikes anti-piracy budget "Too expensive to justify" says minister." *Torrentfreak*, August 3, 2012. <http://torrentfreak.com/three-strikes-anti-piracy-budget-too-expensive-to-justify-says-minister-120603/>

Enigmax. "World's unluckiest bittorrent pirate fined but avoids jail." *Torrentfreak*, February 12, 2012. <http://torrentfreak.com/worlds-unluckiest-bittorrent-pirate-fined-but-avoids-jail-120212/>

Enigmax. You're caught downloading "Dream Pinball," settle now or go broke." *TorrentFreak*, March 31, 2007.

Envisional. *Mininova: Assessment of Copyrighted Torrent Link Removal* (2010).

Ernesto. "200,000 Bittorrent users sued in the United States." *Torrentfreak*, August 8, 2011. <http://torrentfreak.com/200000-bittorrent-users-sued-in-the-united-states-110808/>

Ernesto. "60-year old file-sharer gets 2 years probation and fine." *Torrentfreak*, August 31, 2011. <http://torrentfreak.com/60-year-old-file-sharer-gets-2-years-probation-and-fine-110831/>

Ernesto. "Anti-piracy lawyers sue dead person." *Torrentfreak*, August 26, 2011. <http://torrentfreak.com/anti-piracy-lawyers-sue-dead-person-110826/>

Ernesto. "Anti-piracy warnings have no effect on iTunes sales." *Torrentfreak*, January 24, 2012. <http://torrentfreak.com/anti-piracy-no-effect-on-itunes-sales-120124/>

Ernesto. "Economists urge government to stop war on piracy." *Torrentfreak*, March 27, 2010. <http://torrentfreak.com/economists-urge-government-to-stop-war-on-piracy-100327/>

Ernesto. "France starts reporting 'millions' of file-sharers." *Torrentfreak*, September 21, 2010. <http://torrentfreak.com/france-starts-reporting-millions-of-file-sharers-100921/>

Ernesto. "French 'three strikes' law slashes piracy, but fails to boost sales." *Torrentfreak*, March 30, 2012. <http://torrentfreak.com/french-three-strikes-law-slashes-piracy-but-fails-to-boost-sales-120330/>

Ernesto. "Google discarded 21,000,000 takedown requests in 2013'." *Torrentfreak*, December 27, 2013. <http://torrentfreak.com/google-discarded-21000000-takedown-requests-in-2013-131227/>

Ernesto. "Google relaxes DMCA Takedown restrictions. eyes abuse." *Torrentfreak*, April 11, 2013. <http://torrentfreak.com/google-relaxes-dmca-takedown-restrictions-eyes-abuse-130411/>

Ernesto. "Law to shutdown P2P sites resurrected by Spanish coalition." *Torrentfreak*, January 25, 2011. <http://torrentfreak.com/law-to-shutdown-p2p-sites-resurrected-by-spanish-coalition-110125/>

- Ernesto. "Millions of file-sharers hide their identities online." *Torrentfreak*, November 3, 2009. <http://torrentfreak.com/millions-of-file-sharers-hide-their-identities-online-091103/>
- Ernesto. "Pirate Bay ready for perpetual IP-address whac-a-mole." *Torrentfreak*, May 28, 2012. <https://torrentfreak.com/pirate-bay-ready-for-perpetual-ip-address-whac-a-mole-120528/>
- Ernesto. "Tech News Sites Tout Misleading BitTorrent Piracy Study." *Torrentfreak*, July 24, 2010. <http://torrentfreak.com/tech-news-sites-tout-misleadingbittorrent-piracy-study-100724/>
- Ernesto. "US ISP Disconnects Alleged Pirates for 6 Months." *Torrentfreak*, 24 September 2010. <https://torrentfreak.com/us-isp-disconnects-alleged-pirates-for-6-months-100924/>
- Essers, Loek. "Fransen nemen half miljoen file sharers op de korrel." *Webwereld*, July 14, 2011. <http://webwereld.nl/nieuws/107298/fransen-nemen-half-miljoen-filesnarers-op-de-korrel.html>. accessed on Oct 26, 2011.
- Euractiv. "Brussels denies rumours of secret anti-piracy treaty." *Euractiv*, February 4, 2010. <http://www.euractiv.com/infosociety/brussels-denies-rumours-secret-anti-piracy-treaty>
- European Commission. "Lack of choice driving demand for film downloads." *European Commission press release*, February 6, 2014. http://europa.eu/rapid/press-release_IP-14-120_en.htm
- European Commission. *Commission staff working document on Online services, including e-commerce, in the Single Market*. 11.1.2012. {SEc(2011)1640 final}.
- European Observatory on Infringements of Intellectual Property Rights "IP in Europe." *European Observatory on Infringements of Intellectual Property Rights*. <https://oami.europa.eu/ohimportal/nl/web/observatory/ip-in-Europe>
- Falkvinge, Rick. "Horrorific: Two Years, Heavy Fine For 60-Year-Old Music File Sharer." *Falkvinge&co on infopolicy*, August 31, 2011. <http://falkvinge.net/2011/08/31/horrific-two-years-heavy-fine-for-60-year-old-music-file-sharer/>
- Falot, Nathalie. "Hadopi three years later: 1.15 million notices result in two convictions." *Future of Copyright*, December 31, 2012. <http://www.futureofcopyright.com/home/blog-post/2012/12/31/HADOPI-three-years-later-115-million-notices-result-in-two-convictions.html>
- Farivar, Cyrus. "Disney Anoints Netflix as Its Exclusive Distributor Starting in 2016." *Ars Technica*, December 4, 2012. <http://arstechnica.com/business/2012/12/disney-anoints-netflix-as-its-exclusive-distributor-starting-in-2016/>
- Feinberg, Joel. "Limits to the Free Expression of Opinion." in: *Philosophy of Law*, ed. Joel Feinberg and Hyman Gross. Wadsworth Pub co, 1995.
- Ferran, Benjamin. "Le bilan contrasté de l'action de l'Hadopi." *le Figaro*, March 28, 2012. <http://www.lefigaro.fr/secteur/high-tech/2012/03/27/01007-20120327ARTFIG00670-le-bilan-contrastee-de-l-action-de-l-hadopi.php>
- Filtz, Michael. "File-sharing in Germany: Could the cost of getting caught be about to come down?." *ZDNet*, August 9, 2013. <http://www.zdnet.com/file-sharing-in-germany-could-the-cost-of-getting-caught-be-about-to-come-down-7000018915/>
- Fisher, Ken. "Students largely ignore RIAA instant settlement offers." *Ars Technica*, March 26, 2007.
- Fisher, William. *Promises to keep: Technology, law, and the future of entertainment*. Stanford University Press, 2004.
- Foglesong, Todd, Zainab Latif; Cybele Merrick; Joel Miller; James Parsons; Timothy Ross. "Measuring Progress toward Safety and Justice: A Global Guide to the Design of Performance Indicators across the Justice Sector." *Vera Institute of Justice* (2003).

Fraguas, Antonio. "EE UU afeó a Zapatero la decisión de no aprobar la 'ley Sinde'." *El Pais*, January 4, 2012.
http://cultura.elpais.com/cultura/2012/01/03/actualidad/1325545206_850215.html

FreeAdvice. "DirecTV Lawsuit on End Users." *FreeAdvice*, February 10, 2001.
<http://forum.freeadvice.com/civil-litigation-46/directv-lawsuit-end-users-77220.html>

Freedom house. "Methodology for measuring political rights and civil liberties." on website:
<http://www.freedomhouse.org/report/freedom-world/freedom-world-2012>

Freeman, Richard. "The economics of crime." *Handbook of labor economics* 3 (1999): 3529-3571.

Freeman, Richard. "Who Escapes? The Relation of Church-Going & Other Background Factors to the Socio-Economic Performance of Blk. Male Yths. from Inner-City Pvrty Tracts." *National Bureau of Economic Research* No. w1656 (1985).

FrenchKat. "HADOPI: Where Things Stand." *1709 Blog*, December 31, 2012.
<http://the1709blog.blogspot.nl/2012/12/hadopi-where-things-stand.html>

Fritz, Ben. "Apple prepping movie cloud service." *LA Times*, October 12, 2011.
<http://latimesblogs.latimes.com/entertainmentnewsbuzz/2011/10/apple-prepping-movie-cloud-service-devices-may-work-with-ultraviolet.html>

Fritz, Michael. "File-sharing in Germany: Could the cost of getting caught be about to come down?" *ZDNet*, August 9, 2013. <http://www.zdnet.com/file-sharing-in-germany-could-the-cost-of-getting-caught-be-about-to-come-down-7000018915/>

Fry, William. "3 strikes - Supreme Court rejects Data Protection Commissioner's appeal." *Lexology*, July 24, 2013. <http://www.lexology.com/library/detail.aspx?g=33062c2f-205a-471a-a8ef-ef0cae5e7c0d>

Fung, Brian. "How Microsoft killed off a massive botnet, with trademark law." *The Washington Post*, July 24, 2013.
<http://www.washingtonpost.com/blogs/wonkblog/wp/2013/07/24/how-microsoft-killed-off-a-massive-botnet-with-trademark-law/>

Future of Music Coalition. "Mythbusting: Data Driven Answers to Four Common Assumptions About How Musicians Make Money." *Future of Music Coalition*, December 13, 2012.
<http://money.futureofmusic.org/mythbusting/4/>

Gabbatt, Adam and OWen Bowcott. "Richard O'Dwyer's two-year extradition ordeal ends in Nw York." *the Guardian* (December 7 2012),
<https://www.theguardian.com/uk/2012/dec/06/richard-o-dwyer-avoids-us-extradition>

Gain, Bruce. "Special report: music industry's lavish lobby campaign for digital rights." *Intellectual property watch*, January 6, 2011. www.ip-watch.org/weblog/2011/01/06/special-report-music-industrys-lavish-lobby-campaign-for-digital-rights

Gallie, WB. "Essentially contested concepts." *Proceeding of the Aristotelian society* 51: 167-98 (1956).

Garcia, Rocio. "Gobierno y PP pactan una 'ley Sinde' con más garantías judiciales." *El Pais*, January 24, 2011.
http://cultura.elpais.com/cultura/2011/01/24/actualidad/1295823605_850215.html

Gardner, Eric. "YouTube Again Beats Viacom's Massive Copyright Infringement Lawsuit." *The Hollywood Reporter*, April 18, 2013. <http://www.hollywoodreporter.com/thr-esq/youtube-again-beats-viacoms-massive-442233>

- Gardner, Eric. "Spain Escapes U.S. Trade Rep's Piracy 'Watch List'." *The Hollywood Reporter*, May 1, 2013. <http://www.hollywoodreporter.com/thr-esq/spain-escapes-us-trade-reps-450185>
- Gardner, Eriq. "New Litigation Campaign Quietly Targets Tens of Thousands of Movie Downloaders." *HOLLYWOOD REP.* (Dec. 21, 2010). <http://www.hollywoodreporter.com/blogs/thr-esq/litigation-campaign-quietly-targets-tens-63769>
- Gasser, Urs. Copyright and Digital Media in a Post-Napster World: 2005 Update. *Berkman Publication Series* 2005-03.
- Geiger, Christophe. "Challenges for the Enforcement of Copyright in the Online World: Time for a New Approach" in: *Research Handbook on the Cross-border Enforcement of Intellectual property*. ed. Paul torremans. Edward Elgar Publishing, 2014.
- Geigner, Timothy. "Game Developer Connects With Pirates, Sees Massive Support & Deletion of Torrents." *Techdirt*, February 13, 2013. <https://www.techdirt.com/articles/20130212/10325521952/game-developer-connects-with-pirates-sees-massive-support-deletion-torrents.shtml>
- Geist, Michael. "Music Rights Holders Send 25,000 Copyright Notices in France Daily". *Michael Geist*, October 25, 2010. <http://www.michaelgeist.ca/2010/10/hadopi-25k-notices/>
- Geist, Michael. "Canadian-backed report says music, movie, and software piracy is a market failure, not a legal one." *Business at the Star*, March 18, 2011. <http://www.thestar.com/business/article/956637--geist-canadian-backed-report-says-music-movie-and-software-piracy-is-a-market-failure-not-a-legal-one>
- George, Alexander, and Andrew Bennett. *Case studies and theory development in the social sciences*. Cambridge, Massachusetts, MIT Press, 2005.
- Gerring, John. *Case study Research, principles and practices*. Cambridge University Press, 2007.
- Giannopoulou, Alexandra. "Copyright enforcement measures: the role of the ISPs and the respect of the principle of proportionality." *European Journal for Law and Technology*. Vol. 3. 1, (2012). <http://ejlt.org/article/viewArticle/122/204>
- Giblin, Rebecca. "Evaluating Graduated Response." *Columbia Journal of Law & the Arts* 37 (2014): 147.
- Gibson, John S. *Dictionary of International Human Rights Law*. Lanham, Md.m & London: The Scarecrow Press, Inc. 1996.
- Gielen, Charles, Adonna Alkema, Paul Geerts, Margreet Groenenboom, Ruprecht Hermans, Richard van Oerle, Anne Marie Verschuur. *Kort begrip van het Intellectuele Eigendomsrecht*. Deventer: Uitgeverij Kluwer, 2011.
- Glaeser, Edward. "An overview of crime and punishment." Washington: *World Bank*. Mimeographed (1999).
- Gordon, Wendy. "Fair use as market failure: a structural and economic analysis of the "Betamax" case and its predecessors." *Columbia Law Review* (1982): 1600-1657.
- Graham, Lee. "The NPD Group: Music File Sharing Declined Significantly in 2012." *NPD Group*, February 26, 2012. <https://www.npd.com/wps/portal/npd/us/news/press-releases/the-mp3-group-music-file-sharing-declined-significantly-in-2012/>
- Green, Maria. "What we talk about when we talk about indicators: current approaches to human rights measurement." *Human Rights Quarterly* 23 (2001) 1062-1097.
- Green, Thomas C.. "MPAA, RIAA Sue Scour Over Copyrights." *The Register*, July 24, 2000.
- Griggs, Brandon. "Amazon e-Books Now Outselling Print Books." *CNN*, May 19, 2011. <http://edition.cnn.com/2011/TECH/gaming.gadgets/05/19/kindle.outsells.books/index.html?hpt=T2>

Gross, Grant. "Congress scrutinizes RIAA Tactics." *IDG News*, September 17, 2003.

HADOPI. "L'Essentiel du Rapport D'Activité. 2010. Paris: HADOPI, 2011.

HADOPI. "Réponse Graduée." accessed Apr. 5, 2012. <http://www.HADOPI.fr/usages-responsables/nouvelles-libertes-nouvelles-responsabilites/reponse-graduee.html>

HADOPI. *HADOPI: 1.1/2 year after the launch*. (2012). available at: http://www.HADOPI.fr/sites/default/files/page/pdf/note17_en.pdf

HADOPI. *Réponse graduée – Les chiffres clés*. August 2013. http://www.HADOPI.fr/sites/default/files/page/pdf/Chiffresreponsegraduee_aout.pdf

HADOPI. *Réponse graduée – Les chiffres clés*. July 2014. http://HADOPI.fr/sites/default/files/page/pdf/20140716_Point_presse_CPD_Vdef3_0.pdf

HADOPI. *Report Annuel 2013*.

Halliday, Josh. "ACS:Law solicitor 'breached code with filesharing claims'." *The Guardian*, April 19, 2011. <http://www.theguardian.com/technology/2011/apr/19/acs-law-solicitor-filesharing-claims>

Halliday, Josh. "Illegal filesharing: is this the end of 'speculative invoicing'?" *The Guardian*, January 27, 2011. <http://www.theguardian.com/technology/blog/2011/jan/27/illegal-file-sharing-acslaw>

Halliday, Josh. "Law firm could face £500,000 fine over data breach." *The Guardian*, September 28, 2010. <http://www.theguardian.com/media/2010/sep/28/filesharing-acs-law>

Hamel, E. (2009). "Jaaromzet Mininova 1 miljoen euro." *Webwereld.nl*, March 13, 2009. <http://webwereld.nl/nieuws/56410/jaaromzet-mininova-1-miljoen-euro.html>

Hamilton, Keegan. "Porn, Piracy and Bit Torrent." *Seattle Weekly*, August 10, 2011. <http://www.seattleweekly.com/2011-08-10/news/porn-piracy-bittorrent/>

Hammergren, Linn. "Diagnosing Judicial Performance: toward a tool to help guide judicial reform programs." Latin America and the Caribbean Region. *World Bank*, Washington DC (2000).

Handke, Christian, Bodo Balazs, Joan-Josep Vallbé. "The value of online licenses for recorded music." *Paper presented at Annual Congress of the Society for Economic Research on Copyright Issues*. (2014).

Hardy, Trotter. *Project looking forward: sketching the future of copyright in a networked world: final report*. May 1998. U.S. copyright Office, Library of Congress, 1998.

Hargreaves, Ian. *Digital opportunity: A review of Intellectual property and growth*. An Independent report (May 2011). <http://webarchive.nationalarchives.gov.uk/20140603093549/http://www.ipo.gov.uk/ipreview.htm>

Harrell, Michael J. "Fighting Piracy with Censorship: The Operation in Our Sites Domain Seizures v. Free Speech." *21 Journal of Intellectual Property Law* 137 (2013).

Harris Interactive. *Growing threat from illegal web downloads* (2009). <http://www.wipo.int/ip-outreach/en/tools/research/details.jsp?id=2479>

Harris, John. "On the Economics of Law and Order." *Journal of Political Economy* 78.1 (1970). 165-174.

