# Privacy in Financial Innovation: a Value Sensitive Design for PSD2

Jaimy van der Heijden

Master of Science Thesis

TU Delft

# Privacy in Financial Innovation:
# a Value Sensitive Design for PSD2

Draft master thesis submitted to Delft University of Technology in partial fulfilment of the requirements for the degree of MASTER OF SCIENCE in Management of Technology

by
**Jaimy van der Heijden**
Student number: 4333659

To be defended in public on September 7, 2017

Delft University of Technology
Technology, Policy and Management

| | |
|---|---|
| Chairman | Prof. Dr. M.J. van den Hoven<br>Ethics/Philosophy of Technology |
| First supervisor | Dr. F. Santoni De Sio<br>Ethics/Philosophy of Technology |
| Second supervisor | Dr. Z. Roosenboom-Kwee<br>Economics of Technology and Innovation |
| External supervisor | Drs. S.C. Wegener Sleeswijk<br>Head of Strategy & Development, NIBC Bank N.V. |

## Executive summary

The European Commission introduced PSD2 with the purpose to promote innovation by increasing competition and participation of non-banks in the payments industry. Amongst others, PSD2 requires banks to allow a way for third-party providers to have direct access to a current account's data if authorized by the customer. This forces banks to open up their databases which calls into life a particular stream of questions about how technologies should be designed in order to preserve privacy. Therefore this research was dedicated to designing a framework of general principles for the inclusion of privacy in innovation within the financial industry, in particular for the incumbent bank.

The Value Sensitive Design approach was utilized in order to provide this framework through a qualitative explorative case study. In the conceptualization stage of VSD, privacy was defined through a literature review. For the empirical investigation, data was collected through semi-structured interviews with eleven experts from three of the four types of stakeholders. Values that were identified in literature were qualitatively validated by scoring their importance relative to each other. For the technical investigation, the most important values were translated into design requirements by utilizing the value hierarchy method. The application of VSD to innovation in finance is the theoretical contribution of this research.

Privacy was conceptualized as complex and interrelated with other values. Values related to privacy in the case of PSD2 were also identified in several literature streams. Through a qualitative validation, the final set of values to be reflected by technology designed after PSD2 was determined which shows that privacy is the value of greatest importance to be included in financial innovation. Also, based on the insights experts brought forward during the interviews, five ethical challenges that come with the implementation of PSD2 were identified. The applicability of the value hierarchy method was demonstrated by translating the value privacy into six design requirements. These six design requirements addressed the end-user's ability to make an informed decision for consent, ex-ante privacy assessment through standardized licensing procedures and a shared license database, the possibility for end-users to manage information disclosed through APIs and the limitation of information referring to transaction's counterpart that did not consent.

Further studies should conduct research on the values as held by the public at large towards PSD2 as this research might be biased by solely relying on expert opinions. Also, the implications of the final guidelines as recently published by the EBA on the conclusions of this thesis should be researched. Lastly, further research should be conducted into the practical applicability of the recommend design requirements.

## Acknowledgement

This thesis is the product of many constructive influences. Therefore, certain people deserve my gratitude. First of all, I would like to thank NIBC Bank, and in particular Drs. S.W. Wegener Sleeswijk, for providing me with the opportunity and resources that made this research possible. I would like to thank my graduation committee; first supervisor Dr. F. Santoni De Sio for the elaborate feedback on a regular basis, second supervisor Dr. Z. Roosenboom-Kwee for the helpful suggestions and chair Prof. Dr. M.J. van den Hoven for the flexible and professional guidance. Also, as this research benefitted from the willingness of experts to share their valuable insights, I want to express my gratitude to them who dedicated some of their scarce time to this research. And last, but certainly not least, many thanks to my family and friends who offered me their listing ear, opinions and necessary distraction.

# Table of Contents

## List of acronyms

Because the legislation that is subject in this thesis is rich of acronyms, Table 1 provides a holistic overview along with a short description.

