Going dark? Analysing the impact of end-to-end encryption on the outcome of Dutch criminal court cases

Hartel, Pieter; van Wegberg, Rolf

DOI
10.1186/s40163-023-00185-4

Publication date
2023

Document Version
Final published version

Published in
Crime Science

Crime Science

RESEARCH

Open Access

Going dark? Analysing the impact of end-to-end encryption on the outcome of Dutch criminal court cases

Pieter Hartel*† and Rolf van Wegberg†

Abstract

Law enforcement agencies struggle with criminals using end-to-end encryption (E2EE). A recent policy paper states: "while encryption is vital and privacy and cyber security must be protected, that should not come at the expense of wholly precluding law enforcement". The main argument is that E2EE hampers attribution and prosecution of criminals who rely on encrypted communication - ranging from drug syndicates to child sexual abuse material (CSAM) platforms. This statement - in policy circles dubbed 'going dark' - is not yet supported by empirical evidence. That is why, in our work, we analyse public court data from the Netherlands to show to what extent law enforcement agencies and the public prosecution service are impacted by the use of E2EE in bringing cases to court and their outcome. Our results show that in cases brought to court, the Dutch courts appear to be as successful in convicting offenders who rely on E2EE as those who do not. Our data do not permit us to draw conclusions on the effect of E2EE on criminal investigations.

Keywords End-to-End Encryption (E2EE), PGP, WhatsApp, Serious crime, Law enforcement

Introduction

Mobile phones meet one of the most basic human needs: the ability to communicate. But drug dealers and their customers also love their phones because they no longer have to meet in a dark alley to avoid the police.

End-to-end encryption (E2EE) is a system that, amongst others, allows mobile phone users to communicate with each other without anyone else eavesdropping. So, the police cannot listen in either, even if they are authorized to tap the communication. PGP was the first widely used implementation of E2EE (Zimmermann, 1996), and WhatsApp has been offering E2EE since April 2016 to over a billion users (Menezes & Stebil, 2021). PGP has helped human rights organizations and journalists to communicate in hostile environments. PGP has probably saved hundreds of lives in the Kosovo theatre Letters to Phil Zimmermann from human rights groups. But offenders use PGP phones (O'Rourke, 2020) to defeat lawful interception. A PGP phone is a relatively expensive product on which not only PGP is installed, but from which also all non-essential hard and software have been removed (Europol, 2020).

The content of the communication may be encrypted, but the location of the phones is not. Every PGP phone has a regular phone number and uses the same mobile phone network as all other mobile phones. Suppose PGP phone A sends a message to PGP phone B. Then the encrypted message first goes to a cell tower near A, then via the network of the Telco to a cell tower near B, and finally from the cell tower to B. The police can locate a PGP phone by asking the provider when and with which cell towers the phone was in contact. Location

†Pieter Hartel and Rolf van Wegberg have contributed equally to this work

*Correspondence:
Pieter Hartel
pieter.hartel@tudelft.nl
Delft University of Technology, Delft, The Netherlands

information has been successfully used in several lawsuits to breach the anonymity of PGP phone users. For example, a court judgment describes how cell tower data proved that the telephones of an offender and his co-offender travelled together from Eindhoven to Amsterdam, where both were stopped during a traffic control ECLI:NL:RBAMS:2016:2835. Law enforcement has other special powers to bring offenders to justice that we will discuss below.

E2EE only works properly if it is correctly implemented in a trustworthy execution environment and if the private keys remain secret. However, this is more easily said than done.

In recent law enforcement operations against *criminal service providers* such as Phantom Secure, IronChat, Ennetcom, EncroChat, and Sky ECC, the police have managed to obtain messages - e.g., by infiltration - whereas the companies claimed that this should be impossible. The police were legally allowed to take action against these criminal service providers since there was a well-founded suspicion that these companies provided services to criminals. For example, Phantom Secure was a Canadian company that was infiltrated by FBI employees in 2018. Recorded conversations with the Phantom Secure CEO led to a valid allegation that the company's modified Blackberry phones were used for drug trafficking (Europol, 2020). Offenders not only use PGP, but they also use WhatsApp. For example: "The fact that the offender sold these drugs came to light after four young adults became unwell from drugs they had bought after WhatsApp contact with a dealer" ECLI:NL:RBNNE:2018:5197.