Havoscope. "Online Piracy Rate in the UK in 2012-2013." *Havoscope*. <http://www.havoscope.com/online-piracy-rate-in-the-uk-in-2012-2013/> Last viewed on: February 13, 2014.

Hazelwood Jr, Charles W.. "Fair Use and the Takedown/Put Back Provisions of the Digital Millennium Copyright Act." *Idea* 50 (2009): 307.

- Hazlett, Thomas W., David Porter, Vernon L. Smith. "Radio Spectrum and the Disruptive Clarity of Ronald Coase." *Journal of Law & Economics* 54.21 (2011): S125.
- Heald, Paul J.. "How Notice-and-Takedown Regimes Create Markets for Music on YouTube: An Empirical Study" (March 26, 2014). Available at SSRN: <http://ssrn.com/abstract=2416519>
- Healey, Jon. "Another File-sharer Faces Costly Day of Reckoning." *L.A. Times Technology Blog*, September 2, 2008.
- Hervas-Drane, Andres and Eli M. Noam. "Peer-to-Peer File Sharing and Cultural Trade Protectionism." (September 2014).
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1793131
- Hickson, Ian. *through Google +*, March 19, 2013.
<https://plus.google.com/+IanHickson/posts/iPmatxBYuj2>
- Higgins, Parker and Maira Sutton. "Hollywood, Take Note: New Website Shows Movie Watchers Get What They Want." *Electronic Frontier Foundation*, October 18, 2013.
<https://www.eff.org/deeplinks/2013/10/hollywood-take-note-new-website-shows-movie-watchers-cant-get-what-they-want>
- Higgins, Parker. "In "A Copyright Masquerade," Corporate Lobbying Takes the Spotlight." *Electronic Frontier Foundation*, September 30, 2013.
<https://www.eff.org/deeplinks/2013/09/copyright-masquerade-corporate-lobbying-takes-spotlight>
- Hinze, Gwen. "EU Law does not require ISP to hand over customers' identity data in alleged filesharing case." *Electronic Frontier Foundation*, January 30, 2008.
<https://www.eff.org/deeplinks/2008/01/eu-law-does-not-require>
- Horten, Monica. "France puts copyright in contract." *IPtegrity.com*, August 30, 2011.
<http://www.iptegrity.com/index.php/france/687-france-puts-copyright-in-isp-contract>
- Horten, Monica. "Briefing on France's Creation and Internet Law – DRAFT." *IPtegrity*, November 11, 2008.
<http://www.iptegrity.com/pdf/Monica.Horten.creation.Internet.law.2.11.2008.pdf>
- Horten, Monica. "Hadopi – has it massaged the numbers?." *IPtegrity.com*, March 31, 2012.
<http://www.iptegrity.com/index.php/france/755-hadopi-has-it-massaged-the-numbers>
- Horten, Monica. *The Copyright Enforcement Enigma, Internet Politics and the 'Telecoms Package*. palgrave MacMillan, 2012.
- Houghton, Bruce. "Spotify Offers Additional Response to Independent Label Defections." *Hypebot.com*, September 20, 2011. <http://www.hypebot.com/hypebot/2011/09/spotify-offers-additonal-response-to-independent-label-defections.html>
- Hughenoltz, Bernt. "Copyright and freedom of expression in Europe." in: *Expanding the Boundaries of Intellectual Property*. ed. Rochelle Cooper Dreyfuss, Harry First and Diane Leenheer Zimmerman. Oxford: Oxford University Press, 2001.
- Hughenoltz, Bernt. *Auteursrecht op informatie*. Deventer: Kluwer 1989.
- Hughenoltz, Bernt. "Codes of Conduct and Copyright Enforcement in Cyberspace." *Copyright enforcement and the Internet, Information law series* 21 (2012): 303-320.
- Humphries, Matthew. "Movie Industry Buries Report Proving Pirates are Great Consumers." *Geek.com*, July 20, 2011. <http://www.geek.com/articles/geek-cetera/movie-industry-bins-report-proving-pirates-are-great-consumers-20110720/>
- Hunt, Cassi. "Run Over by the RIAA Don't Tap the Glass." *The Tech*, April 4, 2006.
- Hunt, Robin, Peter Williams, Ian Rowlands and David Nicholas. *Copycats? Digital consumers in the online age, a CIBER report for the strategic advisory board for intellectual property*

- policy* (University College London, May 2009). <http://ciber-research.eu/download/20090601-SABIP-main-1.pdf>
- Hurips. "National Human Rights Body Recommends Abolishing Three-Strike-Out Rule." *Heesob's IP blog*, March 27, 2013. <http://hurips.blogspot.kr/2013/03/national-human-rights-body-recommends.html>
- Huygen, Annelies, Natali Helberger, Joost Poort, Paul Rutten, Nico van Eijk. "Ups and downs; economic and cultural effects of file sharing on music, film and games." *TNO Information and Communication Technology Series* (2009).
- Independent. "Ireland Cracks Down on Internet Piracy." *Independent*, May 29, 2010. <http://www.independent.co.uk/news/media/ireland-cracks-down-on-Internet-piracy-1986733.html>
- International Federation of the Phonographic Industry. *Digital Music Report 2010* (IFPI 2010).
- International Federation of the Phonographic Industry. *Digital Music Report 2011* (IFPI 2011).
- International Federation of the Phonographic Industry. *Digital Music Report 2009* (IFPI 2009).
- International Federation of the Phonographic Industry. Public Consultation on Creative Content Online in the Single Market – Submission of the "International Federation of the Phonographic Industry" (IFPI) in response to the Questionnaire of the European Commission regarding Policy/Regulatory Issues (February 29, 2008). http://ec.europa.eu/avpolicy/docs/other_actions/col_2008/ngo/ifpi_en.pdf
- International Intellectual Property Alliance (IIPA). *Special 301 Report on Copyright Enforcement and Protection on Spain*. (2011). <http://www.iipa.com/rbc/2011/2011SPEC301SPAIN.pdf>
- Internet Society. "Perspectives on Policy Responses to Online Copyright Infringement, an Evolving Policy Landscape." *Internet Society website*. February 20, 2011. <http://www.Internetsociety.org/perspectives-policy-responses-online-copyright-infringement-evolving-policy-landscape>
- Jackson, Mark. "BPI Claims 7 Million UK People Use Illegal Internet Piracy Services." *ISPreview*, February 7, 2013. <http://www.ispreview.co.uk/index.php/2013/02/bpi-claims-7-million-uk-people-use-illegal-Internet-piracy-services.html>
- Jackson, Mark. "Fake UK ISP Internet Piracy Warning Letters Expose Obvious DEAct Flaw." *ISPreview*, July 2, 2012. <http://www.ispreview.co.uk/index.php/2012/07/fake-uk-isp-Internet-piracy-warning-letters-expose-obvious-deact-flaw.html?>
- Jackson, Mark. "Ofcom Claims 16 Percent of UK Internet Users Make Illegal Downloads." *ISPreview*, March 7, 2013. <http://www.ispreview.co.uk/index.php/2013/03/ofcom-study-claims-6-7-million-illegal-downloaders-in-the-uk.html>
- Johns, Adrian. *Piracy: The intellectual property wars from Gutenberg to Gates*. University of Chicago Press, 2009.
- Johnson, Byron. *More God, Less Crime*. Templeton Press, 2011.
- Johnson, Ted. "Showbiz Lobby Puts Capitol Hill Pressure on Google to Take Action on Piracy." *Variety*, September 18, 2013. <http://variety.com/2013/digital/news/google-pressured-by-hollywood-to-do-more-to-fight-piracy-1200616306/>
- Jones, Ben. "How Any BitTorrent User Can Collect Lawsuit Evidence." *Torrentfreak*, September 3, 2010. <http://torrentfreak.com/how-any-bittorrent-user-can-collect-lawsuit-evidence-100903/>
- Julien L.. "La France avec son Hadopi, 1er fournisseur de clients pour Mega." *Numérama*, February 16, 2013. <http://www.numerama.com/magazine/25117-la-france-avec-son-HADOPI-1er-fournisseur-de-clients-pour-mega.html>

- Kafka, Peter. "Warner Brothers Will Make Netflix, Redbox, Blockbuster Wait Longer for New Movies." *All Things D*, January 5, 2012. <http://allthingsd.com/20120105/warner-brothers-will-make-netflix-redbox-blockbuster-wait-longer-for-new-movies>
- Kantar Media. "OCI Tracker Benchmark Study, 'Deep Dive' Analysis Report." *Prepared for Ofcom*, 2013. <http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/online-copyright/deep-dive.pdf>
- Kaplow, Louis. "The value of accuracy in adjudication: An economic analysis." *The Journal of Legal Studies* (1994): 307-401.
- Karaganis, Joe and Lennart Renkema. "Copy culture in the US & Germany." *the American Assembly* (2013).
- Karaganis, Joe and Lennart Renkema. "Copy Culture in the US and Germany." Columbia University: *The American Assembly* (2012).
- Karaganis, Joe. "Copyright Infringement and Enforcement in the US." *The American Assembly* (November 2011). <http://piracy.americanassembly.org/wp-content/uploads/2011/11/AA-Research-Note-Infringement-and-Enforcement-November-2011.pdf>
- Karaganis, Joe. "Kill the Hobbit Subsidies to Save Regular Earth." *Bloomberg View*, December 4, 2012. <http://www.bloombergvie.com/articles/2012-12-04/kill-the-hobbit-subsidies-to-save-regular-earth>
- Karaganis, Joe. "Meganomics." *The American Assembly*. Columbia University (January 24, 2012). see: <http://piracy.americanassembly.org/meganomics/>
- Karich, Swantje. "Wer hat sie verraten? Googles YouTube-Daten!" *Frankfurter Allgemeine Feuilleton*, May 17, 2015. <http://www.faz.net/aktuell/feuilleton/debatten/YouTubes-daten-gefaehrden-islamkritiker-13247806-p3.html?printPagedArticle=true>
- Karunaratne, Sean B. "The Case against Combating BitTorrent Piracy through Mass John Doe Copyright Infringement Lawsuits." *Mich. L. Rev.* 111: 283 (2012). Available at: <http://repository.law.umich.edu/mlr/vol111/iss2/4>
- Katyal, Sonia. "Filtering, Piracy Surveillance, and Disobedience." *Columbia Journal of Law & the Arts* 32.4 (2009).
- Kaufmann, Daniel, Aart Kraay, and Massimo Mastruzzi. "The worldwide governance indicators: methodology and analytical issues." *Hague Journal on the Rule of Law* 3.02 (2011): 220-246.
- Kim, Douglas. "Asset Fofeiture: Giving Up Your Constitutional Rights." 19 *CAMPBELL L. REV.* 527, 565 (1997).
- King, Gary, Robert Keohane and Sidney Verba. *Designing social inquiry: scientific inference in qualitative research*. Princeton, NJ: Princeton university press, 1994.
- Knight, Zachary. "Gaming Company Sees Massive User & Revenue Growth Because of Piracy." *Techdirt*, October 3, 2011. <http://www.techdirt.com/articles/20110930/09182316149/gaming-company-sees-massive-user-revenue-growth-because-piracy.shtml>
- Knopper, Steve. "RIAA will keep on suing." *Rolling Stone*, June 9, 2005.
- Koenis, Chris. "BREIN meldt 10.000 'illegale' zoekresultaten per dag." *Webwereld*, January 15, 2013. <http://webwereld.nl/nieuws/113045/brein-meldt-10-000--illegale--zoekresultaten-per-dag.html>
- Koepsell, David. *Innovation and nanotechnology: Converging technologies and the end of intellectual property*. Bloomsbury Publishing, 2011.

- Koepsell, David. *The Ontology of Cyberspace: Philosophy, Law, and the Future of Intellectual Property* (2000).
- Kopel, Karen. "Operation Seizing Our Sites: How the Federal Government Is Taking Domain Names Without Prior Notice." *Berkeley Technology Law Journal* 28. (July 2013).
- Kravets, David. "File Sparing Lawsuits at a Crossroads, After 5 Years of RIAA Litigation." *Wired*, September 4, 2008. <http://www.wired.com/threatlevel/2008/09/proving-file-sh/>
- Kreiken, Floris and David Koepsell. "Coase and Copyright." *University of Illinois Journal of Law, Technology and Policy* 1 (2013): 1-44.
- Kreps, Daniel. "Richard Marx "'Ashamed" He's Linked to \$1.92 Million RIAA Fine Against Minnesota Mom." *Rolling Stone magazine* (June 24, 2009). <http://www.rollingstone.com/rockdaily/index.php/2009/06/24/richard-marx-ashamed-hes-linked-to-192-million-riaa-fineagainst-minnesota-mom>
- Kuhn, Eric. "Google unveils top political searches of 2009." *CNN*, December 18, 2009. <http://politicalticker.blogs.cnn.com/2009/12/18/google-unveils-top-political-searches-of-2009/>
- la Quadrature du Net. "Hadopi 2 validated, a defeat for the Rule of Law." *la Quadrature du Net website*, October 24, 2009. <https://www.laquadrature.net/en/hadopi-2-validated-a-defeat-for-the-rule-of-law>
- La Rue, Frank. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression." *U.N. DOC. A/HRC/17/27* (2011).
- Landes, William. "Copyright". *Handbook of Cultural Economics*. ed. Ruth Towse. Edward Elgar publishing, 2011: 132-142.
- Landman, Todd. *Studying Human Rights*. New York, Routledge, 2006.
- Larsson, Stefan. "Metaphors and Norms: Understanding Copyright Law in a Digital Society." 36 *Lund Stud. Soc. L.* 36.5 (2011).
- Lateral Economics. "Copyright reports." *report for the Australian Digital Alliance* (september 2012). <http://digital.org.au/content/LateralEconomicsReports>
- Lauinger, Tobias, Kaan Onarlioglu, Abdelberi Chaabane, Engin Kirda, William Robertson and Mohamed Ali Kaafar. "Holiday Pictures or Blockbuster Movies? Insights into Copyright Infringement in User Uploads to One-Click File Hosters." *Torrentfreak*, October 17, 2013. <http://www.scribd.com/doc/176860329/Och-Filename-Analysis-Raid2013>
- Lauinger, Tobias, Martin Szydowski, Kaan Onarlioglu, Gilbert Wondracek, Engin Kirda and Christopher Kruegel. "Clickonomics: Determining the Effect of Anti-Piracy Measures for One-Click Hosting." *Presentation at the NDSS Symposium* (2013). http://www.Internetsociety.org/sites/default/files/07_1_0.pdf
- Layton, Robert and Paul Watters. "Investigation into the extent of infringing content on BitTorrent networks." *Technical report* (Internet Commerce Security Laboratory, University of Ballarat, Australia, 2010).
- Lee, Dave. "A Glimpse at Piracy in the UK and Beyond." *BBC.com*, September 16, 2012. <http://www.bbc.com/news/technology-19599527>
- Lee, Timothy. "ISP flip-flops: why do they now support "six strikes" plan?" *Ars Technica*, July 11, 2011. <http://arstechnica.com/telecom/news/2011/07/why-did-telcos-flip-flop-and-support-six-strikes-plan.ars>
- Lee, Timothy. "New troll scam: Pay us \$495 or face felony charges and jail time." *Ars Technica*, February 22, 2013. <http://arstechnica.com/tech-policy/2013/02/new-troll-scam-pay-us-495-or-face-felony-charges-and-jail-time/>
- Leeds, Jeff. "Labels win suit against song sharer." *New York Times*, October 5, 2007.

- Leenheer, Jorna and Joost Poort. "Alleen maar nette mensen". Consumentenonderzoek Downloadgedrag Films." *IViR/CentERdata* 14 (2014).
http://www.ivir.nl/publicaties/download/alleen_maar_nette_mensen.pdf
- Lehman, Bruce A. *Intellectual property and the national information infrastructure: The report of the working group on intellectual property rights*. Diane Publishing, 1995.
- Leloup, Damian and Jérémie Baruch. "Hadopi, source de la croissance d'iTunes?." *Le Monde*, January 1, 2012. http://www.lemonde.fr/technologies/article/2012/01/24/HADOPI-source-de-la-croissance-d-itunes_1633919_651865.html
- Lemley, Mark and Eugene Volokh. "Freedom of speech and Injunctions in Intellectual Property Cases." *Duke Law Journal* 48. 2 (1998): 147-242.
- Lenhart, Amanda and Susannah Fox. "Downloading free music: Internet music lovers don't think it's stealing." *Pew Internet & American Life Project*, 2000. available at:
<http://www.pewInternet.org/reports/2000/downloading-free-music.aspx>
- Lescure, Pierre. *Mission « Acte II de l'exception culturelle » Contribution aux politiques culturelles à l'ère numérique, Ministère de la Culture et de la Communication*. May 2013.
www.culturecommunication.gouv.fr/var/culture/storage/culture_mag/rapport_lescore/index.htm#/1
- Lessig, Lawrence. *Code And Other Laws of Cyberspace, Version 2.0*. Basic Books, 2006.
- Lessig, Lawrence. *Free culture: How big media uses technology and the law to lock down culture and control creativity*. Penguin, 2004.
- Li, Victor. "Manhattan Federal Judge Kimba Wood Calls Record Companies' Request for \$75 Trillion in Damages 'Absurd' in Lime Wire Copyright Case." *Corporate counsel Register*, March 15, 2011. <http://www.corpcounsel.com/id=1202486102650/Manhattan-Federal-Judge-Kimba-Wood-Calls-Record-Companies-Request-for-75-Trillion-in-Damages-Absurd-in-Lime-Wire-Copyright-Case-#ixzz3HGfgJfPR>
- Lichtman, Douglas and William Landes. "Indirect liability for copyright infringement: an economic perspective." *Harv. JL & Tech.* 16 (2002): 395.
- Lieberman, David. "MPAA's Anti-Piracy Fight Contributed To Financial Loss In 2012 While Chris Dodd Collected \$3.3M." *Deadline*, November 20, 2013.
<http://deadline.com/2013/11/mpaas-anti-piracy-fight-contributed-to-a-financial-loss-in-2012-while-chris-dodd-collected-3-3m-639844/>
- Liebowitz, Stan. "File Sharing: Creative Destruction or Just Plain Destruction?" *Journal of Law and Economics* 49.1 (2006): 1-28.
- Lieske, Robert. "Civil Forfeiture Law: Replacing the Common Law with a Common Sense Application of the Excessive Fines Clause of the Eighth Amendment." *WM. MITCHELL L. REV.* 21 (1995):265.
- Lijphart, Arend. "Comparative politics and the comparative method." *American Political Science Review* 65 (1971): 682-93.
- Lind, Allan and Tom Tyler. *The Social Psychology of Procedural Justice*. Springer Science & Business Media, 1988.
- Litman, Jessica. *Digital Copyright*. Prometheus Books, 2001.
- Litman, Jessica. "Sharing and stealing." *Hastings communications and entertainment law journal* 27 (2004).
- Lofgren, Rep. Zoe. Lofgren, Wyden Question Response to Seizure Inquiries.
<http://commcns.org/tyiKZ>
- Logghe, Francois. "Over de "eerlijke behandeling" volgens artikel 6 van het EVRM." *Jura Falconis* 33.2 (1996-1997): 271-316.