**Table 1: list of acronyms and abbreviations**

| Abbreviation | | Short description |
|---|---|---|
| **AP** | Authoriteit Persoonsgegevens | Dutch national data protection authority |
| **ACM** | Netherlands Authority for Consumers and Markets | Ensures fair competition between businesses, and protects consumer interests. |
| **AFM** | Authoriteit Financiële Markten | Dutch Authority for the Financial Markets |
| **AIS** | Account Information Service | |
| **AISP** | Account Information Services Provider | |
| **ASPSP** | Account Servicing Payment Services Provider | Incumbent banks offering current accounts |
| **CSC** | common and secure open standards of communication | |
| **DPD** | Data protection directive 95/46/EC (European Commission 1995) | |
| **DNB** | De Nederlansche Bank | Dutch national bank, part of the European System of Central Banks |
| **DPD** | Data Protection Directive | Directive 95/46/EC on processing and free movement of personal data |
| **EBA** | European Banking Authority | Authority for effective and consistent prudential regulation and supervision across the European banking sector. |
| **ECB** | European Central Bank | Responsible for safeguarding the value of the euro and maintaining price stability as well as the Single Supervisory Mechanism for banking supervision by. |
| **GDPR** | General Data Protection Regulation | Regulation (EU) 2016/679 to strengthen and unify data protection for individuals |
| **PAAS** | Payment Account Access Services | |
| **PISP** | Payment Initiation Services Provider | |
| **PIS** | Payment Initiation Services | |
| **PSP** | Payment Service Provider | |
| **PSD** | Payment Services Directive | |
| **TPP** | Third Party Provider | |

# 1. Introduction

Introducing the research topic, this chapter delineates the background of the topic, problem description, purpose of the study, research design and deliverables. This thesis was incentivized by the revised Payments Services Directive which the European Commission issued in order to encourage innovation in the European payments industry. However, with the introduction of PSD2, questions came into being regarding the implementation of this legislation without unwanted risks to privacy in digital spaces. Through the Value Sensitive Design methodology, which appears underexposed in the subject innovation in finance, this research will deliver a framework for the inclusion of values in innovation within the financial industry.

## 1.1. Problem background

Innovative payments are one of the emerging markets in the finance industry that potentially offer a huge benefit to the economy (Moody's Analytics, 2013). The European Commission recognizes this and made it part of the Europe 2020 strategy; the 10-year strategy for advancement of the European digital economy (European Commission, 2010). Part of the 2020 strategy was revising the Payment Services Directive. The primary purpose of the revised – or second – Payment Services Directive (PSD2) is to promote innovation by increasing competition and participation of non-banks in the payments industry and to provide a level playing field by harmonizing consumer protection and the rights and obligations for payment providers and users (European Commission, 2015).

The directive should be implemented in each member state's national legislation by January 2018 and fully complied with as of October 2018. Full compliance to the revised directive entails, amongst others, the obligation for banks to allow a way for customers to authorize a third-party provider to have direct access to two aspects of their bank account: their account transactional data and the ability to authorize payments directly from their account (Gimigliano, 2016). This is why the revised Directive on Payment Services is generally regarded as the single biggest change in the banking industry: it forces banks to open up their infrastructure to third parties introducing third-party providers as fellow keepers of personal financial data (PwC, 2016). As incumbent financial organizations have very limited prior experience regarding the consequences of such legislation and the technology it demands, the implementation of PSD2 raises several societal, technological and ethical questions. One particular stream of these questions is about preserving privacy in digital space with the effectuation of the innovation in finance that this legislation incentivizes.