Offenders use PGP and WhatsApp for different reasons. WhatsApp is a success because almost all the people you want to communicate with are already using it - i.e., the network effect. WhatsApp is easy to use, free and even ad-free. PGP phones on the other hand, are an expensive niche product. The users buy such a device because the confidentiality of the messages they exchange with it is of vital importance to them. Specialised companies sell PGP phones and service subscriptions at premium prices. Offenders might use WhatsApp to communicate with victims, but they might use a PGP-phone to communicate with co-offenders.

In the Netherlands, several Ennetcom court cases have now been concluded, and some of the court judgments have been made public as open data. To gain insight into the impact of E2EE on the outcome of Dutch criminal court cases, we will analyse these and other relevant court judgments. We would have liked to investigate also the effect of E2EE on police investigations but unfortunately the required data are not available to researchers. Our results should therefore be taken as a contribution to the discussion on the ramification of E2EE on criminality.

Background and research questions

In the Netherlands, law enforcement has a wide range of special powers at their disposal, as described in Article 126 of the Code of Criminal Procedure. The application of these powers is subject to strict rules. In particular, special powers may only be used for serious offences, and permission from the examining magistrate is required. It should also be possible to check afterwards whether the powers have been used correctly. These checks and balances are in place to ensure a fair trial.

Technical special powers that are often used in investigations where the offender tries to evade detection through technology are (1) reading out and analysing confiscated smartphones, (2) placing telephone or Internet taps, (3) obtaining cell tower data from a Telco to trace the location of a mobile phone, and (4) hacking the computer or another device of the offender. There are other special powers, such as a subpoena for financial data, systematic observation, and systematic gathering of information, but we will not consider these here since they are not specifically designed to deal with technology such as E2EE. We will describe in more detail below two often-used special powers that on the one hand suffer from encryption, but on the other hand provide useful data.

Phone data

Most modern devices have encryption turned on by default. This means, that data on seized devices can only be read out if the device owner supplies the passcode. Law enforcement has several options to obtain phone data.

- The owner may surrender the passcode to the police. This should not be done under duress because, in most countries, the offender should not be obliged to cooperate with his conviction (nemo tenetur) (O'Rourke, 2020).
- In some countries, the police may force one to provide a fingerprint to unlock a smartphone (Europol, 2020).
- In some cases, special tools can bypass the passcode. For example, to crack the San Bernardino terrorist's iPhone 5C, the FBI had to pay more than $ 1 M to a specialist company (Cate et al., 2018).
- With the permission of the examining magistrate, the police may install key logger malware on a smartphone. The key logger reports the passcode without the suspect knowing (Brown, 2020).

Server data

Lawful interception allows authorised law enforcement agencies to obtain communication network data from individual subscribers. The signalling and network management information will be clear text, for example, IP addresses. The contents of the data can be encrypted, for example, when HTTPS or E2EE is used. In almost all implementations of E2EE, devices communicate with each other through a server. Law enforcement has several options to obtain server data:

- If the server contains a bug, an exploit can be used to tap the communication. This has happened to Whats App.
- If the administrators of the server make mistakes, the server can be hacked. This has happened to Encro Chat.
- If the administrators of the server are issued a subpoena by the court to hand over data from specific customers, they will have to comply. This has happened to HushMail.
- If law enforcement can pose as a reseller of handsets, they can insert a backdoor into the handset before delivering them to the customer. This has allegedly happened to Sky ECC.
- The police can also take the servers down and arrest the owners. This has happened to Phantom secure.

Research questions

The law ensures that an offender is only convicted if all evidence is legally obtained and conclusive. Suppose, that the content of a message from an offender is encrypted. The court may still be able to see to whom the offender has sent the message, but the court does not learn the content of the message. Then, the message could be legal evidence, but the court will probably deem it inconclusive. Also, assume that there is no other evidence, just the encrypted message. Then, all cases where the offender has used E2EE will lack conclusive evidence and are either not brought to court or are acquitted by the court. This is a hypothetical situation, as there may be enough other evidence to convict the offender, for example, location data. It does not matter whether the offender has used a PGP phone or WhatsApp, because in both cases, the phone must communicate regularly with a cell tower. The Telco therefore knows the location of the phone in question. And, with the location data obtained from the Telco, the court may decide that the evidence is conclusive. Because E2EE may reduce the number of options that law enforcement has to collect legal and convincing evidence, our first research question is: *To what extent does law enforcement use its special powers when offenders resort to E2EE? (RQ1)*