- Lorrain, Anne-Catherine. "Copyright policymaking and the digital public domain: a bitter-sweet wishful thinking from France." *Infojustice*, May 17, 2013.
<http://infojustice.org/archives/29651>
- Lunney, Jr., Glynn. "Empirical Copyright: A Case Study of File Sharing and Music Output." *Tulane Public Law Research Paper* No. 14-2 (January 2014). Available at
<http://dx.doi.org/10.2139/ssrn.2372630>
- Macavinta, Courtney. "Recording Industry Sues Music Start-up, Cites Black Market." *CNET News.com*, December 7, 1999. <http://www.cnet.com/news/recording-industry-sues-music-start-up-cites-black-market/>
- MacKinnon, Rebecca. *Consent of the Networked: the Worldwide Struggle for Internet Freedom*. New York: Basic Books, 2012.
- Macovei, Monica. "Freedom of Expression, A guide to the implementation of Article 10 of the European Convention of Human Rights." *Council of Europe, Human rights handbooks*. No. 2.
- Madden, Mary . "The state of music online: Ten years after Napster." *Pew Internet & American Life Project*, 2009.
- Madden, Mary and Lee Rainie. "Pew Internet Project Data Memo, Re: Music and Video Downloading beyond P2P." *Pew Internet & American Life Project*, 2005.
- Magi, Trina J. "Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly Literature." *The Library Quarterly* 81.2 (2011): 187-209.
- Makarewicz, David. "5 Reasons Why the US Domain Name Seizures Are Unconstitutional," *Torrentfreak*, March 12, 2011. <http://torrentfreak.com/5-reasons-why-the-us-domain-seizures-are-unconstitutional-110312/>
- Manning, Clinton. "Internet piracy policing could add £24 to every phone bill." *Mirror*, February 3, 2012. <http://www.mirror.co.uk/money/city-news/Internet-piracy-policing-could-add-420183>
- Marcos, Jesús Miguel . "La 'ley Sinde' se salva "sin cambios sustanciales." *Público*, January 25, 2011. <http://www.publico.es/culturas/357997/la-ley-sinde-se-salva-sin-cambios-sustanciales>
- Mark Sweney. "Illegal downloads: music industry to carry cost of catching pirates." *the Guardian*, Sept 14, 2010. <http://www.theguardian.com/technology/2010/sep/14/illegal-downloads-music-industry>
- Mark, Roy. "High Court Bounces Latest RIAA Effort." *InternetNews.com*, October 12, 2004.
- Markmonitor. *Traffic Report: Online Piracy and Counterfeiting*, 2011. See:
[https://www.markmonitor.com/download/report/MarkMonitor - Traffic Report 110111.pdf](https://www.markmonitor.com/download/report/MarkMonitor_-_Traffic_Report_110111.pdf)
- Marzouki, Meryem. "E-Commerce directive: ensure freedom of expression and due process of law." *EDRI Website*, November 18, 2010. <http://history.edri.org/book/export/html/2445>
- Masnack, Mike and Michael Ho. *The Sky is Rising, a detailed look at the state of the entertainment industry*. Jan 2012. <https://www.techdirt.com/skyisrising/>
- Masnack, Mike. "Another Day, Another Study That Says 'Pirates' Are The Best Customers.. This Time From HADOPI." *Techdirt*, July 28, 2011.
<https://www.techdirt.com/articles/20110727/16233815292/another-day-another-study-that-says-pirates-are-best-customers-this-time-hadopi.shtml>
- Masnack, Mike. "Congressional Research Service Shows Hollywood is Thriving." *Techdirt*, Dec 12, 2011. <https://www.techdirt.com/articles/20111212/02244817037/congressional-research-service-shows-hollywood-is-thriving.shtml>, the link contains full report.

- Masnack, Mike. "More Charts The Record Labels Don't Want You To See: Swedish Musicians Making More Money." *Techdirt*, December 14, 2009.
<https://www.techdirt.com/articles/20091213/1648377324.shtml>
- Masnack, Mike. "A Glimpse Of The Future Under SOPA: Warner Bros. Admits It Filed Many False Takedown Notices." *Techdirt*, November 10, 2011.
<http://www.techdirt.com/articles/20111110/10135116708/glimpse-future-under-sopa-warner-bros-admits-it-filed-many-false-takedown-notice.shtml>
- Masnack, Mike. "A History of Hyperbolic Overreaction to Copyright Issues: The Entertainment Industry and Technology." *Techdirt*, November 9, 2011.
<http://www.techdirt.com/blog/innovation/articles/20111108/17562016686/history-hyperbolic-overreaction-to-copyright-issues-entertainment-industry-technology.shtml>
- Masnack, Mike. "Another Judge Blasts Copyright Trolls." *Techdirt*, September 24, 2012.
<http://www.techdirt.com/articles/20120923/22100820477/another-judge-blasts-copyright-trolls.shtml>
- Masnack, Mike. "BPI Insists UK ISPs Overstating The Cost Of Three Strikes; So Will BPI Pay The Difference If Wrong?" *Techdirt*, January 21, 2010.
<http://www.techdirt.com/articles/20100120/1937547848.shtml>
- Masnack, Mike. "File Sharing Pre-Settlement Letters In Europe Get Lawyer Banned For Six Months." *Techdirt*, April 7, 2008).
<http://www.techdirt.com/articles/20080407/002030770.shtml>
- Masnack, Mike. "GoDaddy Takes Down Entire Site Of Copyright Attorney/Photographer Over Bogus DMCA Claim." *Techdirt*, November 21, 2011.
<http://www.techdirt.com/articles/20111119/01060316841/godaddy-takes-down-entire-site-copyright-attorney-photographer-over-bogus-dmca-claim.shtml>
- Masnack, Mike. "Homeland Security Won't Even Admit Whether Or Not It Seized Moo.com, Taking Down 84,000 Innocent Sites." *Techdirt*, February 17, 2011.
<https://www.techdirt.com/articles/20110217/00082213144/homeland-security-wont-even-admit-whether-not-it-seized-moo-com-taking-down-84000-innocent-sites.shtml>
- Masnack, Mike. "Hurt Locker file sharing lawsuit lists hockey stadium IP address." *Techdirt*, September 28, 2011. <http://www.techdirt.com/articles/20110928/02302616122/hurt-locker-file-sharing-lawsuit-lists-hockey-stadium-ip-address.shtml>
- Masnack, Mike. "ICE Finally Admits It Totally Screwed Up; Next Time, Perhaps It'll Try Due Process." *Techdirt*, February 21, 2011.
<https://www.techdirt.com/articles/20110220/17533013176/ice-finally-admits-it-totally-screwed-up-next-time-perhaps-itll-try-due-process.shtml>
- Masnack, Mike. "Massive Growth In Independent Musicians & Singers Over The Past Decade." *TechDirt*, May 30, 2013.
<https://www.techdirt.com/blog/casestudies/articles/20130529/15560423243/massive-growth-independent-musicians-singers-over-past-decade.shtml>
- Masnack, Mike. "Ridiculous: Lamar Smith Basing His Plan To Massively Regulate The Internet On False Or Misleading Research." *Techdirt*, December 15, 2011.
<https://www.techdirt.com/articles/20111214/23451317095/ridiculous-lamar-smith-basing-his-plan-to-massively-regulate-Internet-false-misleading-research.shtml>
- Masnack, Mike. "Study Shows That Web Blocking Ignores Real Problems, Doesn't Solve Anything & Is Used As A Political Tool." *Techdirt*, September 30, 2010.
<http://www.techdirt.com/articles/20100930/10105711238/study-shows-that-web-blocking-ignores-real-problems-doesn-t-solve-anything-is-used-as-a-political-tool.shtml>

- Masnack, Mike. "UK Government Report Shows That Digital Economy Bill Will Cost More Than Highest 'Piracy' Estimates, Drive 40,000 Offline." *Techdirt*, December 28, 2009. <http://www.techdirt.com/articles/20091228/0335197514.shtml>
- Masnack, Mike. "UK Law Enforcement Tells UK Gov't: Please Don't Kick File Sharers Offline." *Techdirt*, October 27, 2009. <http://www.techdirt.com/articles/20091027/0254326689.shtml>
- Masnack, Mike. "UK Trying To Censor Parody Video About The 2012 Olympics." *Techdirt*, February 29, 2012. <http://www.techdirt.com/articles/20120229/04115017911/uk-trying-to-censor-parody-video-about-2012-olympics.shtml>
- Masnack, Mike. "Why It is Almost Impossible To Get Punished For A Bogus DMCA Takedown." *Techdirt*, October 17, 2012. <https://www.techdirt.com/articles/20121017/10355320733/why-its-almost-impossible-to-get-punished-bogus-dmca-takedown.shtml>
- Mathur, Vijay. "Economics of crime: an investigation of the deterrent hypothesis for urban areas." *the review of economics and statistics* 60.3 (1978): 459-466.
- McAllister, Neil. "Lawyers: We'll pillory porn pirates who don't pay up." *The Register*, August 23, 2012. http://www.theregister.co.uk/2012/08/23/german_pirate_pillory/
- McBride, Sarah and Ethan Smith. "Music Industry to Abandon Mass Suits." *The Wall Street Journal*, December 19, 2008. <http://online.wsj.com/article/SB122966038836021137.html>
- McCandless, David. "Warez Wars." *Wired*, April 1997. http://www.wired.com/wired/archive/5.04/ff_warez.html
- McCullagh, Declan. "Copyright bill controversy grows as rhetoric sharpens." *CNET*, October 31, 2011. <http://www.cnet.com/news/copyright-bill-controversy-grows-as-rhetoric-sharpens/>
- McCullagh, Declan. "Copyright Office will endorse SOPA anti-piracy bill." *CNET*, November 15, 2011. <http://www.cnet.com/news/copyright-office-will-endorse-sopa-anti-piracy-bill/>
- McCullagh, Declan. "SOPA bill won't make U.S. a 'repressive regime,' Democrat says." *CNET*, November 16, 2011. <http://www.cnet.com/news/sopa-bill-wont-make-u-s-a-repressive-regime-democrat-says/>
- McCullagh, Declan. "SOPA's most aggressive defender: U.S. Chamber of Commerce." *CNET*, November 30, 2011. <http://www.cnet.com/news/sopas-most-aggressive-defender-u-s-chamber-of-commerce/>
- McDougal, Dennis. "Double-Cross at the WGA." *LA Weekly*, May 2, 2007. <http://www.laweekly.com/2007-05-03/news/double-cross-at-the-wga/>
- McGonagle, Tarlach, Christina Angelopoulos, Annabel Brody, Wouter Hins, Bernt Hugenholtz, Patrick Leerssen, Thomas Margoni, Ot van Daalen and Joris van Hoboken. "Study of Fundamental Rights Limitations for Online Enforcement through Self-Regulation." *Institute for Information Law (IvIR)*. University of Amsterdam, forthcoming.
- McGuire, Dave. "Kids Pirate Music Freely." *Washingtonpost.com*, May 18, 2004. <http://www.washingtonpost.com/wp-dyn/articles/A37231-2004May18.html>
- Meadows, Chris. "Publishers Find Amazon Self-publishing 'Threatening', Self-published Writer Suggests." *TeleRead*, September 11, 2011. <http://www.teleread.com/ebooks/publishers-find-amazon-self-publishing-threatening-self-published-writer-suggests/>
- Mearian, Lucas. "Music industry sucks life from subscription services." *Computerworld*, February 14, 2014.

- http://www.computerworld.com/s/article/9246365/Music_industry_sucks_life_from_subscription_services?taxonomyId=71&pageNumber=1
- Mearian, Lucas. "Online movie streaming can be profitable as TV, disc sales." *Computerworld*, January 23, 2014.
http://www.computerworld.com/s/article/9245666/Online_movie_streaming_can_be_profitable_as_TV_disc_sales
- Mearian, Lucas. "60TB disk drives could be reality in 2016." *Computerworld*, May 22, 2012.
http://www.computerworld.com/s/article/9227382/60TB_disk_drives_could_be_a_reality_in_2016
- Mediatique. "Online piracy – downloading the facts." *Mediatique*, May 6, 2009.
<http://www.mediatique.co.uk/sitedata/Reports/piracy.pdf>
- Mehr, Bob. "Gnat, Meet Cannon." *Chicago Reader*, February 4, 2005.
- Meliá, Jorge Cancio. "The administrative and judicial Procedure concerning Internet Infringements: much more than a simple notice and takedown procedure." *WIPO Advisory Committee on Enforcement*, WIPO/ACE/9/21. December 20, 2014.
- Mennecke, Thomas. "Canada Plans P2P and file-sharing Crackdown." *Slyck*, March 24, 2005.
<http://www.slyck.com/news.php?story=720>
- Mennecke, Thomas. "P2P Population Remains Steady." *Slyck*, October 20, 2006.
http://www.slyck.com/story1314_P2P_Population_Remains_Steady
- Mennecke, Thomas. "RIAA Announces new campus lawsuit strategy." *Slyck*, February 28, 2007.
- Mennecke, Thomas. "RIAA Not Impressed with Legal Concerns Surrounding MediaSentry." *Slyck*, February 6, 2008.
http://www.slyck.com/story1657_RIAA_Not_Impressed_with_Legal_Concerns_Surrounding_MediaSentry
- Merlo, Antonio. "Introduction to economic models of crime." *International Economic Review* 45.3 (2004): 677-679.
- Merrill, Stephen A. and William J. Raduchel, eds. *Copyright in the Digital Era: Building Evidence for Policy*. National Academies Press. 2013.
- Metro. "Game file-sharers told to pay £2,750." *Metro* (1 July 2008).
<http://metro.co.uk/2008/07/01/game-file-sharers-told-to-pay-2-750-230423/>
- Meyer, David. "Copyright Isn't Working, Says European Commission." *ZDNet*, November 19, 2011. <http://www.zdnet.co.uk/blogs/communication-breakdown-10000030/copyright-isnt-working-says-european-commission-10024835/>
- Meyer, Trisha. "Graduated response in France: The Clash of Copyright and the Internet." *Journal of Information Policy* 2 (2012): 107-127.
- Miceli, Thomas. "Optimal criminal procedure: fairness and deterrence." *International review of law and economics* 11.1 (1991).
- Mick, Jason. "MPAA Chief Threatens Obama, Congress for SOPA Rejection." *DailyTech*, January 22, 2012.
<http://www.dailytech.com/MPAA+Chief+Threatens+Obama+Congress+for+SOPA+Rejection/article23842.htm#sthash.yVWsy0Hu.dpu>
- Milton, John. *Aeropagitica* (1644). The full text is available online, for example at the website of Dartmouth College:
https://www.dartmouth.edu/~milton/reading_room/areopagitica/text.shtml
- Miners, Zach. "Google scores a win in SOPA-tinged Mississippi case." *PC World*. 2 March 2015.
<http://www.pcworld.com/article/2891852/google-scores-a-win-in-sopatinged-mississippi-case.html>