Recent research has addressed privacy aspects of technology designed after PSD2 but this research is scattered, incomplete and questions remain unanswered (Reijers, 2016; Fuster, 2016). *Under which conditions will this legislation impact society as wished-for? How should the technologies be designed in order to promote the relevant values? In particular, how to implement this legislation without unwanted risks to*

*privacy in digital spaces?* A new stream of research focusses on responsible innovation within the financial industry providing a framework for addressing these questions (Halbac, 2015; Waagmeester, 2016). Also, the European Union is one of the leaders in supra-national governing regarding privacy legislation, making the revised Payments Services Directive a suited case for study (Heisenberg, 2005). Therefore this research will focus on Dutch incumbent financial organizations in the case of PSD2, in order to design a framework of general principles for the inclusion of values in innovation within the financial industry.

## 1.2.Problem description

The current Payment Services Directive was revised with the purpose of stimulating innovation in the financial industry by incentivizing non-banks to enter this market. By law, banks will be forced to give access to payment initiation and account information under the conditions of customer consent and the accessing party being licensed (European Commission, 2015). Because a payment reveals several different client preferences, personal financial data is considered highly sensitive. For new entrants to the market, this means that a valuable new source of data becomes available sprouting a vast amount of new business models based upon this type of data. However, besides promoting innovation, the implementation of PSD2 also raises ethical concerns (Gimigliano, 2016). Control over personal financial data shifts from incumbent banks with extensive experience in handling, maintaining and securing payment and data infrastructure, towards Third-Party Providers (TPPs) that have yet to prove themselves in this practice. These TPPs are expected to base their business models on the exchange of personal financial data for economic benefits and convenience. Examples such as Facebook and Google have proven that customers are willing make this trade in large quantities (Jordaan & Heerden, 2017). But, even though legislation is in place that addresses the etiquette for data, the way TPPs will develop their business models on personal financial data, as well as the role of incumbent banks (ASPSP) towards privacy remains subject to debate. This ambiguity is the result of conflicting values in society. Values of several economic, social, technical and moral origin influence the way a product or service is developed (Pesch, 2015). In the case of PSD2, values influence the way technology for the disclosing of financial data is developed.

On the one hand, the financial industry is characterized by strict legislation which is well monitored and enforced. This legislative climate restricts opportunities for novelty within the financial industry to ensure stability, safety and security (Waagmeester, 2016). On the other hand, the financial market now faces legislation that does not necessarily protect these values with the introduction of PSD2. While PSD2 does address aspects of security and privacy, it only does so to a limited extent in order to ensure technology neutrality (i.e. legislation not hampering future technological improvement) (Giambelluca & Masi, 2016). This is in line with the vision of Lee and Petts (2013) who regard legislation as a measure to control and supervise that only applies to upfront characterized risks. PSD2 thus contains other values than is usual for financial regulation. Therefore, PSD2 can be considered to contrast the status quo; incumbent financial

organizations are required to drastically redesign infrastructure with yet unknown consequences without providing a framework for preserving privacy sufficient for ASPSPs to rely on.

Because of its emergent nature, PSD2 leaves many implications unknown. One of those aspects is the chance on privacy related ethical challenges that surface during implementation. However, even though ethical challenges are unknown, PSD2 does require banks to develop certain technology before the effects of implementation in society become evident. As ethical challenges are caused by conflicting values, the values at conflict are unknown when ethical challenges are unknown (Owen, et al., 2013). The problem that incumbent financial organizations face is thus that they are forced to design, or have technology designed for them while the values that society holds towards the technology to be developed are unknown. While consciously taking into account ethical challenges within the innovation process can potentially lead to more adequately designed products (Waagmeester, 2016). Or, as van den Hoven & Weckert (2008) put it; the inclusion of values "can lead to more careful, adequate, and responsible design". By not only addressing functional requirements but also taking individual and social values into consideration, agents are better equipped to deal with potential ethical challenges (van den Hoven & Weckert, 2008). In the case of PSD2, examples of such challenges could be the conditions that provide for a certain impact of PSD2 on society, a design that faces a trade-off between relevant values or, in particular, avoiding risks to privacy while achieving the goals of the legislation.