Cases for which the police cannot obtain sufficient evidence are normally not tried in court. We have made inquiries at the Netherlands Forensic Institute, but unfortunately, no public data or statistics are available on these types of cases. Our analysis is, therefore, limited to cases brought to the courts. Because acquittal can be a consequence of the use of E2EE, our second research question is: *To what extent are offenders using E2EE acquitted? (RQ2)*

A court judgment is a decision about the offender. However, a judgment also contains information about other persons involved in an investigation, such as co-offenders but also unknown persons with a criminal role. If unknown persons appear more often in E2EE investigations, this could be an indication that E2EE hinders the work of the police. We will investigate this by reviewing the PGP judgments for the relationship between the offender and unknown persons. For example: "The suspect always received the orders from the same client. The suspect received the orders on his Samsung phone on which an Ironchat program was installed." ECLI:NL:RBOVE:2019:4844. In this judgment, the offender was convicted, but the unknown person remained at large because the communication was via a PGP telephone. Suppose that the police could have used data for this case from seized Iron chat servers. Then perhaps the PGP phone would not have been an obstacle to the investigation. With data requisitioned from criminal service providers, the police have a powerful weapon in their hands against abuse of E2EE. We therefore pose as a third research question: *To what extent do unknown persons occur in investigations using data from criminal service providers. (RQ3)*

Method

In six years (2015–2020), the Dutch district courts published 25366 anonymized court judgments on rechtspraak.nl. This represents about 5% of the total number of court judgments in that period. The courts publish all judgments with a crime against life, where the maximum sentence is at least four years, or when the court expects interest from the public. Therefore, judgments of the most serious crimes are likely to be included in the published data set.

Offenders and the police are engaged in an on-going battle. As soon as one wins, the other tries to nullify that lead. E2EE gives the offender a head start, and the question is to what extent the special powers of the police can cope. We will therefore construct a comparison group of judgments in which the police used their special powers, but in which the offender did not use

E2EE. These judgments form a baseline for judgments in which the offender *has* used E2EE.

To answer RQ1, we will compare the use of special powers in the group of judgments where the offender has used E2EE to the comparison group. To answer RQ2, we will compare the conviction rates of the group of WhatsApp users, the group of PGP users and the comparison group. To analyse the court judgments, we define three variables as follows:

- The first variable *special power* encodes the technical special powers used by law enforcement in reaction to the offender using E2EE.
- The second variable *decision* encodes whether the offender is convicted or acquitted.
- The third variable *technology* encodes whether the offender used PGP, WhatsApp, or neither (comparison). A judgment with both WhatsApp and PGP is considered a PGP judgment; the three groups are therefore independent.

To answer RQ3, we will identify judgments stating whether law enforcement obtained relevant data from a criminal service provider and whether there were unknown persons in a criminal role. The unit of assessment for RQ3 is the investigation, not the judgment as for RQ1 and RQ2. Investigations have a unique name that is usually mentioned in the judgments. To analyse the investigations, we define two variables: *criminal service provider data* and *unknown persons*. The first variable encodes whether or not law enforcement has had access to criminal service provider data. There are two possibilities:

- Server data have been obtained from criminal service providers, such as Ennetcom, EncroChat, PGP-safe, Sky-ECC, and IronChat, or from police operations Onymous and Bayonet.
- The PGP phone of the offender has been read out or his PGP keys were seized.

The second variable, *unknown persons*, encodes whether or not unknown persons played a criminal role in the investigation. This can be stated in many ways, for example: "The offender is a career criminal of the worst kind who lives in circles where liquidation orders are given and received" ECLI:NL:RBAMS:2017:5136. We have also looked for judgments stating that the case against one of the co-offenders has been dropped. However, this does not occur in the PGP judgments.

Descriptive statistics

A total of 6,619 relevant court judgments were available for analysis. This is about 1.5% of the total number of criminal judgments processed by the Dutch district courts in the given 6-year period. In 439 judgments PGP was used, WhatsApp was used in 2,390 judgments, and the comparison group consists of 3,790 judgments. The groups are unbalanced, which weakens some of the statistical analysis. We sampled 20% of the WhatsApp group and 12% of the comparison group (both uniform and at random). This gave us a WhatsApp group of 437 judgments and a comparison group of 469 judgments, in total N=1,345.