- Mitchell, Anne P. "Is the "Internet Copyright Law Enforcement Agency" Real or a Scam? Here's What We Know." *The Internet Patrol*, February 21, 2013.
<http://www.theInternetpatrol.com/is-the-Internet-copyright-law-enforcement-agency-real-or-a-scam-heres-what-we-know/>
- Montezuma Panez, Oscar. "Spanish Court Rules That Linking to Potential Copyright Infringing Material Is Not Copyright Infringement ." *Electronic Frontier Foundation*, August 5, 2011.
<https://www.eff.org/deeplinks/2011/08/spanish-court-rules-linking-potential-copyright>
- Moody, Glyn. "Once Again Top Downloaders Are Top Spenders, According to UK Gov't Study." *Techdirt*, May 14, 2013.
<https://www.techdirt.com/articles/20130513/11270823061/once-again-top-downloaders-are-top-spenders-according-to-uk-govt-study.shtml>
- Moody, Glyn. "First HADOPI Victim Convicted, Not For His Own Infringement, But Because His Wife Downloaded Songs." *Techdirt*, September 13, 2012.
<http://www.techdirt.com/articles/20120913/06550920370/first-HADOPI-victim-convicted-not-his-own-infringement-because-his-wife-downloaded-songs.shtml>
- Moody, Glyn. "French Hadopi Scheme Guttled; Other Bad Ideas To Be Introduced Instead." *Techdirt*, December 10, 2012.
<http://www.techdirt.com/articles/20121209/07085621316/french-HADOPI-scheme-guttled-other-bad-ideas-to-be-introduced-instead.shtml>
- Moody, Glyn. "Hacktivist Judo: Musician Exploits New Spanish Law To Overwhelm System With Legitimate Infringement Complaints ." *Techdirt* , March 2, 2012.
<http://www.techdirt.com/articles/20120302/09570417949/hacktivist-judo-musician-exploits-new-spanish-law-to-overwhelm-system-with-legitimate-infringement-complaints.shtml>
- Moody, Glyn. "Leading French Presidential Candidate Would Repeal HADOPI But Keep Net Surveillance." *Techdirt*, October 26, 2011.
<http://www.techdirt.com/articles/20111023/05483716480/leading-french-presidential-candidate-would-repeal-HADOPI-keep-net-surveillance.shtml>
- Moor, James H. "Towards a theory of privacy in the information age." *Computers and society* (1997): 27-32.
- Morrissey, Colin. "Behind the Music: Determining the Relevant Constitutional Standard for Statutory Damages in Copyright Infringement Suits." *Fordham L. Rev.* 78: 3059 (2010).
<http://ir.lawnet.fordham.edu/flr/vol78/iss6/11>
- Morton, John. "Statement of John Morton, Director of U.S. Immigration and Customs Enforcement, Department of Homeland Security." *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part II: Hearing Before the H. Comm. on the Judiciary, Subcomm. on Intellectual Property, Competition, and the Internet*, 112th Cong. 11-12 (2011). <http://commcns.org/t38zzN>
- Moss, Pamela. "shifting conceptions of validity in educational measurement: implications for performance assessment." *Review of educational research* 62 (fall): 229-58.
- Motion Picture Association of America. "Theatrical Market Statistics 2013." *Motion Picture Association of America*. http://www.mpa.org/wp-content/uploads/2014/03/MPAA-Theatrical-Market-Statistics-2013_032514-v2.pdf
- Motion Picture Association. Public Consultation on Creative Content Online in the Single Market – Submission of the "Motion Picture Association" (MPA) in response to the Questionnaire of the European Commission regarding Policy/Regulatory issues, February 29, 2008,

- available at
http://ec.europa.eu/avpolicy/docs/other_actions/col_2008/comp/mpa_en.pdf
- Moya, Jared. "NSA "Yelled" at France Over "Three-Strikes" Legislation." *ZeroPaid*, October 6, 2010. <http://www.zeropaid.com/news/90967/nsa-yelled-at-france-over-three-strikes-legislation/>
- Mueller, Milton U. "Activists Fear Sarkozy's Efforts to Tame Web." *Spiegel Online International*, May 24, 2011. <http://www.spiegel.de/international/Europe/0,1518,764305,00.html>
- Mueller, Milton, Andreas Kuehn, and Stephanie Michelle Santoso. "Policing the network: Using DPI for copyright enforcement." *Surveillance & Society* 9.4 (2012): 348.
- Muñoz, R. and R.J. Cano. "Fracasa la 'ley Sinde' en el Congreso tras el último intento del PSOE de conseguir apoyo ." *El Pais*, December 21, 2010. http://cultura.elpais.com/cultura/2010/12/21/actualidad/1292886001_850215.html
- Murray, Andrew. "Internet Regulation." in: *Handbook on the Politics of Regulation*, ed. David Levi-faur. Edward Elgar Publishing, 2011.
- Murray, Andrew. *Information Technology law: the Law and Society*. Oxford University Press, 2010.
- Murray, Andrew. *Information Technology law: the Law and Society*. Oxford University Press, 2013.
- Music Ally. "Eircom launches MusicHub service and reveals graduated response policy." *Musically*, Dec 9, 2010. <http://musically.com/2010/12/09/eircom-launches-musichub-service-and-reveals-graduated-response-policy/>
- Music Ally. "Spotify helps Swedish music sales rise 30.1% in first half of 2012." *Musically*, July 13, 2012. <http://musically.com/2012/07/13/spotify-sweden-ifpi-figures/>
- Nagin, Daniel. "Criminal deterrence research at the outset of the twenty-first century." *Crime and justice* (1998): 1-42.
- National Intellectual Property Rights Coordination Center. "Press Release – Operation in Our Sites." *National Intellectual Property Rights Coordination Center*. www.iprcenter.gov/reports/fact-sheets/operation-inour-sites/view
- National Research Council (US). Committee on Intellectual Property Rights. *The Digital Dilemma: Intellectual Property in the Information Age*. National Academy Press, 2000.
- Negativland & The RIAA. "RIAA releases yearend anti-piracy statistics." *Negativland & The RIAA*. http://www.negativland.com/archives/014riaa/piracy_stats.html (the original link was on the RIAA website, but it has dissapeared: http://www.riaa.com/newsitem.php?news_year_filter=&resultpage=140&id=876C1BEF-6ACE-E99D-2755-71A875EF2A66)
- Netanel, Neil Weinstock. "Impose a noncommercial use levy to allow free peer-to-peer file sharing." *Harvard Journal of Law & Technology* 17 (2003): 2-84.
- New Zealand Federation Against Copyright Theft. "Copyright (Infringing File Sharing) Regulations – Fee Review." *Ministry for Economic Development*. 2012. www.med.govt.nz/business/intellectual-property/pdf-docs-library/copyright/notice-process/illegal-peer-to-peer-file-sharing-submissions-on-fee-review-discussion/nzfact.pdf
- News.com.au. "Cyber-prankster iLCreation gets all of Justin Bieber's clips yanked from YouTube." *News.com.au*, August 30, 2011. <http://www.news.com.au/entertainment/music/cyber-prankster-gets-all-of-justin-biebers-clips-yanked-from-youtube/story-e6frfn09-1226125502750>
- Notice-and-Take-Down Code of Conduct. version 1.04. 9 October 2008.

- Nu.nl. "Muziek via Internet veslaat cd in 2015." *Nu.nl*, August 27, 2013.
<http://www.nu.nl/tech/3560636/muziek-via-Internet-verslaat-cd-in-2015.html>
- O'Brien, Damien and Professor Brian Fitzgerald. "Digital copyright law in a Youtube world."
Internet Law Bulletin 9.6 & 7 (2006): 71-74.
- O'Brien, Danny. "France declares three strikes unconstitutional." *Electronic Frontier Foundation*,
 June 10, 2009. <https://www.eff.org/deeplinks/2009/06/three-strikes-dead-in-france>
- Oberholzer-Gee, Felix and Koleman Strumpf. "The Effect of File Sharing on Record Sales: An
 Empirical Analysis." *Journal of Political Economy* 115 (February 2007): 1-42.
- OECD. "OECD project on counterfeiting and piracy." *OECD Website*.
<http://www.oecd.org/sti/ind/oecdprojectoncounterfeitingandpiracy.htm>
- OECD. "OECD Broadband Statistics." *OECD Website*, January 2005. see:
<http://www.oecd.org/sti/broadband/oecdbroadbandstatisticsjune2005.htm>
- OECD. Digital Broadband Content: Music (2005). DSTI/ICCP/IE(2004)12/FINAL
- Office of the United Nations High Commissioner for Human Rights. *Rule-of-law tools for post-
 conflict states, Monitoring legal systems*. United Nations Office on Drugs and Crime,
 Criminal Justice Assessment Toolkit, Vienna, 2006.
- Official office of the U.S. Trade Representative response. We the People.
<https://petitions.whitehouse.gov/response/role-anti-counterfeiting-trade-agreement-acta>
- Oremus, Will. "Did YouTube Really Block Michelle Obama's DNC Speech for Copyright
 Infringement?" *Slate*, September 5, 2012.
http://www.slate.com/blogs/future_tense/2012/09/05/michelle_obama_dnc_speech_why_did_youtube_flag_it_for_copyright_infringement_.html
- Oswald, Ed. "RIAA Sues LimeWire Over Piracy." *BetaNews*, August 4, 2006.
<http://betanews.com/2006/08/04/riaa-sues-limewire-over-piracy/>
- Page Will and Chris Carey. "Adding Up the Music Industry for 2008." *PRS for Music*, 2009.
[http://www.prsformusic.com/creators/news/research/Documents/Will%20Page%20and%20Chris%20Carey%20\(2009\)%20Adding%20Up%20The%20Music%20Industry%20for%202008.pdf](http://www.prsformusic.com/creators/news/research/Documents/Will%20Page%20and%20Chris%20Carey%20(2009)%20Adding%20Up%20The%20Music%20Industry%20for%202008.pdf)
- Palmedo, Mike. "BSA Report on Global Software Piracy." *Infojustice.org*, May 17, 2012.
<http://infojustice.org/archives/23902>
- Palmer, Doug. "Some secrecy needed in trade talks: Ron Kirk." *Reuters*, May 13, 2012.
<http://www.reuters.com/article/2012/05/14/us-usa-trade-kirk-idUSBRE84C0AQ20120514>
- Panther, Stephan. "The economics of crime and criminal law: An antithesis to sociological
 theories?" *European Journal of Law and Economics* 2.4 (1995): 365-378.
- Pasternack, Alex. "NASA's Mars Rover Crashed Into a DMCA Takedown." *Motherboard*, August
 6, 2012. <http://motherboard.vice.com/blog/nasa-s-mars-rover-crashed-into-a-dmca-takedown>.
- Patry, William. *Moral panics and the copyright wars*. Oxford University Press, 2009.
- Pearson, Dan. "Guillemot: as Many PC players pay for F2P as boxed product."
Gamesindustry.biz, August 22, 2012. <http://www.gamesindustry.biz/articles/2012-08-22-guillemot-as-many-pc-players-pay-for-f2p-as-boxed-product>
- Peck, Morgen. "Spain's SOPA Law: How It Works And Why It Won't." *IEEE Spectrum*, January 9,
 2012. <http://spectrum.ieee.org/tech-talk/telecom/Internet/spains-sopa-law-how-it-works-and-why-it-wont-work>

- Pegoraro, Rob. "DRM Ends, Variable Pricing Begins for iTunes Music." *Washingtonpost.com*, April 7, 2009. http://voices.washingtonpost.com/fasterforward/2009/04/the_drm_era_ends_for_itunes_mu.html.
- Perset, Karine. "The economic and social role of Internet intermediaries." *OECD*, 2010.
- Peukert, Alexander. "Why Do 'Good People' Disregard Copyright on the Internet?" in: *Criminal Enforcement: A Blessing or a Curse for Intellectual Property?* Ed: Cristophe Geiger. Edward Elgar Publishing, 2012.
- Pfanne, Eric. "Music Industry Sales Rise, and Digital Revenue Gets the Credit" *The New York Times*, February 26, 2013. <http://www.nytimes.com/2013/02/27/technology/music-industry-records-first-revenue-increase-since-1999.html? r=0>
- Pfanner, Eric. "Copyright Cheats Face the Music in France." *The New York Times*, February 19, 2012. <http://www.nytimes.com/2012/02/20/technology/20iht-piracy20.html?pagewanted=all>
- Pfanner, Eric. "French Appear Ready to Soften Law on Media Piracy." *The New York Times*, June 2, 2013. <http://www.nytimes.com/2013/06/03/technology/03iht-piracy03.html? r=0>
- Piatek, Michael, Tadayoshi Kohno, Arvind Krishnamurthy. "Challengers and Directions for Monitoring P2P File Sharing Networks – or – Why my printer received a takedown notice." *HotSec*, 2008.
- Plumer, Brad. "SOPA: How Much Does Online Piracy Really Cost the Economy?" *Washington Post*, January 5, 2012. http://www.washingtonpost.com/blogs/wonkblog/post/how-much-does-online-piracy-really-cost-the-economy/2012/01/05/gIQAXknNdP_blog.html
- Poort, Joost and João Pedro Quintais. "The Levy Runs Dry: A Legal and Economic Analysis of EU Private Copying Levies." *4 Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 205 (2013).
- Poort, Joost and Jorna Leenheer. "File sharing 2@12: Downloading from illegal sources in the Netherlands." Institute for Information Law & CentERdata, Amsterdam/Tilburg (2012). Retrieved from http://www.ivir.nl/publications/poort/Filesharing_2012
- Porter, Eduardo. "The Perpetual War: Pirates and Creators." *The New York Times*, February 4, 2012. <http://www.nytimes.com/2012/02/05/opinion/sunday/perpetual-war-digital-pirates-and-creators.html? r=3&>
- Postel, Jon. "DOD Standard for the Internet Protocol." *Prepared for DARPA*, January 1980. <http://tools.ietf.org/html/rfc760>
- Postel, Jon. "Internet Protocol, DARPA Internet Program, Protocol Specification." *Prepared for DARPA*, September 1981. <http://tools.ietf.org/html/rfc791>
- Posting of Moby to Moby.com (June 20, 2009). <http://www.moby.com/journal/2009-0620/riaa-have-sued-jammie-thomas-rasset-minn.html>
- Poulsen, Kevin. "DirecTV dragnet snares innocent techies." *SecurityFocus*, July 7, 2003. <http://www.securityfocus.com/news/6402>
- Poulter, Sean. "Guilty until proven innocent: Families will have to pay £20 to show they DIDN'T illegally download music under new law." *Daily Mail Online*, June 26, 2012. <http://www.dailymail.co.uk/news/article-2165004/Illegal-downloading-Families-illegally-download-music-movies-online-face-court-action-copyright-theft.html>
- Prabhaka, Binoy. "Bollywood no longer talks of piracy; but ignoring dangers of online can be costly." *The Economic Times*, February 3, 2013. http://articles.economictimes.indiatimes.com/2013-02-03/news/36704530_1_piracy-box-office-alliance-against-copyright-theft

- Prenafeta, Javier. "Procedimiento de salvaguarda de derechos de propiedad intelectual de acuerdo con la Ley Sinde." *Javier Prenafeta*, January 2, 2012. <http://www.iprenafeta.com/2012/01/02/procedimiento-salvaguarda-propiedad-intelectual-ley-sinde/#>
- Price, David. "An estimate of infringing use of the Internet." *Envisional* 2011. See: <http://documents.envisional.com/docs/Envisional-Internet-Usage-Jan2011.pdf>. P.3-4
- Price, David. "Sizing the piracy universe", *Netnames*, September 2013. available at: <https://copyrightalliance.org/sites/default/files/2013-netnames-piracy.pdf>
- Princeton Survey Research Associates Int. "Spring Tracking Survey." *Pew Internet & American Life Project*, 2008. Available at: http://www.pewInternet.org/files/old-media/Files/Questionnaire/Old/PIP_Broadband.2008.Topline.pdf
- Protalinski, Emil. "Researchers find Megaupload shutdown hurt box office revenues, despite gains for blockbusters." *The Next Web News*, November 24, 2012. <http://thenextweb.com/insider/2012/11/24/researchers-find-megaupload-shutdown-had-a-negative-effect-on-box-office-revenues/#!ziy1X>
- Public Citizen. "Record Industry Cuts Corners in Crusade Against File-Sharers." *Public Citizen*, February 2, 2004. <http://www.citizen.org/pressroom/pressroomredirect.cfm?ID=1636>
- Pulver, Andrew. "British Cinema's Golden Age is Now." *The Guardian*, Oct. 13, 2011. <http://www.guardian.co.uk/film/2011/oct/13/british-cinema-golden-age>
- Quintais, João Pedro. "A Shifting Copyright Zeitgeist: Alternative Compensation Models for Digital Content Sharing." *Working Paper presented at the Transatlantic Workshop on Intellectual Property Research – ETH Zurich* (January 14, 2014) (on file with the author).
- Rainie, Lee, Mary Madden, Dan Hess, Graham Mudd. "Pew Internet Project and Comscore Media Metrix Data memo, The state of Music Downloading and File-Sharing Online." *Pew Research Center*, 2004. http://www.pewInternet.org/~media//Files/Reports/2004/PIP_FilesSharing_April_04.pdf
- Ramadge, Andrew. "Top Three Reasons We Choose Illegal Downloads." *news.com.au*, May 7, 2010. <http://www.news.com.au/technology/why-do-australians-choose-illegal-downloads/story-e6frfo0-1225863649562>
- Rawls, John. *A Theory of Justice*. Oxford University Press, Twelfth Impression, 1992.
- Realwire. "Report Sheds Light on Scale and Complexity of Online Piracy and Counterfeiting Problem." *Realwire*, January 12, 2011. <http://www.realwire.com/releases/Report-Sheds-Light-on-Scale-and-Complexity-of-Online-Piracy-and-Counterfeiting-Problem>
- Rees, Marc. "Hadopi : 600 € d'amende et quinze jours de suspension pour un abonné." *Next Inpact*, June 12, 2013. <http://www.pcinpact.com/news/80487-HADOPI-600-d-amende-et-quinze-jours-suspension-pour-abonne.htm>
- Reflets. "Le honeypot de TMG." *Reflets.info*, May 13, 2011. <http://reflets.info/le-honeypot-de-tmg/>
- Reijerman, Dimitri. "Brein krijgt naw-gegevens via betalingsprovider –update." *Tweakers*, September 26, 2011. <http://tweakers.net/nieuws/77014/brein-krijgt-naw-gegevens-via-betalingsprovider.html>
- Reitman, Rainey. "Repealing French Three Strikes Law is the Next Step to Safeguarding Free Expression." *Electronic Frontier Foundation*, August 8, 2012. <https://www.eff.org/deeplinks/2012/08/repeal-french-three-strikes-law>
- République Française. *Annex au projet de loi de finances pour 2013, Rapport sur les Autorités publiques indépendantes*.