Another rationale for the importance of addressing the above mentioned challenges is the social acceptance of products and services. The lack of ethical consideration in the innovation and design stage leads to rejection (van de Kaa, 2014). For new technologies to become accepted by society, they have to be aligned with societal needs and values (von Schomberg, 2011). In developing products, organizations need to consider existing standards and institutions, or try to influence them (Waagmeester, 2016). For financial institutions, especially retail banking, social acceptance is considered to be of importance because the capital brought in by consumer saving and current accounts funds the banks profitable lending activities etc. Social acceptance – or trust – is thus a desirable asset for a bank's revenue model. Ex-ante assessment for ethical privacy related challenges is therefore necessary.

Value-sensitive design (VSD) is an approach to guide engineering design processes "to prevent situations which are morally dilemmatic and which must inevitably lead to suboptimal solutions or compromises and trade-offs from a moral point of view" (van den Hoven, 2012). The focus of Value Sensitive Design is on "incorporating moral values into the design of technical artifacts and systems by looking at design from an ethical perspective" (van den Hoven, 2005). Van den Hoven *et al* (2012) propose that technology could be the solution rather than the source of moral tension by saying that "technological progress can create moral progress". They suggest that some moral trade-offs may have engineering solutions and that certain types of moral dilemma can be tackled by means of technological innovations. Despite that several researches have

addressed the application of VSD to innovation in finance, a framework for the inclusion of values in innovation for incumbent financial organizations is missing. The focus of the research is to address social and ethical issues related to privacy in the implementation of PSD2 by identifying the values at stake for incumbent financial organizations, prioritizing and translating the most important one in to design requirements.

## 1.3.Research objective

Through a brief literature review both practical and theoretical research gaps appear in literature. The framework of VSD is one that has been applied to many industries including the financial industry, proving its potential. The approach to include values at stake in order to reduce the chance on moral problems has been utilized for value Payment Value Added Services, platform based FinTech companies by social acceptance of smart meters and wind-energy applications (Halbac, 2015; Waagmeester, 2016; Kizhakenath, 2016; Taebi & Kadak, 2010). These previous studies on VSD in financial industries, however, have concentrated on subjects that are incomparable to this research. For example, platform based fin-tech companies that are characterized by maturity issues, resource scarcity and short time-to-market (Waagmeester, 2016). These are characteristics that bring different challenges than those that characterize the environment of incumbent banks –the unit of analysis for this research. A dedicated framework for including values in innovation in the European incumbent financial industry is thus missing.

The theoretical gap concerns the underexplored application of VSD in incumbent financial industry and the lack of an overview that links values as derived from literature to empirical values specific to the incumbent financial industry. The practical gap in literature concerns a body of generic principles for the inclusion of values during innovation in finance to PSD2. To reduce the chance of issues during the implementation of PSD2 in society, this research will therefore take inventory of the privacy related values at stake and translate those into generic principles for incumbent financial institutions to take into account when innovating after PSD2, providing a framework for the inclusion of values in financial innovation for incumbents. To provide this framework, first the value of privacy will be conceptualized as a complex and interrelated construct (Nissenbaum, 2004). The interrelatedness refers to values relating to privacy which are identified in several streams of literature. Thereafter, the priority of these values will be determined from interviews with experts on the subject of PSD2. Lastly, the method to translate values into design requirements is demonstrated by applying the value hierarchy method to the value determined to be of greatest importance.

The contribution of this thesis to the literature is twofold: Firstly, it identifies the values at stake in the case of PSD2 and connects those to values as given in certain streams of literature. Secondly, it contributes to the practical understanding of how VSD can be applied in incumbent financial organizations, specifically in response to the effectuation of PSD2 preventing a mismatch between industry practices and the public's interest.