Of the 1,345 judgments, 25.5% were drugs-related, and 26.6% were violence-related. These percentages are higher than the national averages of 9.7% and 9.2% respectively (Meijer et al., 2021, Table 6.2 and 6.12) because the courts mainly publish judgments of serious crimes.

The offender is female in 7.9% of judgments. The average age of the offender at the time of the court judgment is 36.2 (SD = 12.5) years. Of the offenders, 37.9% are first-time offenders, and 31.5% are repeat offenders. These demographics are consistent with the demographics of the whole population of Dutch criminal offenders convicted for serious crime (Wingerden et al., 2016).

Of the 1,345 judgments, 80.0% have resulted in incarceration, including involuntary commitment, imprisonment, and military detention. The average length of incarceration is 42.7 (SD = 50.0) months, which is more than 10 times the national average of 4 months (Meijer et al., 2021), [Table 6.11], again because of the focus on serious crime. Community service represents 5.2%, acquittal 6.3%, and a fine 3.0%. The remaining 4.7% of the judgments are procedural, such as an extradition request.

The police have used their technical special powers as follows: In 68.0% of judgments, a phone or Internet connection was tapped (offenders with a PGP-phone may also have a regular phone). In 26.9% of judgments, a seized mobile phone was read out. In 10.9% of judgments, a phone was located by requesting cell tower data. The Dutch police have hacked into the offender's systems eight times in 2019, just after passing the relevant law that made this possible. However, none of those judgments are public (yet), so that we have no data on police hacks.

The 439 PGP judgments are the result of 196 criminal investigations. In the majority of these (83.3%), law enforcement used server or phone data from criminal service providers.

Results

Table 1 tabulates the crime rates for the main offence types defined by Statistics Netherlands cbs.nl. *Other criminal offence* includes offences not covered by any of the other categories, for example, road traffic offences, and environmental crime. Sometimes procedural judgments are not tied to a specific offence, for instance, extraditions. The "Other" column also accounts for these procedural judgments. An offender may commit more than one crime, but we have counted only the offence with the most severe maximum sentence. A χ^2 test of association between *technology* and *offence type* was found to be statistically significant (see caption). This means, that the difference in crime rates between the three groups is unlikely to exist due to chance. For example, offenders using WhatsApp commit mostly violent crime (41.6%), whereas PGP offenders mostly commit drugs-related offences (53.1%).

Assuming that the police will use their special powers for each type of crime, we would expect that the distribution of crimes in the comparison group corresponds to the distribution of published serious crimes. The last row in table 1, taken from our previous work (Hartel et al., 2022), shows that the correspondence is indeed reasonable.

Table 2 shows the relationship between the variables *technology* and *special power*. The police prefer the tap (47.3%) to reading out phones (22.2%) and gathering cell tower data (10.9%). By the construction of the comparison group, special powers were used in all comparison judgments. A χ^2 test of association between *technology* and *special power* was found to be statistically significant (see caption). This means, that the difference in the use of special powers between the three groups is unlikely to exist due to chance. For example, the police use special powers more for PGP (100−19.8=80.2%) than for WhatsApp (100−40.5=59.5%) judgments.

Table 1 Contingency table of court judgments using specific *technology* (left) versus *offence type* (top) ($\chi^2(10) = 350.48, p < 0.001$, Cramer's V= 0.36, $p < 0.001, \alpha = 0.01$). Boldface percentages are discussed in the text

Judgments	Property Offence	Violent Offence	Public order Offence	Drug Offence	Weapon Offence	Other Offence	Total	
							Row	Column (%)
WhatsApp	119	182	39	41	11	45	437	
	27.2%	**41.6%**	8.9%	9.4%	2.5%	10.3%	100%	32.5
PGP	30	60	50	233	12	54	439	
	6.8%	13.7%	11.4%	**53.1%**	2.7%	12.3%	100%	32.6
Comparison	122	116	41	69	12	109	469	
	26.0%	24.7%	8.7%	14.7%	2.6%	23.2%	100%	34.9
Total	271	358	130	343	35	208	1,345	
	20.1%	26.6%	9.7%	25.5%	2.6%	15.5%	100.0%	100.0
Hartel et al. (2022)	27.9%	31.6%	9.7%	12.1%	3.1%	15.6%		