- Reuters. "Spain readies hefty jail terms over Internet piracy." *Reuters*, September 20, 2013. <http://www.reuters.com/article/2013/09/20/net-us-spain-piracy-idUSBRE98JORD20130920>
- Revoir, Paul. "Up to 25,000 British illegal downloaders sued for £300 as games developers turn to courts." *Daily Mail* (21 August 2008). <http://www.dailymail.co.uk/news/article-1046607/Up-25-000-British-illegal-downloaders-sued-300-games-developers-turn-courts.html>
- RIAA. "For students writing papers." *RIAA website*, <http://www.riaa.com/faq.php>, last visited on 20-9-2011
- RIAA. "Recording Industry Begins Suing P2P File Sharers Who Illegally Offer Copyrighted Music Online." *RIAA website*, September 8, 2003. <http://www.riaa.com/news/newsletter/090803.asp>
- RIAA. "RIAA Brings lawsuits against 762 file sharers." *RIAA press release*, September 30, 2004.
- Roberts, Paul. "RIAA Sues 532 John Does." *IDG News*, January 21, 2004..
- Rodriguez, Jose Elias. "Spain's anti-piracy law may already be obsolete." *Reuters*, March 26, 2012. <http://www.reuters.com/article/2012/03/26/net-us-spain-piracy-idUSBRE82POJV20120326>
- Rodríguez, Sergio. "'Ley Sinde' for dummies." *El Mundo*, January 24, 2011. <http://www.elmundo.es/blogs/elmundo/cataleio/2011/01/24/ley-sinde-for-dummies.html>
- Roettgers, Janko. "Three strikes: Five minutes per court decision." *P2P Blog*, January 7, 2009. <http://www.p2p-blog.com/item-1101.html>
- Rolf, Pamela. "Spanish Government Tables Law to Fight Illegal Downloads." *The Hollywood Reporter*, 12 March, 2011. <http://www.hollywoodreporter.com/news/sinde-law-illegal-downloads-269328>
- Rolling Stone Magazine. "RIAs gaze turns from users to ISPs in piracy fight." *Rolling Stone Magazine*, December 19, 2012. <http://www.rollingstone.com/rockdaily/index.php/2008/12/19/riaas-gaze-turns-from-users-to-isps-in-piracy-fight/>
- Romero, Pablo. "Ésta es la 'Comisión Sinde'." *El Mundo.es*, February 11, 2013. <http://www.elmundo.es/elmundo/2013/02/11/navegante/1360581254.html>
- Rosen, Rebecca J. "The Hole in Our Collective Memory: How Copyright Made Mid-Century Books Vanish." *the Atlantic*, July 30, 2013. <http://www.theatlantic.com/technology/archive/2013/07/the-hole-in-our-collective-memory-how-copyright-made-mid-century-books-vanish/278209/>
- Roughol, Isabelle. "Why Courts Can Barely Dent Online Piracy." *LinkedIn*, November 29, 2013. <https://www.linkedin.com/today/post/article/20131129161636-13333827-why-courts-can-barely-dent-online-piracy>
- Rowan, David. "Inside the web of thieves." *the Guardian*, April 21, 2002. <http://www.theguardian.com/technology/2002/apr/21/observersciencepages.theobserver>
- Rubin, Herbert and Irene Rubin. *Qualitative interviewing: The art of hearing data*. Thousand Oaks, California, Sage, 2005.
- Rutherford, Malcolm. "Institutional economics: then and now." *Journal of Economic Perspectives* (2001): 173-194.
- Ryan, Johnny and Caitriona Heintz. "Internet Access Controls: Three Strikes' Graduated Response' Initiatives." *The Institute of International and European Affairs* (2010).

- Saarinen, Juha. "Kiwis put a price on copyright notices: \$23." *ITnews*, September 29, 2010. <http://www.itnews.com.au/News/233676,kiwis-put-a-price-on-copyright-notices-23.aspx>
- Sabbagh, Dan. "Average Teenager's iPod Has 800 Illegal Music Tracks." *The Times*, June 16, 2008.
- Salmon, Felix. "Counterfeiting: Much Less Prevalent Than You Think." *Upstart Business Journal*, Oct 26, 2007. <http://upstart.bizjournals.com/views/blogs/market-movers/2007/10/26/counterfeiting-much-less-prevalent-than-you-think.html?page=all>
- Samuelson, Pamela and Ben Sheffher. Debate, "Unconstitutionally Excessive Statutory Damage Awards in Copyright Cases." *University of Pennsylvania Law Review*: 158. 53 (2009). <http://www.pennumbra.com/debates/pdfs/CopyrightDamages.pdf>
- Samzenpus. "Terrorists Used False DMCA Claims To Get Personal Data of Anti-Islamic Youtuber." *Slashdot*, November 6, 2014. <http://yro-beta.slashdot.org/story/14/11/06/0435252/terrorists-used-false-dmca-claims-to-get-personal-data-of-anti-islamic-youtuber>
- Sanchez, Julian. "Internet Regulation & the Economics of Piracy." *CATO Institute*, January 17, 2012. <http://www.cato.org/blog/Internet-regulation-economics-piracy>
- Sandoval, Greg. "Porn studios' copyright lawyer: 'I will sue' (Q&A)." *CNET*, October 5, 2010.
- Sandoval, Greg. "HBO Forces Netflix to Go Elsewhere for Its DVDs." *CNET*, January 5, 2012. http://news.cnet.com/8301-31001_3-57353134-261/hbo-forces-netflix-to-go-elsewhere-for-its-dvds/
- Sandoval, Greg. "Hollywood's SOPA testimony links job loss to piracy." *CNET*, November 16, 2011. <http://www.cnet.com/news/hollywoods-sopa-testimony-links-job-loss-to-piracy/>
- Sandoval, Greg. "Porn Studios to Subpoena Accused File Sharers." *CNET*, October 2, 2010. http://news.cnet.com/8301-31001_3-20018358-261.html
- Sandoval, Greg. "RIAA demands ReDigi stop selling used downloads." *CNET*, November 14, 2011. http://news.cnet.com/8301-31001_3-57324477-261/riaa-demands-redigi-stop-selling-used-downloads/
- Sandoval, Greg. "Exclusive: Top ISPs poised to adopt graduated response to piracy." *CNET*, June 22, 2011. <https://www.cnet.com/news/exclusive-top-isps-poised-to-adopt-graduated-response-to-piracy/>
- Sartori, Giovanni. "Concept misinformation in comparative politics." *the American Political Science Review* 64 (1970): 1033-53.
- Schauer, Frederick. *Free speech: a philosophical enquiry*. Cambridge University press, 1982.
- Schellevis, Joost. "Usenetproviders zien flinke toename takedown-requests." *Tweakers*, November 9, 2012. <http://tweakers.net/nieuws/85442/usenetproviders-zien-flinke-toename-takedown-requests.html>
- Schermer, Bart and Martine Wubben. *Feiten om te delen: digitale contentdistributie in Nederland*. Considerati, 2011.
- Schilpzand, Wouter. "Large scale European police action against piracy networks." *Future of Copyright*, September 14, 2010. <http://www.futureofcopyright.com/home/blog-post/2010/09/14/large-scale-european-police-action-against-piracy-networks.html>
- Schruers, Matt. "The Search Fixation: Infringement, Search Results, and Online Content." *Computer & communications Industry Association research paper*, August 2013. http://cdn.cciinet.org/wp-content/uploads/2013/08/CCIA_TheSearchFixation.pdf
- Schulze, Hendrik and Klaus Mochalski. "Internet study 2007." *Ipoque GmbH White Paper* (2007).
- Schulze, Hendrik and Klaus Mochalski. "Internet Study 2008/2009." *Ipoque Report* 37 (2009).

- Schwartz, John. "Recording Industry is accusing 532 people of Music piracy." *The New York Times*, January 21, 2004.
- Searle, John R. *The Construction of Social Reality*. 1997.
- Sell, Susan. "The global IP upward ratchet, anti-counterfeiting and piracy enforcement efforts: the state of play." *Institute for Global and International Studies*. George Washington University, 2010.
- Senator Ron Wyden. "Letter by U.S. Senator Ron Wyden to Attorney General Eric Holder." *Senator Ron Wyden website*, February 2, 2011. <http://www.wyden.senate.gov/download/?id=103d177c-6f30-469b-aba8-8bbfdd4fd197&download=1>
- Shaw, Zach. "Earache Records Responds to Spotify Press Release." *Metal Insider*, August 10, 2011. <http://www.metalinsider.net/digital-media/exclusive-earache-records-responds-to-spotify-press-release>
- Shelanski, Howard. "Network Neutrality: Regulating With More Questions Than Answers." *Journal of Telecommunications and High Tech* 6 (2007): 23-40.
- Shepard, Lorrie. "Evaluating test validity." *Review of research in education* (1993): 405-450.
- SJD. "Judge Baylson wants to test copyright trolls' evidence in a bellwether trial." *Fight Copyright Trolls*, October 7, 2012. <http://fightcopyrighttrolls.com/2012/10/07/judge-boylson-wants-to-test-copyright-trolls-evidence-in-a-bellwether-trial/>
- Smith, Michael D. and Rahul Telang. "Delaying Content Leaves Money on the Table." *the Hill*, November 29, 2011, 6:34 PM. <http://thehill.com/opinion/op-ed/196051-delaying-content-leaves-money-on-the-table>
- Sohn, David. "Statement of David Sohn, Senior Policy Counsel, Center for Democracy & Technology." *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part I: Hearing Before the H. Comm. on the Judiciary, Subcomm. on Intellectual Property, Competition, and the Internet*, 112th Cong. 6-9 (2011). <http://commcns.org/sCSXbA>
- Solmecke, Christian. "An overview of file sharing in Germany." *Wilde Beuger Solmecke*, February 28, 14. <https://www.wbs-law.de/eng/file-sharing-eng/overview-file-sharing-germany-50767/>
- Solove, Daniel. "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy." *San Diego Law Review* (2008).
- Solove, Daniel. "A Taxonomy of Privacy." *University of Pennsylvania Law Review* 154.3 (2006): 477-560.
- Solove, Daniel. "Conceptualizing Privacy." *California Law Review* 90 (2002): 1087-1155.
- Spanish ministry of Education, Culture and Sports. "La Policía y la Guardia Civil incautaron objetos que vulneraban derechos de propiedad intelectual por un valor superior a 6 millones de euros." *Press release, Spanish ministry of Education, Culture and Sports*, June 11, 2013. <http://www.mecd.gob.es/prensa-mecd/actualidad/2013/06/20130611-propiedad-intelectual.html>
- Spoor, J.H., D.W.F. Verkade, D.J.G. Visser. *Auteursrecht, naburige rechten en databankenrecht*. Deventer: Kluwer, Third print, 2005.
- Spotify. "Adventures in the Netherlands." *Press at Spotify*, July 17, 2013. <http://press.spotify.com/us/2013/07/17/adventures-in-netherlands/>
- Stadler, Sara K. "Copyright as Trade Regulation." *University of Pennsylvania Law Review* (2007): 899-960.

- Stamatoudi, Irini A. *Copyright enforcement and the Internet*. Vol. 21. Kluwer Law International, 2010.
- Steadman, Ian. "Study: copyright takedown notices are ineffective at stopping piracy." *Wired*, January 10, 2013. <http://www.wired.co.uk/news/archive/2013-01/10/blocking-no-effect-fileshearing>
- Stephan Ockhuijsen. "Stijgende prijs- en rockconcertkaartjes bevestigd." *Sargasso.nl*, March 28, 2013. <http://sargasso.nl/stijgende-prijs-pop-en-rockconcertkaartjes-bevestigd/>
- Stigler, George. "The Optimum Enforcement of Laws." in: *Essays in the Economics of Crime and Punishment*. ed. Gary Becker and William Landes, (1974), 55-67.
- Story, Louise. "Michigan Town Woos Hollywood, but Ends Up With a Bit Part." *the New York Times*, December 3, 2012. <http://www.nytimes.com/2012/12/04/us/when-hollywood-comes-to-town.html>
- Strowel, Alain. "The 'Graduated Response' in France: Is It the Good Reply to Online Copyright Infringement." in: *Copyright Enforcement and the Internet*, ed. Stamatoudi. Kluwer Law International, The Netherlands, 2010.
- Strumpf, Koleman. "Using Markets to Measure the Impact of File sharing on Movie Revenues." *Conference paper* (July 11, 2014), <http://conference.nber.org/confer/2014/SI2014/PRIT/Strumpf.pdf>
- Suzor, Nicolas and Brian Fitzgerald. "The Legitimacy of Graduated Response Schemes in Copyright Law." *University of New South Wales Law Journal* 34 (2011): 1.
- Svensson, Måns and Stefan Larsson. "Intellectual property law compliance in Europe: Illegal file sharing and the role of social norms." *New media & society* 14.7 (2012): 1147-1163.
- Swash, Rosie. "Online piracy: 95% of music downloads are illegal." *The Guardian*, January 17, 2009. <http://www.theguardian.com/music/2009/jan/17/music-piracy>
- Sweney, Mark. "Music, TV and film piracy rises among UK Internet users." *The Guardian*, May 28, 2013. <http://www.theguardian.com/media/2013/may/28/music-tv-film-piracy-uk-Internet>
- Taylor, Chris. "Hey hollywood, Online Piracy Doesn't Hurt Your U.S. Box Office Returns [STUDY]." *Mashable*, February 13, 2012. <http://mashable.com/2012/02/13/online-piracy-box-office/#mTHsb11Q9skl>
- Tech Law Journal. "DOJ/FBI Seize Domain Names by Warrant." *Tech Law Journal*, August 21, 2012. <http://www.techlawjournal.com/topstories/2012/home.asp>
- Telecompaper. "French ISPs demand compensation for Hadopi cooperation." *Telecompaper*, August 12, 2010. <http://www.telecompaper.com/news/french-isps-demand-compensation-for-HADOPI-cooperation--750964>
- Telecompaper. "French online music worth EUR 110 mln in 2011 – study." *Telecompaper*, January 31, 2012. <http://www.telecompaper.com/news/french-online-music-worth-eur-110-mln-in-2011-study--852719>
- Telecompaper. "Global broadband subscribers reach 700 million in 2012." *Telecompaper*, April 19, 2012. <http://www.telecompaper.com/news/global-broadband-subscribers-reach-700-mln-in-2012>
- The 1709 Blog. "Lescure Report on Cultural Exception in France - The Way Forward?" *The 1709 Blog*, May 20, 2013. <http://the1709blog.blogspot.nl/2013/05/lescurereport-on-cultural-exception-in.html>
- The Baltimore Sun. "DirecTV accuses thousands of signal theft." *The Baltimore Sun*, November 30, 2003. http://articles.baltimoresun.com/2003-11-30/business/0311290123_1_directv-satellite-television-piracy

The British Recorded Music Industry. *Digital Music Nation 2010*. BPI Limited 2010.

The Independent. "Rhodri Marsden: Why did my YouTube account get closed down?" *The Independent*, August 12, 2009. <http://www.independent.co.uk/life-style/gadgets-and-tech/features/rhodri-marsden-why-did-my-youtube-account-get-closed-down-1770618.html>

The Local Es. "Half of Spain's Internet users download illegally." *The Local Es*, April 9, 2014. <http://www.thelocal.es/20140409/spain-failing-in-fight-against-Internet-piracy>

The NPD Group. "After Years of Defection, The Number of U.S. Music Buyers is On The Upswing." *The NPD Group*, March 6, 2012. https://www.npd.com/wps/portal/npd/us/news/press-releases/pr_120306/.

Thompson, Derek. "How Hollywood accounting can make a \$450 million dollar movie unprofitable." *The Atlantic*, September 14, 2011. see: <http://www.theatlantic.com/business/archive/2011/09/how-hollywood-accounting-can-make-a-450-million-movie-unprofitable/245134/>

Thornburg, Elizabeth. "Going private: Technology, due process, and Internet dispute resolution." *University of California at Davis Law Review* (2000).

Tighe, Mark. "Eircoms 3 strikes scheme." *The blog of an Irish Journalist*, March 2012. <http://irishjournalist.blogspot.nl/2012/03/eircoms-3-strikes-scheme.html>

Tighe, Mark. "Eircom Cut Off 100 Illegal Downloaders." *Sunday Times*, March 4, 2012. <http://www.thesundaytimes.co.uk/sto/news/ireland/article988221.ece>

Timothy. "YouTube Identifies Birdsong As Copyrighted Music." *Slashdot*, February 26, 2012. <http://yro.slashdot.org/story/12/02/26/2141246/youtube-identifies-birdsong-as-copyrighted-music>

TMZ. "Justin Bieber Music Videos Yanked from YouTube." *TMZ*, August 29, 2011. <http://www.tmz.com/2011/08/29/justin-bieber-music-video-vevo-youtube-hacked-ilcreation-baby-somebody-to-love-that-should-be-me/>

Toner, Alan. "Ireland: Three Strikes and Fair Use." *kNOW Future Inc*. March 3, 2011. <http://knowfuture.wordpress.com/2011/03/03/ireland-three-strikes-and-fair-use/>

Torremans, Paul. *Intellectual property and human rights*. Vol. 18. Kluwer Law International, 2008.