## 1.4.Research questions

The main research question is derived from the problem statement as delineated before:

- **What general principles for the inclusion of values in innovation within incumbent financial organizations can be derived from the (privacy-related) values of stakeholders to optimize the anticipated effects of PSD2 on society?**

Sub-questions have been composed in order to answer the main research question in its entirety. The first sub-question creates insight into the conceptualization of values in financial industries. This entails making inventory of what theories exist that allow for the analysis of values and their application. In this part information about financial legislation and innovation within the financial industry will be collected. Also, the theoretical values – both social and moral – of certain stakeholders will be searched for from ethics in economics, VSD, business ethics and ethics of technology literature. Sub-question 1 will also delineate the content of PSD2, the VSD methodology and through this analysis identify the main stakeholders.

1. **How can privacy in innovation within the financial industry be conceptualized?**

The second sub-question clarifies the ethical challenges (i.e. main value at stake) by taking inventory of the relevant values at stake, which values conflict, how they conflict and prioritizing them.

2. **What is the importance of the values to be reflected by technology designed after PSD2 and what are the main ethical privacy related challenges that PSD2 brings to society?**

After having determined the values at stake in the case of PSD2, the next iteration is to determine how the most important values can be structured into design requirements. The outcome of sub-question 3 will illustrate the value hierarchy method and the steps required to formulate the design requirements for optimizing the impact of PSD2 on society. This sub-question connects theoretical concepts to empirical findings.

3. **How can the most important values be included by design?**

Lastly, sub-question four will transpose the design requirements, as formed in sub-question three, into practical principles for incumbent financial organizations in order to optimize the impact of PSD2 in society.

4. **What recommendations can be made regarding the inclusion of values by design in innovation with respect to PSD2?**

The sub-questions as stated above will accumulate to the answering of the main research question.

## 1.5.Research design

The proposed research will be of an exploratory nature as contemporary literature is scattered and incomplete. As is typical in a scene of scattered literature, the concepts used in this research are existent in literature individually. The specific combination made in this research however, is not. The lack of insight in interplay of these topics makes forming hypothesis or propositions difficult. Therefore, an exploratory form of research is chosen to gain understanding of qualitative nature. Specifically, this entails doing a case study – the case of PSD2 in incumbent financial organizations – as this is considered a generally well accepted method for exploratory research.

To answer the research questions and sub questions the research proposed will be conducted in three phases. The first being desk research and literature review, the second contain semi-structured interviews and the last is the application of value sensitive design method.

**Desk research and literature review**

The purpose of desk research is to identify values and create a framework for inclusion of values in innovation in the case of PSD2. The subjects of literature are amongst others business and finance ethics, ethics of technology, with a specific focus on Value Sensitive Design. The desk research and literature review will provide a subset of results for sub-question 1. Academic papers, essays, books and reports will be used as sources. These are accessed through the TU Delft library, google Scholar, Sciencedirect and Scopus. Additional sources such as news articles found through Google may be referred to as well, if appropriate. Keywords used are combinations of, or individually stated: *PSD2, design for values, value sensitive design, value, privacy, identity, autonomy, security, payment services directive, privacy by design, financial, banking, ethics in finance, privacy legislation.*

**Semi structured interviews**

Semi-structured interviews will be structured based upon the findings of the desk research and literature review. The values found in literature are validated through the data collected in these interviews and possibly extend the set of values. Access to experts will largely be granted by NIBC Bank and its network. The interviewees will be systematically selected to provide for a broad spectrum of perspectives (different organizations with different backgrounds; financial, semi-governmental, government, etc.). Chapter 3 elaborates on the procedures and approach of the semi-structured interviews.

**Value sensitive design**

We approach PSD2 technology as a socio-technical system, which means that we take the embedding of the technology in social and societal structures to be of essential importance to its effect. The validated values as found through literature review and semi-structured interviews are included to form a framework for innovation including values in incumbent financial industry

and answer sub-question 3. VSD is an approach that focuses on optimizing value of a product, system or process through the inclusion of a multitude of stakeholders with different priorities and preferences by and optimally combining those values in a design. These dimensions presumably increase an organization's active responsibility, if implemented properly. VSD is also considered to benefit socio-political acceptance (Kroes & van de Poel, 2015).