Table 2 Contingency table of court judgments using specific *technology* (left) versus *special power* used by law enforcement (top) ($\chi^2(6) = 336.31, p < 0.001$, Cramer's V= 0.35, $p < 0.001, \alpha = 0.01$, and for the table without the first column with a zero cell count: $\chi^2(4) = 94.73, p < 0.001$, Cramer's V= 0.30, $p < 0.001, \alpha = 0.01$). Boldface percentages are discussed in the text

Judgments	No Special Power	Tapped Only	Readout w/ or w/o Tapped	Located w/ or w/o Tapped, readout	Total	
					Row	Column (%)
WhatsApp	177	153	85	22	437	
	40.5%	35.0%	19.5%	5.0%	100.0%	32.5
PGP	87	145	123	84	439	
	19.8%	33.0%	28.0%	19.1%	100.0%	32.6
Comparison	0	338	91	40	469	
	0.0%	72.1%	19.4%	8.5%	100.0%	34.9
Total	264	636	299	146	1,345	
	19.6%	**47.3%**	**22.2%**	**10.9%**	100.0%	100.0

Table 3 shows the relationship between the variables *technology* and *decision*. To focus on the differences between conviction and acquittal, we have omitted the procedural judgments; hence the total number is 1,282 instead of 1,345. In all three groups, the vast majority of offenders is convicted. A χ^2 test of association did not reveal a significant difference between the conviction rates of the three groups (see caption). This means, that there is no evidence in our data that the outcome of a trial depends on whether the offender used PGP, WhatsApp or neither.

Table 4 shows the relationship between the variables *criminal service provider data* and *unknown persons*. The 439 judgments constitute 196 investigations. In 36.7% of the investigations, criminal service provider data were used, and in 61.2% unknown persons were involved. A χ^2 test showed that there is no significant relationship between the variables. This means, that there is no evidence in our data that the availability of criminal service provider data influence the number of investigations with unknown persons.

Table 3 Contingency table of court judgments using specific *technology* (left) versus *decision* (top) ($\chi^2(2) = 3.09, p = 0.213$, Cramer's V=0.05, $p = 0.21, \alpha = 0.01$)

Judgments	Convicted	Acquitted	Total	
			Row	Column (%)
WhatsApp	405	22	427	
	94.8%	5.2%	100.0%	33.3
PGP	397	28	425	
	93.4%	6.6%	100.0%	33.2
Comparison	395	35	430	
	91.9%	8.1%	100.0%	33.5
Total	1,197	85	1,282	
	93.4%	6.6%	100.0%	100.0

Discussion

Research questions

The answer to RQ1 is that law enforcement uses more special powers in cases where offenders use PGP than where they use WhatsApp. This is to be expected, as E2EE encrypts the communication so that telephone and Internet taps are no longer useful. This makes the remaining special powers more important. This also places a burden on law enforcement and ultimately on the taxpayer. However, law enforcement does not use all its special powers, and it does not use special powers for all investigations either. This means that, in principle, some of the special powers are still unused in E2EE cases. Whether these available powers would have been effective cannot be deduced from the data.

The answer to RQ2 is that there is no evidence in our dataset that the conviction rate of offenders who use EE2E differs from the conviction rate of offenders who do not use EE2E. This means, that our data show no evidence that the outcome of court decisions is influenced by E2EE. Apparently, the strength of the evidence is not affected by E2EE use. This is explainable because there is usually more evidence available than the court needs for the conviction (Peterson et al., 2013).

The answer to RQ3 is that the data available to us show no difference in the extent to which unknown persons are criminally involved in investigations with, or without, data from criminal service providers. On the one hand, law enforcement has made frequent use of data from criminal services providers (Soudijn et al.,2022) in investigations where individuals have remained unknown. This is an indication that the police have pulled out all the stops to bring these unknown persons to court. On the other hand, the differences in the frequencies of Table 4 are not statistically significant. Hence, the differences between investigations with and without unknown persons could also be due to chance. The court judgments show that the courts are not affected by E2EE. Unfortunately, court judgments contain too little information to