Tremlett, Giles. "Spain finds that film piracy is a hard habit to break." *The Guardian*, March 31, 2010. <http://www.guardian.co.uk/world/2010/mar/31/spain-film-piracy-downloading-dvds>

Tripp, Volkter. "Germany gets warning about warning letters." *EDRI website*, January 14, 2015. see: <https://edri.org/germany-gets-warning-about-warning-letters/>

TruOptik. *Digital media unmonetized demand and peer-to-peer file sharing report* (2015). See: <http://truoptik.com/digital-media-unmonetized-demand-and-peer-to-peer-file-sharing-report-2014>

Tumbit. "Spain's latest 'Ley Sinde' revision." *Tumbit.spain*, April 14, 2011. <http://www.tumbit.com/news/articles/3047-spains-latest-ley-sinde-revision.html>

U.S. Chamber of Commerce. "19 Million American Jobs at Risk." *U.S. Chamber of Commerce*, May 12, 2011. <https://www.uschamber.com/ad/19-million-american-jobs-risk>

U.S. Copyright Office. "The Digital Millennium Copyright Act of 1998 - U.S. Copyright Office Summary" (December 1998). See: <http://www.copyright.gov/legislation/dmca.pdf>

U.S. Immigration and Customs Enforcement. "ICE, CBP announce year-end intellectual property seizure statistics." *News release, U.S. Immigration and Customs Enforcement* (March 24,

2014). <https://www.ice.gov/news/releases/ice-cbp-announce-year-end-intellectual-property-seizure-statistics>

- U.S. Immigration and Customs Enforcement. "ICE, European partners seize 328 Internet domains selling counterfeit goods in coordinated operation." *News release, U.S. Immigration and Customs Enforcement*, June 26, 2013. <https://www.ice.gov/news/releases/ice-european-partners-seize-328-Internet-domains-selling-counterfeit-goods-coordinated>
- U.S. Immigration and Customs Enforcement. "ICE, international law enforcement agencies seize 706 domain names selling counterfeit merchandise." *News release, U.S. Immigration and Customs Enforcement*, December 2, 2013. <https://www.ice.gov/news/releases/ice-international-law-enforcement-agencies-seize-706-domain-names-selling-counterfeit>
- U.S. Immigration and Customs Enforcement. "ICE, European partners seize 328 Internet domains selling counterfeit goods in coordinated operation." *News release, U.S. Immigration and Customs Enforcement*, June 26, 2013. <https://www.ice.gov/news/releases/ice-european-partners-seize-328-Internet-domains-selling-counterfeit-goods-coordinated>
- U.S. Immigration and Customs Enforcement. "ICE, European partners seize 328 Internet domains selling counterfeit goods in coordinated operation." *News release, U.S. Immigration and Customs Enforcement*, June 26, 2013. <https://www.ice.gov/news/releases/ice-european-partners-seize-328-Internet-domains-selling-counterfeit-goods-coordinated>
- U.S. Immigration and Customs Enforcement. "Department of Justice Seizes More Than \$1.5 Million in Proceeds from the Online Sale of Counterfeit Sports Apparel Manufactured in China." *News Release, U.S. Immigration and Customs Enforcement*, May 11, 2012. available at <http://www.justice.gov/opa/pr/2012/May/12-crm-610.html>
- U.S. Immigration and Customs Enforcement. "European Law Enforcement Agencies and Europol Seize 132 Domain Names Selling Counterfeit Merchandise in 'Project Cyber Monday 3' and 'Project Transatlantic Operations'." *News Release, U.S. Immigration and Customs Enforcement*, November 26, 2012. available at <http://www.ice.gov/news/releases/1211/121126washingtondc.htm>
- U.S. Immigration and Customs Enforcement. "HIS Seizes 686 Websites Selling Counterfeit Medicine to Unsuspecting Consumers." *News Release, U.S. Immigration and Customs Enforcement*, October 4, 2012. available at <https://www.ice.gov/news/releases/1210/121004washingtondc.htm>
- U.S. Immigration and Customs Enforcement. "Houston HIS Seizes 89 Websites Selling Counterfeit Goods." *News Release, U.S. Immigration and Customs Enforcement*, December 20, 2012. available at <https://www.ice.gov/news/releases/1212/121220houston.htm>
- U.S. Immigration and Customs Enforcement. "ICE Seizes 82 Website Domains Involved In Selling Counterfeit Goods As Part of Cyber Monday Crackdown." *News Release, U.S. Immigration and Customs Enforcement*, November 29, 2010. available at <https://www.ice.gov/news/releases/1011/101129washington.htm>
- U.S. Immigration and Customs Enforcement. "ICE, CBP, USPIA seize more than \$13.6 million in fake NFL merchandise during 'Operation Red Zone'." *News Release, U.S. Immigration and Customs Enforcement*, January 31, 2013. <https://www.ice.gov/news/releases/1301/130131neworleans.htm>

- U.S. Immigration and Customs Enforcement. "ICE, CBP, USPIIS seize more than \$13.6 million in fake NFL merchandise during 'Operation Red Zone'." *News Release, U.S. Immigration and Customs Enforcement*, January 31, 2013. <https://www.ice.gov/news/releases/1301/130131neworleans.htm>
- U.S. Immigration and Customs Enforcement. "ICE, international law enforcement agencies seize 706 domain names selling counterfeit merchandise." *News release, U.S. Immigration and Customs Enforcement*, December 2, 2013. <https://www.ice.gov/news/releases/ice-international-law-enforcement-agencies-seize-706-domain-names-selling-counterfeit>
- U.S. Immigration and Customs Enforcement. "ICE-Led IPR Center Seizes 70 Websites Duping Consumers Into Buying Counterfeit Merchandise." *News Release, U.S. Immigration and Customs Enforcement*, July 12, 2012. <https://www.ice.gov/news/releases/1207/120712washington.htm>
- U.S. Immigration and Customs Enforcement. "Leader of Internet piracy group "IMAGiNE" sentenced in Virginia to 60 months in prison for criminal copyright conspiracy." *News Release, U.S. Immigration and Customs Enforcement*, January 3, 2013. <https://www.ice.gov/news/releases/1301/130103washingtondc2.htm>
- U.S. Immigration and Customs Enforcement. "New York Investigators Seize 10 Websites That Illegally Streamed Copyrighted Sporting and Pay-per-view Events." *News Release, U.S. Immigration and Customs Enforcement*, February 2, 2011. available at <http://www.ice.gov/news/releases/1102/110202newyork.htm>
- U.S. Immigration and Customs Enforcement. "Operation In Our Sites" Targets Internet Movie Pirates, ICE, Manhattan U.S. Attorney Seize Multiple Web Sites for Criminal Copyright Violations." *News Release, U.S. Immigration and Customs Enforcement*, June 30, 2010. available at <https://www.ice.gov/news/releases/1006/100630losangeles.htm>
- U.S. Immigration and Customs Enforcement. "Operation In Our Sites Protects American Online Shoppers, Cracks Down on Counterfeiters." *News Release, U.S. Immigration and Customs Enforcement*, November 28, 2011. available at <https://www.ice.gov/news/releases/1111/111128washingtondc.htm>
- U.S. Immigration and Customs Enforcement. "Special Agents and Officers Seize More Than \$4.8 Million in Fake NFL Merchandise and Seize 307 Websites During 'Operation Fake Sweep.'" *News Release, U.S. Immigration and Customs Enforcement*, February 2, 2012. available at <https://www.ice.gov/news/releases/1202/120202indianapolis.htm>
- U.S. Immigration and Customs Enforcement. "Sweetheart, But Fake, Deals Put On ICE "Operation Broken Hearted" Protects Consumers From Counterfeit Valentine's Day Goods." *News Release, U.S. Immigration and Customs Enforcement*, February 14, 2011. available at <https://www.ice.gov/news/releases/1102/110214washingtondc.htm>
- U.S. Immigration and Customs Enforcement. "Federal Courts Order Seizure of Three Website Domains Involved in Distributing Pirated Android Cell Phone Apps." *Press Release, U.S. Department of Justice*, August 21, 2012. available at <http://www.justice.gov/opa/pr/2012/August/12-crm-1033.html>
- U.S. Immigration and Customs Enforcement. "Houston HSI seizes 10 domain names selling counterfeit cycling products." *News Release, U.S. Immigration and Customs Enforcement*, April 29, 2013. <https://www.ice.gov/news/releases/1304/130429houston.htm>
- Ulanoff, Lance. "The End of Content Ownership." *PC Mag*, April 11, 2011. <http://www.pcmag.com/article2/0,2817,2383373,00.asp>

- Unite the Cows. "UK ISPs to block the pirate bay and other file sharing sites." *Unite the Cows*, <http://www.unitethecows.com/content/366-uk-isp-s-block-pirate-bay-other-file-sharing-sites.html>, retrieved on 26-10-2011.
- United States Trade Representative. "2013 Special 301 Report." *The Office of the United States Trade Representative* (USTR), January 5, 2013. <https://ustr.gov/sites/default/files/05012013%202013%20Special%20301%20Report.pdf>
- Urban, Jennifer and Laura Quilter. "Efficient Process or 'Chilling Effects'? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act." *Santa Clara Computer and High Technology Law Journal* 22 (2006): 621.
- Urban, Jennifer M. and Karaganis, Joe and Schofield, Brianna L. "Notice and Takedown in Everyday Practice." *UC Berkeley Public Law Research Paper* No. 2755628. March 29, 2016. Available at SSRN: <http://ssrn.com/abstract=2755628>
- USA Today. "Minnesota Woman Caught in Crackdown on Music Downloaders." *USA Today*, June 11, 2004.
- Van Bergen, Matthijs. "Communitysite geven te gemakkelijk toe bij auteursrechtclaims." *Hostingrecht.nl*, <https://hostingrecht.nl/auteursrecht/communitysites-geven-te-gemakkelijk-toe-bij-auteursrechtclaims/>, the full study by ICT Recht can be found here: <https://ictrecht.nl/notice-takedown-rapport-communitysites-ictrecht-20090306.pdf>
- Van Buskirk, Elliot. "Report Shows Big Increase in Spotify's Payouts to Indie Labels (Updated)." *Evolver.fm*, May 8, 2012. <http://evolver.fm/2012/05/08/confidential-report-shows-big-increase-in-spotifys-payouts-to-indie-labels/>
- Van Buskirk, Elliot. "A poison pen from the RIAA." *Wired*, February 28, 2007.
- Van Buskirk, Elliot. "RIAA to stop suing music fans, cut them off instead." *Wired*, December 19, 2008. <http://www.wired.com/epicenter/2008/12/riaa-says-it-pl/>.
- Van der net, Cyril. "De Civielrechtelijke Aansprakelijkheid van Internetproviders na de Richtlijn Elektronische Handel." *JAVI* (2002/1).
- Van Hoek, Colin. "Netflix zorgt voor afname Bittorrent-verkeer." *Nu.nl*, November 8, 2012. <http://www.nu.nl/Internet/2953432/netflix-zorgt-afname-bittorrent-verkeer.html>
- Vernik, Dinah A., Devavrat Purohit, and Preyas S. Desai. "Music Downloads and the Flip Side of Digital Rights Management." *Marketing Science* 30 (2011): 1011.
- Visser, Dirk. "De interrectuele eigendom van het Grootkapitaal." *AMI: tijdschrift voor auteurs-, media-en informatierecht* 2011 (2011): 2.
- Volokh, Eugene and Brett McDonnell. "Freedom of Speech and Independent Review in Copyright Cases." *The Yale Law Journal* 107.8 (1998): 2431-2471.
- Von Lohmann, Fred. "Report: How Google Fights Piracy." *Google Public Policy Blog*, September 10, 2013. <http://googlepublicpolicy.blogspot.nl/2013/09/report-how-google-fights-piracy.html> and Google. *How Google Fights Piracy*, Google Report, September 2013. See: <https://docs.google.com/a/google.com/file/d/0BwxyRPFduTN2dVFqYml5UENUeUE/edit?pli=1>
- Von Lohmann, Fred. "RIAA v. The People turns from lawsuits to 3 strikes." *the Electronic Frontier Foundation*. December 19, 2008. <http://www.eff.org/deeplinks/2008/12/riaa-v-people-turns-lawsuits-3-strikes>
- Von Lohmann, Fred. "Fair use, film, and the advantages of Internet distribution." *Cinema Journal* (2007): 128-133.

- Fred von Lohmann. "Testing YouTube's Audio Content ID System." *Electronic Frontier Foundation*. April 29 2009. available at <https://www.eff.org/deeplinks/2009/04/testing-youtubes-aud>
- Wallei, Linus. *Copyright does not exist* (chapter 'subculture of subcultures'). Found through Way back machine (July 25, 2011): <http://web.archive.org/web/20110725143825/http://home.c2i.net/nirgendwo/cdne/ch5web.htm>
- Watercutter, Angela. "Mumford & Sons warn against 'unauthorized lending' of their CD." *Wired*, December 23, 2012. <http://www.wired.com/2012/12/mumford-sons-lending-copyright/>
- Watt, Richard. *Copyright and Economic Theory: Friends or Foes?* Edward Elgar Publishing, 2000.
- Waxy. "No Copyright Intended." *Waxy*, December 9, 2011. http://waxy.org/2011/12/no_copyright_intended/
- Webwereld. "Brein: 600 sites offline gehaald in 2011." *Webwereld*, February 21, 2012. <http://webwereld.nl/e-commerce/56117-brein-600-sites-offline-gehaald-in-2011>
- Weiss, Debra Cassens. "Porn Industry Lawyer Is New Copyright King with 16,700 Lawsuits Filed." *ABA Journal*, November 10, 2010. http://www.abajournal.com/news/article/porn_industry_lawyer_is_new_copyright_king_with_16700_lawsuit_filed
- Weitenberner, Christian. "New YouTube Features for Music Artists." *The Official YouTube Blog*, October 16, 2011. <http://youtube-global.blogspot.com/2011/10/new-youtube-features-for-music-artists.html/>
- Welsh, Nancy. "Remembering the Role of Justice in Resolution: Insights from Procedural and Social Justice Theories." *Journal of Legal Education* (2004): 49-59.
- Westerlaken, Niels. "BREIN verwijdt onterecht advertenties: auteurs de dupe." *Bits of Freedom*, October 10, 2012. <https://www.bof.nl/2012/10/10/brein-verwijdt-onterecht-advertenties-auteurs-de-dupe/>
- White, Lynette and Sean Elliot. "Large-scale Copyright Infringement: the Inevitable Consequence of the Digital Age." *Melbourne School of Engineering, Department of Computer Science and Software Engineering* (2001).
- Wiggin Entertainment Media Research. *Digital Entertainment Survey* (2011). Available at: <http://www.slideshare.net/WigginLLP/digital-entertainment-survey-2011>
- Williams, Christopher. "Filesharing ambulance chasers get into the gay smut racket." *The Register*, November 19, 2008. http://www.theregister.co.uk/2008/11/19/davenport_lyons_filesharing/
- Wilson, Drew. "French Government and ISPs Negotiating Who Foots Approx. \$64 Million USD a Year HADOPI Bill." *ZeroPaid*, August 12, 2010. <http://www.zeropaid.com/news/90268/french-government-and-isps-negotiating-who-foots-approx-64-million-usd-a-year-HADOPI-bill/>
- Wilson, Drew. "HADOPI Blamed for ISP Rate Hikes in France." *ZeroPaid*, January 1, 2011. http://www.zeropaid.com/news/91800/HADOPI-blamed-for-isp-rate-hikes-in-france/?utm_source=twitterfeed&utm_medium=twitter
- Winistorfer, Andrew. "Seven crimes that will get you a smaller fine than file sharing." *Prefixmag*, August 21, 2009.
- Winseck, Dwayne. "Restrictive copyright plays into music industry myths." *The Globe and Mail*, May 17, 2011. <http://www.theglobeandmail.com/technology/digital-culture/restrictive-copyright-plays-into-music-industry-myths/article624736/#articlecontent>
- Wired. "The Second Coming." *Wired Magazine*, November 7, 2011. <http://castroller.com/Podcasts/WiredFeatures/2678827>

Witt, Ryan. "GOP works to cover up video they previously published on Internet." *Examiner.com*, March 30, 2011. <http://www.examiner.com/political-buzz-in-national/gop-trying-desperately-to-cover-up-video-they-previously-published-on-Internet>

Wortham, Jenna. "The Unrepentant Bootlegger." *The New York Times* (Set. 27, 2014). <http://www.nytimes.com/2014/09/28/technology/the-unrepentant-bootlegger.html>

Wyden, Ron. "Letter from Ron Wyden, U.S. Senator, to Eric Holder, U.S. Attorney Gen., & to John Martin, Dir., U.S. Immigration & Customs Enforcement" (Feb. 2, 2011). available at <http://www.wyden.senate.gov/download/?id=103d77C-6f30-469b-ab98-8bbfdd4>

Yin, Robert. *Case study research, Design and methods*. Third edition, Sage Publications, 2003.

Yu, Peter. "The Graduated Response." *Florida Law Review* 62 (2010): 1373-1430.

Zentner, Alejandro. "Measuring the effect of file sharing on music purchases." *Journal of Law and Economics* 49.1 (2006): 63-90.

ZeroPaid. "8 Technical Methods that make the protect IP act useless." *ZeroPaid*, <http://www.zeropaid.com/news/95013/8-technical-methods-that-make-the-protect-ip-act-useless/>, retrieved on 26-10-2011.