PSD2 brings technology in a socio-technical context. Because complex interdependencies are vital to the functioning of nearly all of the technologies of modern societies, it is false to think of the study of technology's impact on people and societies as an investigation of stand-alone products. Rather the object of study is the product construed in terms of key social interdependencies as responsible for its features, function and impact as for its physical characteristics (Nissenbaum, 2010). Taking into account such complex interdependencies when referring to a technology, scholars of social and humanistic study of technology refer to them as socio-technical products and systems. The technologies of concern in this research, i.e. those altering the flow of personal information in radical ways, are thus socio-technical. On the VSD methodology is elaborated in chapter 2.

## 1.6.Thesis overview

The chapters in this thesis are structured according to the order of the sub-questions, answering the before addressing the next. Chapter two gives a review of privacy in digital technology as well as other values relevant to innovation within the financial industry. Chapter three elaborates on the existing literature regarding the payment Services directive legislation and relevant legislation surrounding PSD. Chapter four addresses the research design of this thesis entailing the approach, purpose and an explanation of the units of analysis. Thereafter, in the same chapter, an overview of the cases and overviews of the methods for data collection and analysis are given. Chapter five is entirely dedicated to the results. In chapter six the case studies are analyzed and a discussion of these results with literature. Chapter seven will conclude this thesis with answers to the research questions, the contribution of this study to theory, the limitations of this thesis and opportunities for future research.

## 1.7.Conclusion

This thesis was incentivized by the revised Payments Services Directive which the European Commission issued in order to encourage innovation in the European payments industry. However, with the introduction of PSD2, questions came into being regarding the implementation of this legislation without unwanted risks to privacy in digital spaces. Through the Value Sensitive Design methodology, which appears underexposed in the subject innovation in finance, this research will deliver a framework for the inclusion of values in innovation within the financial industry. A research question was formulated: "What general principles for the inclusion of values in innovation within incumbent financial organizations can be derived from

the (privacy-related) values of stakeholders to optimize the anticipated effects of PSD2 on society?"

The main research question will be answered through four sub-questions. Sub-question 1 addresses the conceptualization of privacy as a value. The second sub-question determines what privacy related ethical challenges are inherent to PSD2 and what the relative importance is amongst the values as conceptualized in the first sub-question. Sub-question 3 finds how values can be translated to design requirements and sub-question 4 demonstrates the translation of values into design requirements by applying the value hierarchy method to privacy.

The thesis is composed 7 chapters; the first introducing the topic of research, the second geared towards the literature review, the third zooming in on the legislation PDS2, the fourth explaining the methods used for data collection, the fifth analyzing the interview results, the sixth reviewing and applying the value hierarchy and the last concluding this research.

# 2. Literature review

This chapter gives the conceptual part of the value sensitive design. This entails delineating and elaborating on concepts central to this research through reviewing literature on the concept of privacy and the affiliated values and previous research on the inclusion of values in the financial industry. This together answers sub question 1: "how can values in innovation within the financial industry be conceptualized?"

Chapter two is structured as follows. First, the VSD approach is elaborated on in order to construct a solid understanding of the way this study is conducted. Secondly, the definition of privacy in the scope of this research is researched. Thereafter, the exact subject within the scope is delineated; identity relevant information. Also, the reasons for which to preserve privacy are given. Lastly, privacy and values related to privacy are listed and conceptualized.

## 2.1. Value Sensitive Design

Technological innovation and engineering design sometimes provide opportunities to avert or offer ways out of moral dilemmas. Innovation in that sense is considered a strategy to reduce regret and moral residues in hindsight by changing the world in such a way that one is able to live by all its values (Van den Hoven, Lokhorst, & Van de Poel, 2012). Value Sensitive Design is the theoretical embodiment of this notion.