Table 4 Contingency table of investigations using specific *criminal service provider data* (left) versus the criminal involvement of *unknown persons* (top) ($\chi^2(1) = 4.426, p = 0.035$, Cramer's V= 0.15, $p < 0.001, \alpha = 0.01$). Boldface percentages are discussed in the text

Investigation	No unknown	With unknown	Total	
	Persons	Persons	Row	Column (%)
Without data from	55	69	124	
Criminal service providers	44.4%	55.6%	100.0%	63.3
With data from	21	51	72	
Criminal service providers	29.2%	70.8%	100.0%	**36.7**
Total	76	120	196	
	38.8%	**61.2%**	100.0%	100.0

draw a conclusion about the influence of E2EE on the criminal investigation.

Public-policy debate

We provide some observations as a contribution to the public-policy debate (Hewson & Harrison, 2021). Some courts seem to hint towards legislative action against criminal use of E2EE, as evidenced by phrases from court judgments such as: "This crypto phone belongs to the accused and is of such a nature that its uncontrolled possession is contrary to the law or the public interest." ECLI:NL:RBZWB:2020:1216. What the courts have probably not considered is whether controlling possession is feasible. If the legislator restricts the use of EE2E, the authorities would have to verify that all service providers duly implement the restrictions. We think that this would be a heavier burden on governments (and on the taxpayer) than the status quo.

Next to the burden of additional police costs to work around E2EE, there are other interests too (Veen & Boeke, 2020). For example, national security agencies are unlikely to use backdoor encryption because of the risk of the key to the back door ending up in the wrong hands. And confidentiality is crucial for national security agencies. Also, the commercial use of E2EE with a back door would probably not be viable because of the risk that a competitor would get hold of the keys. This means, that many legitimate users of E2EE will find alternative means of secure communication that law enforcement will not be able to tap, thus aggravating the problem for law enforcement rather than ameliorating it.

If E2EE is weakened - or in essence, broken - by policies that demand a backdoor, a supra-national infrastructure is needed to manage those backdoors. Every nation-state will need to access backdoors to prosecute its nationals, including states on the EU sanctions list. We believe, that this is a recipe for disaster. Banning E2EE will simply force terrorists, drug dealers, and paedophile rings to use alternative technologies. Well-funded offenders are already starting to develop their own encryption platforms MPC. Initially, such tools will have issues, but over time they will get better and will create an obstacle to law enforcement.

Law enforcement currently does an excellent job of taking down criminal service providers like EncroChat. Recent law enforcement operations against these companies show that there are opportunities to monitor them and to act upon information that shows their involvement in illegal activity. Our recommendation is not to build a back door into every application of E2EE, but to keep a watchful eye on relevant, criminal service providers.

Limitations

The most important limitation is that we do not know when special powers have proven insufficient for law enforcement to build a case because such information is confidential. Instead, we have used acquittal by the courts as an indication of inconclusive evidence. The data we have used originate from the Dutch government and is not necessarily representative of other countries. The data also only represent about 1.5% of all criminal judgments in the Netherlands. Our analysis is focused on PGP and WhatsApp, as only nine judgments mention Signal and two mention Telegram (Albrecht et al., 2021). Signal and Telegram may not have been popular when the events described in the court cases occurred.

This paper does not seek to address the privacy vs security debate. It merely provides insight in how the courts are able to prosecute offenders who use E2EE in comparison to offenders who do not such technologies.

Conclusions

The criminal justice system is often described as a funnel that inputs orders of magnitude more crime reports than that it outputs convicted offenders (Felson & Eckert, 2019). Few crime reports lead to a police investigation, and even fewer investigations lead to a court case. The court judgments that we have been able to analyse make the convictions transparent but the rest of the funnel remains opaque. However, by searching for criminal roles played by unknown persons, we have tried to see beyond convictions, and into the investigations.

The information position of technology companies and governments today is superior to that of the nineties due to surveillance from online and offline sources. Encryption is one of the few technologies available to law-abiding citizens, corporations, and national security agencies that protect privacy. Yet, criminals (mis)use that same technology.

We have shown that the Dutch courts can do their work without legislation that breaks encryption. We cannot make a similar conclusion for law enforcement as our data are inconclusive on this point. One way to gain insight into this problem is by examining police files and interviewing police detectives. This we suggest as future work.