Zevenberg, Ben. "Empirical Data Suggests That Website Blocking Is A Useless Weapon Against Infringement." *Techdirt*, October 24, 2012. <http://www.techdirt.com/articles/20121018/02011120745/empirical-data-suggests-that-website-blocking-is-useless-weapon-against-infringement.shtml>

Zittrain, Jonathan, Kendra Albert and Alicia Solow-Niederman. "A Close Look at SOPA." *Future of the Internet*, December 2, 2011. <http://futureoftheInternet.org/reading-sopa>

Zittrain, Jonathan. *The future of the Internet--and how to stop it*. Yale University Press, 2008.

Zwetsloot, Joris. "Buma Stemra betaalt te weinig voor online muziek." *de Volkskrant*, June 1, 2015.

Case law used and referenced

US

- A&M v. Napster, 239 F.3d 1004 (9th Cir. 2001)
- Achte/Neunte Boll Kino Beteiligungs GMBH & Co KG v. Does 1–4,577, No. 1:10-cv-00453, 2010 WL 3522256 (D.D.C. Mar. 18, 2010)
- AF Holdings, LLC v. Does 1-97, No. C-11-03067-CW (DMR), 2011 WL 2912909, at *1 (N.D. Cal. July 20, 2011)
- AIDS Action Comm. v. Massachusetts Bay Transp. Auth., 42 F3d 1, 7 (1st Cir. 1994)
- Aimster, 334 F.3d 643 (7th Cir. 2003)
- Association of Community Orgs. for Reform Now v. St. Louis County, 930 F.2d 591, 595-96 (8th Cir. 1991)
- Baker v. Selden, 101 U.S. 99, 105 (1879)
- BitTorrent Adult Film Copyright Infringement Cases, 296 F.R.D. 80, 92 (E.D.N.Y. 2012)
- Braun v. Soldier of Fortune Magazine, Inc., 968 F.2d 1110, 1120-21 (11th Cir. 1992)
- Call of the wild movie v. Jason Smith, Joseph Sonka, and Does 1-331, Civol action no. 10-0455 (BAH), United States District Court for the District of Columbia
- Capitol Records Inc. v. Thomas, 579 F. Supp. 2d 1210, 1213 (D. Minn. 2008)
- Capitol Records Inc. v. Thomas-Rasset, No. 06cv-1497 (D. Minn. Jan. 22, 2010).

- Charter Commc'ns, Inc.m 393 F.3d
- Charter Commc'ns, Inc., Subpoena Enforcement Matter, 393 E3d 771, 777 (8th Cir. 2005)
- Collins, Inc v. Does 1–118, No. 3:10cv92 (N.D.W. Va. Sept. 24, 2010)
- Combat Zone, Inc v. Does 1–1037, No. 3:10cv95 (N.D.W. Va. Sept. 24, 2010)
- Combat Zone, Inc v. Does 1–245, No. 3:10cv96 (N.D.W. Va. Sept. 24, 2010)
- Digital Sin, Inc. v. Does 1-176, No. 12-CV-00126 (AJN), 2012 WL 263491 (S.D.N.Y. Jan. 30, 2012)
- Dragon Quest Prods., LLC v. Does 1–100, Civ. Nos. 12–6611 (JHR/AMD), 12–6633 (NLH/AMD), 13–482 (NLH/AMD), 13–483 (NLH/AMD), 13–484 (NLH/AMD), 13–485 (NLH/AMD), 13–486 (NLH/AMD), 13–487 (NLH/AMD), 2013 WL 2949407 (D.N.J. June 14, 2013)
- Estate of Martin Luther King, Jr., Inc. v. CBS, Inc. (194 F.3d 1211 (11th Cir. 1999))
- Fannie Mae Derivative Litig., 227 F.R.D. 142, 142 (D.D.C. 2005)
- Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 261 (9th Cir. 1996)
- Hard Drive Prods., Inc. v. Does 1-188, 809 E Supp. 2d 1150 (N.D. Cal. 2011)
- Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 558 (1985)
- Herceg v. Hustler Magazine, Inc., 814 F.2d 1017, 1021 (5th Cir. 1987)
- Luke Records, Inc. v. Navarro, 960 F.2d 134, 138 (11 Cir. 1992)
- MCGIP, LLC v. Does 1-149, No. C 11-02331 LB, 2011 WL 4352110 (N.D. Cal. Sept. 16, 2011)
- Memorandum of Amicus Curiae Electronic Frontier Foundation in Support of Third Party Time Warner Cable's Motion to Quash or Modify Subpoena at 1, Third World Media LLC v. Does 1-1243, No. 3:10-cv-0090, (N.D. W. Va. Nov. 23, 2010), <https://www.eff.org/files/filenode/wvcopyrighttroll/thirdworldmediavdoesamicus.PDF>
- MGM v. Grokster, 380 F.3d 1154 (9th Cir. 2004)
- New York Times Co. v. Sullivan, 376 U.S. 254, 279-90 (1964)
- Nu Image, 799 F. Supp. 2d 34; New Sensations, Inc. v. Does 1-1474, No. C 11-2770 MEJ, 2011 WL 4407222 (N.D. Cal. Sept. 22, 2011)
- On the Cheap, LLC v. Does 1-501t, No. C10-4472 BZ, 2011 WL 4018258 (N.D. Cal. Sept. 6, 2011)
- OPG v. Diebold, 337 F. Supp. 2d 1195 (N.D. Cal. 2004)
- Pac. Century Int'l, Ltd. v. Does 1-101, No. C-1 1-02533 (DMR) (N.D. Cal. July 8,2011), 2011 WL 246114
- Patrick Collins, Inc v. Does 1–281, No. 3:10cv91(N.D.W. Va. Sept. 24, 2010)
- Peel v. Attorney Registration & Disciplinary COmm'n, 496 U.S. 91, 108 (1990)
- Recording Industry Association of America, Inc. v. Verizon Internet Servs., Inc., 351 F3d 1229, 1232 (D.C. Cir. 2003)

- Righthaven v. Leland Wolf and It makes sense blog, Civil action no. 1:11-ev-00830-JLK, United States District Court for the District of Colorado
- Settlement Letter from John L. Steele, Attorney, Steele Hansmeier, PLLC (May 16, 2011), http://msnbcmedia.msn.com/i/MSNBC/Sections/NEWS/z_Personal/AJohnson/110719_Steele_Hansmeier_Settlement_Letter.pdf, also found here: <https://dietrolldie.files.wordpress.com/2011/09/57230736-settlement-letter.pdf>
- Sony BMG Music Entm't v. Tenenbaum, No. 07cv1 1446-NG (D. Mass. Dec. 7, 2009)
- Standing Comm. v. Yagman, 55 F.3d 1430, 1443 (9th Cir. 1995)
- Stephanie Lenz v. Universal Music Group Corp., Universal Music Publishing, Inc., and Universal Music Publishing Group, No. C 07-3783, Second Amended Complaint (N.D. Cal. Apr. 18, 2008)
- Swineford v. Snyder County, 15 F.3d 1258, 1265 (3rd Cir. 1994)
- Third World Media, LLC v. Does 1–1243, No. 3:10cv90 (N.D.W. Va. Sept. 24, 2010)
- Turner Broad. Sys., Inc. v. FCC (Turner I), 512 U.S. 622, 666-67 (1994)
- United States v. Moghadam, 175 F.3d 1269, 1277 (11th Cir. 1999)
- Voltage Pictures, LLC v. Does 1–5,000, No. 1:10-cv-00873 (D.D.C. June 7, 2010), ECF No. 4-3
- VPR Internationnale v. Does 1-1017, U.S. District Court, ILCD, (April 29, 2011)
- West Coast Prods., Inc v. Does 1–535, No. 3:10cv94 (N.D.W. Va. Sept. 24, 2010)
- West Coast Prods., Inc., v. Does 1–2010, No. 3:10cv93 (N.D.W. Va. Sept. 24, 2010)
- White-Smith Music Pub. Co. v. Apollo Co., 209 U.S. 1, 18 (1908)

Netherlands

- Hof 's-Gravenhage 15 nov. 2010, IER 2011/27, p.174 with annotation by Koelman (ACI Adam c.s./ThuisKopie)
- Hof 's-Gravenhage 15 nov.2010, IER 2011/28, p.197 with annotation by Koelman (FTD/Eyeworks)
- Hof Amsterdam 28 maart 2002, AMI 2002, nr 13, p. 134, LJM AE805, Mf 2002, nr 19, p. 188 m.nt. K.J.Koelman (Buma/KaZaA)
- Hof Amsterdam 7 nov. 2002, NJ 2003, 54 (XS4ALL/Deutsche Bahn)
- HR 25 nov. 2005, NJ 2009, 550 with annotation by P.B. Hugenholtz (Lycos/Pessers)
- Rb. 's-Gravenhage 9 June 1999, AMI 1999 (Scientology/XS4ALL)
- Rb. Jaarlem 12 mei 2004, AMI 2004, nr 15, p. 185 with annotation by Koelman, LJM AO9318 (Techno Design/Brein)
- Rechtbank Amsterdam 22 October 2009, LJM BK1067 The Pirate Bay versus BREIN
- Rechtbank Utrecht 26 August 2009, LJM BJ6008, BREIN versus Mininova
- Vزر. Rb. 's-Gravenhage 5 jan. 2007, IER 2007/22, p.96 (Brein/KPN)
- Vزر.Rb. Haarlem 12 mei 2004, IER 2004/57, p.263 (Brein/Techno Design)
- Vزر. Rb. Utrecht 12 june 2005, NJ 2005, 387 (Brein/UPC)

France

- Decision 2009-580 DC of 10 June 2009, at: www.conseil-constitutionnel.fr

Ireland

- EMI Records (Ireland Ltd v Data Protection Commissioner (2012) IEHC 264
- EMI Records (Ireland) Ltd & Ors –v- UPC Communications Ireland Ltd (2010) IEHC 377 (10 November 2010)
- EMI Records (Ireland) Ltd & Ors v. Eircom Ltd & Anor [2005] IEHC 233 (8 July 2005)
- EMI Records v. Eircom Ltd., [2010] IEHC 108

UK

- Media CAT Ltd v Adams & Ors [2011] EWPC 6 (08 February 2011)
- Solicitors Disciplinary Tribunal, Case No. 10619-2010, Miller and Gore
- Solicitors Disciplinary Tribunal, Case No. 10726-2011, Crossley

EU

- CJEU Case C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, 29 January 2008.
- CJEU Case C-324/09, L'Oréal SA v. International AG, 12 July 2011.
- CJEU Case C-70/10, Scarlet Extended SA v. SABAM, 24 November 2011.

Interviews and personal communication

- Alex de Joode (Leaseweb), interviewed by author, January 2014
- Alex de Joode (Leaseweb), interviewed by author, May 2013
- Andrew Bridges (Lawyer at Fenwick & West LLP), interviewed by author, September 2013.
- Arjan van Hattum (XS4ALL), interviewed by author, November 2013
- Cara Duckworth (Communications at the Recording Industry Association of America) email to author, October 2013
- Corynne McSherry (Intellectual Property Director Electronic Frontier Foundation) interviewed by author, September 2013
- Delvan Neville (technologist), interviewed by author, September 2013
- Dick Doyle (IRMA) interviewed by author, January 2014
- Dick Doyle (IRMA) interviewed by author, November 2013
- Digimarc Guardian, interviewed by author, October 2013
- Fred Felman (DtecNet) interviewed by author, November 2013
- Fred von Lohmann (Intellectual Property Director Google) interviewed by author, August 2013
- Frédéric Dejonckheere (SFR) email to author, March 2014
- Frederic Delacroix (SFR) email to author, February 2014
- Gill Sperlein (Lawyer) interviewed by author, September 2013

- Kate O Sullivan (UPC Ireland) interviewed by author, June 2013
- Marcel Eswilder (Ziggo), interviewed by author, May 2013
- Margreth Verhulst (XS4ALL), interviewed by author, May 2013
- Mark Lemley (Professor at Stanford Law School), interviewed by author, September 2013
- Miguel Perez Subias (AUI), interviewed by author, February 2014
- Mitch Stoltz (Staff attorney at Electronic Frontier Foundation) interviewed by author, September 2013
- Nancy Gertner (Professor at Harvard Law School) interviewed by author, October 2013
- Otis D. Wright, II (District Judge) interviewed by author, September 2013
- Sarah Jacquier (Legal Director of HADOPI) interviewed by author, January 2014
- Solicitors Disciplinary Tribunal (SDT) email to author, April 2014
- Steven Welk (USACAC), interviewed by author, October 2013
- Tim Kuik (BREIN), email to author, July 2013
- Tim Kuik (BREIN), interviewed by author, May 2013
- Victor Domingo (Internautas), email to author, April 2014
- Wilko Miletic (Clinic), email to author, June 2013

ACKNOWLEDGEMENTS

Terwijl ik nadacht over mijn dankwoord zocht ik naar treffende metaforen om het promotieproces te omschrijven. Ik kwam niet verder dan clichés: het voelde soms als het leren van een nieuwe vechtsport waarbij ik moest incasseren, of een nieuwe dans waarbij de leraar mij een nieuwe techniek bijbracht. In de lichtere dagen voelde ik me deel van een eeuwenoude traditie en ging ik in gedachten gehuld in witte toga met krullende baard met anderen de discussie aan. Op de donkerdere dagen voelde het als legertraining. Maar meestal voelde het als een soort lange reis, die me op verschillende plekken bracht met verschillende reisgenoten, een ‘buddy movie’ en een ‘coming of age film’ waarbij de hoofdpersoon een aantal ingrijpende wijzigingen in zijn leven maakt om door te kunnen.

Al die beelden doen natuurlijk geen recht aan het proces. Promoveren is een voorrecht. De mogelijkheid om echt lang over ‘de dingen’ na te denken, te leren over echt onderzoek doen en het toevoegen van nieuwe kennis is een zeldzaamheid in onze gejaagde samenleving. Je leert hoe je nieuwe dingen kan weten en hoeveel je eigenlijk niet weet. Ik beschouw het als een eer dat ik dat proces heb meegemaakt. Dat geldt overigens ook voor college geven en vakken coördineren aan de universiteit.

Misschien doen die beelden ook geen recht aan het proces omdat ze ten onrechte suggereren dat ik als een soort hoofdpersoon of regisseur alle keuzes heb gemaakt en zelf alle stappen heb gezet. Dat is niet zo: ik had een geweldige ‘supporting cast’:

Binnen de wetenschap geldt dat in ieder geval voor mijn promotor Michel van Eeten. Ik hoop dat ik niet het beeld heb gewekt dat je een soort martial arts sensei, dansleraar, bebaarde filosoof, of leger officier was. Je was geen van dat alles en ze allemaal tegelijk. Je was een leermeester, steun, inspirator en ik ben erg dankbaar dat je me na een jaar onder je vleugels nam en mij daar tot ver na mijn tijd in Delft hebt gehouden. Ik heb erg veel van je geleerd en altijd veel gehad aan onze gesprekken samen. Ik vond het puzzelen ook plezierig al kan ik me voorstellen dat ik tegen einde die indruk niet meer gaf. Als ik een fractie van jouw kritische vermogen heb meegekregen tijdens mijn promotietijd is dat iets waar ik voorgoed van profiteer.

I owe many thanks to David Koepsell. I am very thankful that I barged into your office in my first year after I read your book on genetics. Through your help, I could get started on my research and you helped me with some of my first publications. Your continued advice in the following years added much to the research and to my development as a thinker. I’m glad we got to know each other afterwards and enjoyed our many conversations on the state of society. I would not be here if it was not for you. Thank you.

I would also like to thank my committee members. Thank you for taking the time to read my work, and for your comments. Although the last step was tough, I’m positive my dissertation has become much better as a result.

Dan Delft. Ik wil graag NGI bedanken voor de beurs die dit onderzoek mogelijk maakte. Verder wil ik graag al mijn oud collega’s in Delft bedanken bij de POLG sectie. In het bijzonder Nienke Saanen, met wie ik de colleges rechten verzorgde en met wie ik veel heb samen gewerkt. Daarnaast heb ik binnen Delft met veel plezier deelgenomen aan de PhD groep Internet Governance, met Hadi, Harald, and Shirin. Ook ben ik prof. Helen Stout en prof. Suzan Stoter dankbaar voor hun hulp in het begin. Tijdens en na mijn werk heb ik daarnaast veel ondersteuning (en steun) gehad van het secretariaat. Dank jullie wel!

During my PhD I was fortunate enough to travel abroad a couple of times. I had an excellent time at the University of Essex, where I was schooled in methodology by Sebastian Dellepiane-Avellaneda. Afterwards, I was particularly fortunate to become an International Google Policy Fellow, which allowed me to spend almost three months at the Electronic Frontier Foundation in San Francisco. I thank Google for granting me the opportunity, and the EFF for their hospitality, particularly Danny O' Brien and Maira Sutton. After San Francisco, I spent one month at Michigan State University. I would like to thank Professor Johannes Bauer for his warm welcome and support. Without your help I would also never have been to overcome the administrative hurdles I faced to get to the US.

Buiten Delft heb ik verder goede gesprekken gehad met de mensen van het instituut voor Informatierecht in Amsterdam en ben ik (ook van de UvA) Ronald van Ooijk dankbaar, die mij als mijn scriptiebegeleider ooit in contact heeft gebracht met de Universiteit Delft.