Value Sensitive Design (VSD) is an approach for responsible innovation through an 'iterative tripartite process' consisting of conceptual, empirical, and technical investigations. It aims to integrate knowledge of ethical impacts of a technology into a design process. It requires that the goals and criteria for judging the quality of technological systems are broadened to include those that advance human values. Technology's foremost purpose is translating scientific and technological knowledge into new artefacts and systems to solve certain societal problems. What is considered to be a societal problem or a solution is a question that is relative and subject to interpretation. Technological developments are the outcome of a sequence of decisions made by several types of actors: engineers who made design choices in order to solve specific problems; companies, universities or state organizations who have engineers on their payroll that pursue the creation of wealth, knowledge or welfare; and consumers who have to choose what to buy and how to use certain products. Value-sensitive design (VSD) reasons that, since technology should mainly serve societal needs, the various societal complications and ethical problems should be anticipated for as early as possible in a design process (Pesch, 2015).

VSD is a theoretically grounded approach that proactively considers human values throughout the process of technology design in a just and inclusive way (Davis & Nathan, 2015; Friedman, Kahn, & Boring, 2013). A value is a lasting conviction or matter that people feel is generally worth striving for, not just for them self to be able to gain in quality of life but also to contribute to a good society (Van de Poel & Royakkers, 2011). They are not to be confused with individual

preferences or facts because facts do not logically entail value. They are considered of being of importance for everyone. They provide means for orientation, justification, and evaluation of decisions of actions and preferences. Friedman et al. (2013) define a 'value' as "what a person or group of people consider important in life".

VSD is based on the notion that technologies are intrinsically value-laden. This reflects the interactional perspective of VSD as values are neither considered to be endogenously inscribed into technology nor as conveyed by exogenous forces. People and social systems affect technological development, and new technologies shape individual behavior and social systems (Freier et al., 2011). Its principle is that by proactively identifying relevant societal values, the design of a new technology can be adjusted so that its social acceptability is increased through reconstructing a sociotechnical public and the identification of its values. Its goal is the opportunity to include the concerns and values of this sociotechnical public in the design of the technology at stake, and its institutional context (Pesch, 2015). VSD emerged as an approach to the design of information and computer systems that accounts for human values in a principled and comprehensive manner throughout the design process (Friedman & Kahn, 2002; Van den Hoven, 2007). Later the methodology was elaborated to address the inclusion of values in other domains of technological design such as architecture, economics, nuclear technology (Van den Hoven, Vermaas & Van de Poel, 2015). VSD aims to create a technological design that effectively incorporates the relevant public values, seeking solutions through design changes. Designing for values contributes to the success, acceptance and acceptability of innovations and therefore has economic benefits (Van den Hoven et al., 2015).

VSD's tripartite process consists of conceptual, empirical, and technical investigations. The conceptual investigation includes the identification and articulation of central values at stake in a particular design context and the identification of stakeholders that are affected by this design (Pesch, 2015). Identifying stakeholders affected by the technology entails both the individuals using the technology (direct stakeholders) and individuals influenced without using the technology (indirect stakeholders). It, amongst others, comprises a philosophically informed analysis of the conceptualization of certain values and provides criteria for trade-offs. The findings from the conceptual investigations are used to find out how stakeholders experience technologies with regard to the values they consider important. This is the empirical investigation. It focusses on the human response to the technology in question and on the larger social context. This investigation may be conducted through a range of quantitative and qualitative methods. The technological investigation focusses on the design and performance of the technology itself through the human moral values identified in other parts. Technical investigations can involve either reflective analyses of existing technologies or the design of new technological products and systems. Altogether, VSD is considered to be a form of 'front-loading ethics', allowing a proactive stance with regards to ethics and technology (Pesch, 2015).