Acknowledgements

Conversations with Phil Zimmermann have been a great source of inspiration for this work. We thank Roel Wieringa and the anonymous reviewers for their comments on the paper.

Author contributions

Both authors read and approved the final manuscript.

Funding

No outside funding was used to support this work.

Availability of data and materials
The data that has been analysed is open data, available from https://www.rechtspraak.nl

Declarations

Ethics approval and consent to participate
The research complies with ethical standards because all data that has been analysed is open data that has been made public to be analysed.

Competing interests
The authors declare that they have no competing interests.

Received: 6 October 2022 Accepted: 23 February 2023
Published online: 06 March 2023

References

Albrecht, M.R., Blasco, J., Jensen, R.B., Mareková, L. (2021). Collective information security in large-scale urban protests: the case of hong kong. In: 30th USENIX Security Symposium, pp. 3363–3380. USENIX Association, Online. https://www.usenix.org/conference/usenixsecurity21/presentation/albrecht

Brown, S. D. (2020). Hacking for evidence: The risks and rewards of deploying malware in pursuit of justice. *ERA Forum: J. of the Academy of European Law, 20*, 423–438. https://doi.org/10.1007/s12027-019-00571-z

Cate, F. H., Boneh, D., Chang, F. R., Charney, S., Goldwasser, S., Hoffman, D. A., Kamara, S., Kris, D., Landau, S., Lipner, S. B., Littlehale, R., Martin, K., Rishikof, H., & Weinberger, P. J. (2018). *Decrypting the encryption debate: A framework for decision makers. Consensus study report*. Washinton DC: The National Academies Press.

Europol: Second report of the observatory function on encryption. Joint reports, EuroPol and EuroJust public information (Feb 2020). https://www.europol.europa.eu/publications-documents/second-report-of-observatory-function-encryption

Felson, M., & Eckert, M. (2019). *Crime and everyday Life* (6th ed.). Thousand Oaks, CA: Sage publishing.

Hartel, P., van Wegberg, R., & van Staalduinen, M. (2022). Investigating sentence severity with judicial open data: A case study on sentencing high-tech crime in the Dutch criminal justice system. *European Journal on Criminal Policy and Research Online first*. https://doi.org/10.1007/s10610-021-09503-5

Hewson, E. C., & Harrison, P. S. (2021). Talking in the dark: Rules to facilitate open debate about lawful access to strongly encrypted information. *Computer Law & Security Review, 40*(105526), 1–13. https://doi.org/10.1016/j.clsr.2020.105526

Meijer, R.F., Moolenaar, D.E.G., Choenni, S. & van den Braak, S.W. (2021). Criminaliteit en rechtshandhaving 2020 ontwikkelingen en samenhangen. Cahier 2021-22, Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC). https://repository.wodc.nl/handle/20.500.12832/254. Accessed 2 Mar 2023

Menezes, A., & Stebil, D. (2021). End-to-end security: When do we have it? *IEEE Security & Privacy, 19*(4), 60–64. https://doi.org/10.1109/MSEC.2021.3077403

O'Rourke, C. (2020). Is this the end for 'encro' phones? *Computer Fraud & Security, 2020*(11), 8–10. https://doi.org/10.1016/S1361-3723(20)30118-4

Peterson, J. L., Strom, K. J., & Johnson, D. J. (2013). Effect of forensic evidence on criminal justice case processing. *J. of forensic science, 58*(S1), 78–90. https://doi.org/10.1111/1556-4029.12020

Soudijn, M. R. J., Vermeulen, I. J., & van der Leest, W. P. E. (2022). When encryption fails: A glimpse behind the curtain of synthetic drug trafficking networks. *Global Crime, 23*(2), 216–239. https://doi.org/10.1080/17440572.2022.2086125

van Wingerden, S., van Wilsem, J., & Johnson, B. D. (2016). Offender's personal circumstances and punishment: Toward a more refined model for the explanation of sentencing disparities. *Justice Quarterly, 33*(1), 100–133. https://doi.org/10.1080/07418825.2014.902091

Veen, J., & Boeke, S. (2020). No backdoors: Investigating the Dutch standpoint on encryption. *Policy and Internet, 12*(4), 503–524. https://doi.org/10.1002/poi3.233

Zimmermann, P. R. (1996). *The official PGP user's guide*. Cambridge, MA: The MIT Press.

Publisher's Note