Mijn proefschrift was een lange reis, die zich lastig liet combineren met een nieuwe baan en andere zaken. Dat was zwaar. Ik heb echt ongelooflijk veel mazzel gehad dat ik de volledige reis niet alleen hoefde te maken en al die tijd een goede en gezellige reisgenoot had. Theo, ik ben blij dat je tegelijkertijd begon en dat je al die jaren mijn kamergenoot was. We deelden frustraties, lange wandelingen, mooie tijden, goede gesprekken, kerstlunch bij IKEA, kerstbomen en meer. En je weet van alles wat: van kookrecepten tot chemie en ICT. Dat is ook fijn. Heel veel dank.

Buiten de wetenschap zijn er velen die ik zeer dankbaar ben. Inmiddels ben ik twee werkgevers verder. Ik wil mijn oude collega's bij Bits of Freedom van harte bedanken voor het sparren over het onderwerp en voor het dulden van mijn geklaag. In het bijzonder ben ik directeur Hans de Zwart dankbaar voor het begrip en de ruimte die hij bood (en de hulp met Inkscape).

Ik wil mijn huidige werkgever, het ministerie van Binnenlandse Zaken, bedanken, omdat ik een maand later kon beginnen met mijn nieuwe baan zodat ik de laatste puntjes op de i kon zetten.

Daarnaast ben ik mijn verdere vrienden en familie erg dankbaar. Bijvoorbeeld Ferry, met wie ik tijdens mijn promotie volgens mij gemiddeld twee avonden van de week doorbracht. Gesprekken tot diep in de nacht. Ik had mazzel dat je zo dichtbij woonde. En eerlijk is eerlijk, het was gewoon tof die tijd. Voor mijn gevoel was ik bijna net zoveel tijd op het Funen. Pepijn, ik ben blij dat ik altijd bij je terecht kon. Ook koester ik de intellectuele en veel minder intellectuele discussies met Thijs. En alles wat buiten Funen valt maar ook eigenlijk Funen is. Hidde, "Jasper," Ivo, Sascha, Bart, FJ en verder.

Verder veel dank voor de gesprekken met- en aanmoediging van Barend, en Julius. In Brussel en in Amsterdam. Welcome distraction was spent in Germany with Falk. Ook andere 'boys' ben ik dankbaar: "Stefan", Jort, Zohar en Max. In het bijzonder ben ik ook Nikki dankbaar, die vanaf het begin met mij mee dacht, zoals hij dat al jaren doet op elk vlak van het leven. Ik wil ook graag Maral bedanken. Je was een grote steun in het begin. Heel erg bedankt. Ik bedank ook graag Menno, het betekent erg veel voor me dat we al sinds we twaalf zijn elk klein detail van het leven delen en uitwisselen.

Veel van jullie hebben mij ook feedback gegeven op mijn proefschrift (in het bijzonder veel dank voor de hulp van Ella), heel erg veel dank daarvoor. Volgens mij krijgen jullie nog een etentje van me. Voor alle anderen die ik niet noem en die iets hebben bijgedragen, veel dank!

Ik begon dit dankwoord onbedoeld met de metafoer van een film. Een vaak onderbelichte speler in de totstandkoming van een film is de producer. Ik wil daarom nog

mijn ouders bedanken, en natuurlijk mijn broertje (en Anna!), voor de steun en alle kansen die jullie mij geboden hebben.

Tot slot wil ik natuurlijk Dian bedanken. Oorspronkelijk voelde mijn reis naar Michigan als een vervelende verplichting om naar San Francisco te kunnen. Ik had nooit kunnen voorzien dat ik daar de vrouw zou ontmoeten met wie ik nu zo fijn samen woon, aan wie ik zo veel steun heb beleefd en met wie ik zulke leuke dingen doe. Samen kunnen we alles aan.

CURRICULUM VITAE

Floris Kreiken (1982) studied European studies (BA) and Law (LLM) at the University of Amsterdam. During his studies he worked as an intern in the Dutch and European Parliament and was chair of the Young Democrats, a Dutch political youth organisation. He obtained his masters degree in International and European law in 2007.

From 2009 to 2013 Floris was a PhD candidate at the Faculty of Technology, Policy and Management of Delft University of Technology. During this time, he served as a deputy member of the city council of Amsterdam. During his research, he spent 3 months as an International Google Policy Fellow at the Electronic Frontier Foundation in San Francisco, and 1 month as a visiting scholar at Michigan State University.

He worked at Dutch NGO Bits of Freedom as a human rights advocate from 2014 to 2016. He currently works for the Dutch Ministry of Home Affairs as a policy advisor on the information society and government.

Floris (co) authored several articles, including:

- **Kreiken, F.H.**, and Koepsell, D. (2013), *Coase and Copyright*, Illinois Journal of Law, Technology & Policy, Spring 2013.
- De Bruijn, H., van Bueren, E., **Kreiken, F.H.** (2012) *Framing en reframing in het klimaatdebat*, Bestuurskunde, November 2012.
- Koepsell, D. and **Kreiken, F.H.** (2012) *The Open Source Society and its Enemies*, Humanities and Technology Review, October 2012.
- **Kreiken, F.H.** (2009) *Criminaliteitsbestrijding of interne markt?*, Nederlands tijdschrift voor Europees recht, juli 2009, nr. 6.

NGInfra Ph.D Thesis Series on Infrastructures

1. Strategic behavior and regulatory styles in the Netherlands energy industry
Martijn Kuit, 2002, Delft University of Technology, the Netherlands.
2. Securing the public interest in electricity generation markets, The myths of the invisible hand and the copper plate
Laurens de Vries, 2004, Delft University of Technology, the Netherlands.
3. Quality of service routing in the internet: theory, complexity and algorithms
Fernando Kuipers, 2004, Delft University of Technology, the Netherlands.
4. The role of power exchanges for the creation of a single European electricity market: market design and market regulation
François Boisseleau, 2004, Delft University of Technology, the Netherlands, and University of Paris IX Dauphine, France.
5. The ecology of metals
Ewoud Verhoef, 2004, Delft University of Technology, the Netherlands.
6. MEDUSA, Survivable information security in critical infrastructures
Semir Daskapan, 2005, Delft University of Technology, the Netherlands.
7. Transport infrastructure slot allocation
Kaspar Koolstra, 2005, Delft University of Technology, the Netherlands.
8. Understanding open source communities: an organizational perspective
Ruben van Wendel de Joode, 2005, Delft University of Technology, the Netherlands.
9. Regulating beyond price, integrated price-quality regulation for electricity distribution networks
Viren Ajodhia, 2006, Delft University of Technology, the Netherlands.
10. Networked Reliability, Institutional fragmentation and the reliability of service provision in critical infrastructures
Mark de Bruijne, 2006, Delft University of Technology, the Netherlands.
11. Regional regulation as a new form of telecom sector governance: the interactions with technological socio-economic systems and market performance
Andrew Barendse, 2006, Delft University of Technology, the Netherlands.
12. The Internet bubble - the impact on the development path of the telecommunications sector
Wolter Lemstra, 2006, Delft University of Technology, the Netherlands.
13. Multi-agent model predictive control with applications to power networks
Rudy Negenborn, 2007, Delft University of Technology, the Netherlands.
14. Dynamic bi-level optimal toll design approach for dynamic traffic networks
Dusica Joksimovic, 2007, Delft University of Technology, the Netherlands.
15. Intertwining uncertainty analysis and decision-making about drinking water infrastructure
Machtelt Meijer, 2007, Delft University of Technology, the Netherlands.
16. The new EU approach to sector regulation in the network infrastructure industries
Richard Cawley, 2007, Delft University of Technology, the Netherlands.
17. A functional legal design for reliable electricity supply, How technology affects law
Hamilcar Knops, 2008, Delft University of Technology, the Netherlands and Leiden University, the Netherlands.

18. Improving real-time train dispatching: models, algorithms and applications
Andrea D'Ariano, 2008, Delft University of Technology, the Netherlands.
19. Exploratory modeling and analysis: A promising method to deal with deep uncertainty
Datu Buyung Agusdinata, 2008, Delft University of Technology, the Netherlands.
20. Characterization of complex networks: application to robustness analysis
Almerima Jamaković, 2008, Delft University of Technology, Delft, the Netherlands.
21. Shedding light on the black hole, The roll-out of broadband access networks by private operators
Marieke Fijnvandraat, 2008, Delft University of Technology, Delft, the Netherlands.
22. On stackelberg and inverse stackelberg games & their applications in the optimal toll design problem, the energy markets liberalization problem, and in the theory of incentives
Kateřina Staňková, 2009, Delft University of Technology, Delft, the Netherlands.
23. On the conceptual design of large-scale process & energy infrastructure systems: integrating flexibility, reliability, availability, maintainability and economics (FRAME) performance metrics
Austine Ajah, 2009, Delft University of Technology, Delft, the Netherlands.
24. Comprehensive models for security analysis of critical infrastructure as complex systems
Fei Xue, 2009, Politecnico di Torino, Torino, Italy.
25. Towards a single European electricity market, A structured approach for regulatory mode decision-making
Hanneke de Jong, 2009, Delft University of Technology, the Netherlands.
26. Co-evolutionary process for modeling large scale socio-technical systems evolution
Igor Nikolić, 2009, Delft University of Technology, the Netherlands.
27. Regulation in splendid isolation: A framework to promote effective and efficient performance of the electricity industry in small isolated monopoly systems
Steven Martina, 2009, Delft University of Technology, the Netherlands.
28. Reliability-based dynamic network design with stochastic networks
Hao Li, 2009, Delft University of Technology, the Netherlands.
29. Competing public values
Bauke Steenhuisen, 2009, Delft University of Technology, the Netherlands.
30. Innovative contracting practices in the road sector: cross-national lessons in dealing with opportunistic behaviour
Mónica Altamirano, 2009, Delft University of Technology, the Netherlands.
31. Reliability in urban public transport network assessment and design
Shahram Tahmasseby, 2009, Delft University of Technology, the Netherlands.
32. Capturing socio-technical systems with agent-based modelling
Koen van Dam, 2009, Delft University of Technology, the Netherlands.
33. Road incidents and network dynamics, Effects on driving behaviour and traffic congestion
Victor Knoop, 2009, Delft University of Technology, the Netherlands.
34. Governing mobile service innovation in co-evolving value networks
Mark de Reuver, 2009, Delft University of Technology, the Netherlands.
35. Modelling risk control measures in railways
Jaap van den Top, 2009, Delft University of Technology, the Netherlands.

36. Smart heat and power: Utilizing the flexibility of micro cogeneration
Michiel Houwing, 2010, Delft University of Technology, the Netherlands.
37. Architecture-driven integration of modeling languages for the design of software-intensive systems
Michel dos Santos Soares, 2010, Delft University of Technology, the Netherlands.
38. Modernization of electricity networks: Exploring the interrelations between institutions and technology
Martijn Jonker, 2010, Delft University of Technology, the Netherlands.
39. Experiencing complexity: A gaming approach for understanding infrastructure
Geertje Bekebrede, 2010, Delft University of Technology, the Netherlands.
40. Epidemics in Networks: Modeling, Optimization and Security Games. Technology
Jasmina Omić, 2010, Delft University of Technology, the Netherlands.
41. Designing Robust Road Networks: A general method applied to the Netherlands
Maaïke Snelder, 2010, Delft University of Technology, the Netherlands.
42. Simulations of Energy Transitions
Emile Chappin, 2011, Delft University of Technology, the Netherlands.

43. De ingeslagen weg. Een dynamisch onderzoek naar de dynamiek van de uitbesteding van onderhoud in de civiele infrastructuur .
Rob Schoenmaker, 2011, Delft University of Technology, the Netherlands
44. Safety Management and Risk Modelling in Aviation: the challenge of quantifying management influences.
Pei-Hui Lin, 2011, Delft University of Technology, the Netherlands.
45. Transportation modelling for large-scale evacuations
Adam J. Pel, 2011, Delft University of Technology, Delft
46. Clearing the road for ISA Implementation?: Applying Adaptive Policymaking for the Implementation of Intelligent Speed Adaptation
Jan-Willem van der Pas, 2011, Delft University of Technology, the Netherlands
47. Designing multinational electricity balancing markets.
Reinier van der Veen, 2012, Delft University of Technology, the Netherlands
48. Understanding socio-technical change. A system-network-agent approach.
Catherine Chiong Meza, 2012, Delft University of Technology, the Netherlands
49. National design and multi-national integration of balancing markets.
Alireza Abbasy, 2012, Delft University of Technology, the Netherlands
50. Regulation of gas infrastructure expansion.
Jeroen de Joode, 2012, Delft University of Technology, the Netherlands
51. Governance Structures of Free/Open Source Software Development. Examining the role of modular product design as a governance mechanism in the FreeBSD Project.
George Dafermos, 2012, Delft University of Technology, the Netherlands
52. Making Sense of Open Data – From Raw Data to Actionable Insight. Chris Davis, 2012, Delft University of Technology, the Netherlands
53. Intermodal Barge Transport: Network Design, Nodes and Competitiveness. Rob Konings, 2009, Delft University of Technology, Trail Research School, the Netherlands
54. Handling Disruptions in Supply Chains: An integrated Framework and an Agent-based Model. Behzad Behdani, 2013, Delft University of Technology, the Netherlands
55. Images of cooperation; a methodological exploration in energy networks. Andreas Ligtvoet, 2013, Delft University of Technology, the Netherlands

56. Robustness and Optimization of Complex Networks: Spectral analysis, Modeling and Algorithms, Dajie Liu, 2013, Delft University of Technology, The Netherlands
57. Wegen door Brussel: Staatssteun en publieke belangen in de vervoersector, Nienke Saanen, 2013, Delft University of Technology, The Netherlands
58. The Flexible Port, Poonam Taneja, 2013, Delft University of Technology, The Netherlands
59. Transit-Oriented Development in China; How can it be planned in complex urban systems?, Rui Mu, 2013, Delft University of Technology, The Netherlands
60. Cross Culture Work; Practices of collaboration in the Panama Canal Expansion Program, Karen Smits, 2013, University Amsterdam, The Netherlands
61. Structuring Socio-technical Complexity; Modelling Agent Systems Using Institutional Analysis, Amineh Ghorbani, 2013, Delft University of Technology, The Netherlands
62. Towards Playful Organizations; How online gamers organize themselves (and what other organizations can learn from them), Harald Warmelink, 2013, Delft University of Technology, The Netherlands
63. Electricity without borders; The need for cross-border transmission, Carlo Brancucci Martinez-Anido, 2013.....
64. The Power of Electric Vehicles; Exploring the Value of Flexible Electricity Demand in a Multi-actor Context, Remco Verzijlbergh, 2013, Delft University of Technology, The Netherlands
65. The impact of the policy mix on service innovation. The formative and growth phases of the sectoral innovation system for Internet video services in the Netherlands, Martijn Poel, 2013, Delft University of Technology, The Netherlands.
66. Acceptance-by-Design; Elicitation of Social Requirements for Intelligent Infrastructures, Layla AlAbdulkarim, 2013, Delft University of Technology, The Netherlands.
67. 'Publieksvriendelijk' versnellen van innovatie in netwerksectoren. Een exploratie van wetstechnische mogelijkheden ter bevordering van innovatie in de telecomsector, met behoud van de bescherming van publieke belangen, Lesley Broos, 2014, University of Twente, The Netherlands.
68. Spectrum Trading in the United Kingdom: Considering Market-Based Liberalization from Two Perspectives, Rajen Akalu, 2014, Delft University of Technology, The Netherlands.
69. Platform Dilemmas: Collective Action and the Internet of Things, Fatemeh Nikayin, 2014, Delft University of Technology, The Netherlands.
70. Scripting Transitions: A framework to analyse structural changes in socio-technical systems, Anish Patil, 2014, Delft University of Technology, The Netherlands.
71. Eco-transformation of industrial parks in China, Chang Yu, 2014, Delft University of Technology, The Netherlands.
72. Market-based support schemes for renewable energy sources, Riccardo Fagiani, 2014, Delft University of Technology, The Netherlands.
73. Strategic Behavior in the Liberalized Electricity Sector: Game Theoretical Formal Modeling in Policy Analysis, Sertaç Oruç, 2014, Delft University of Technology, The Netherlands.

74. European short-term electricity market designs under high penetration of wind power, José Pablo Chaves Ávila. 2014, Delft University of Technology, The Netherlands.
75. The Princess in the Castle: Challenging Serious Game Play for Integrated Policy Analysis and Planning, Qiqi Zhou, 2014, Delft University of Technology, The Netherlands.
76. Fostering Climate Resilient Electricity Infrastructures, Lynn Andrew Bollinger, 2014, Delft University of Technology, The Netherlands.
77. Reconfiguration of electricity distribution grids with distributed energy resources, Parvathy Chittur Ramaswamy, 2015, University of Ghent, Belgium.
78. Serving the Poor: Designing a Mobile Service Platform for Smallholder Farmer Inclusion in Global Value Chains, Tina George Karippacheril, 2015, Delft University of Technology, The Netherlands.
79. Cybersecurity via Intermediaries: Analyzing Security Measurements to Understand Intermediary Incentives and the Implications for Policy Making, Hadi Asghari, 2016, Delft University of Technology, The Netherlands
80. Response Arenas. A comparative study of multidisciplinary emergency management in virtual reality exercises, Theo van Ruijven, 2016, Delft University of Technology, The Netherlands.
81. Large-scale copyright enforcement and human rights safeguards in online markets: A comparative study of 22 sanctioning mechanisms from eight enforcement strategies in six countries between 2004 and 2014, Floris Kreiken, 2017, Delft University of Technology, The Netherlands.