### 2.1.1. Applications of VSD

Streams of research that have applied VSD relevant to this research are the 'design for values in ICT' and 'privacy by design'. The former, design for values, is a field of research which is concerned with the social and cultural context of ever evolving technological trends (Huldtgren, 2015). Designing for moral values has become a progressively central subject in the development of ICT. One difficulty is that the effects of a technology and the impact on human values can only be completely assessed after the technology has been developed. When the technology is already in use, policies are not in place to avoid harm. Therefore, amongst others Huldtgren (2015) argues that "including considerations of human values and systemic effects of technology early on in the design process is the most reasonable solution (Huldtgren, 2015)." Freier et al (2011), for example, created an analytic tool that provides designers with the knowledge to recognize the privacy implications of their designs and through their designs to proactively improve privacy together with other enduring human values before the technology is implemented in society (Freier et al., 2011). This framework is somewhat related to this research as location related information is a form of identity-relevant information and thus privacy sensitive. The specific commitment of design for values in ICT is particularly relevant to this research as products and services in financial industry are mainly products of ICT.

Privacy is one of the most enduring social issues associated with information technologies (Nissenbaum, 2004). This makes for a good motivation to implement privacy into technological designs. The 'Privacy by Design' approach provides general guidelines for designing privacy protective products. Its ideology revolves around the notion that data protection needs to be approached proactive instead of reactive which makes privacy by design preventive rather than corrective. Privacy by design also states that data protection should be a prominent subject in all of a product's life cycles. The principles of the Privacy by Design method revolve around the idea that "data protection needs to be viewed in proactive rather than reactive terms, making privacy by design preventive and not simply remedial (Davis & Nathan, 2015)". The framework of Privacy by Design following from this idea is a of VSD approach with the specific aim to integrate privacy protection into technologies for analysis by design, so that an analysis takes privacy requirements in consideration in every step of the process (Warnier, Dechesne, & Brazier, 2015). Privacy by Cavoukian (2009) proposes seven foundational principles for a design to be privacy proof: (1) being proactive, (2) privacy as default, (3) privacy embedded in design, (4) commitment to functionality in a positive-sum strategy (e.g., avoid privacy vs. security trade-offs), (5) life cycle management of data, (6) visibility and transparency to users and providers, and (7) respect for user privacy (Huldtgren, 2015). Through the Value Sensitive Design approach, Friedman et al. (2006) developed similar rules to preserve privacy, such as informed consent, i.e., give users the option on what information is stored (or not), and transparency, i.e., tell users which information is stored about them.

### 2.1.2. Critiques on VSD

The critique on VSD is comes in four arguments: universal values, ethical commitments, stakeholder management and the emergence of values and voice. The first one, universal values, entails the critique on the stance that VSD assumes that certain values are universal across cultures while values are contextual and differ in the context of a technology (Borning & Muller, 2012). This led to the belief that VSD should not bias a VSD practitioner on the basis of universality or relativism of values but rather let a value be free to any position in context to a particular research, while at the same time not stray too far from the list of values as proposed by Friedman et al. (2013). A value can both be empirical or philosophical of construct. A value as taken from a stakeholder can be related to an empirical base. The process of empirically conceptualizing a value, however, is vulnerable to fallacy which should be avoided through referencing to existing values in VSD literate. The values used in this research for VSD are formulated in a prescriptive way in order to ensure sound reasoning and avoid such fallacy.

Also, several scholars support the claim that VSD does not provide a method to identify stakeholders and does not include stakeholders' values to the design process (Borning & Muller, 2012; Manders-Huits, 2011). Therefore this research derives the priority of each of the values at stake through the identified stakeholders. This also addresses the concern of several scholars who argue that values should emerge from the work with the stakeholders rather than by the research alone from the conceptual investigation in order to reduce the chance of areas of concern being overlooked (Le Dantec, Poole, & Wyche, 2009). Literature streams related to PSD2 have clarified the stakeholders at play and relevant values. The values as derived from literature will be compared to the list of values from Friedman et al. (2013) and if necessary adapted. The above mentioned approaches to this research will remedy the shortcomings of VSD and result in a sound and comprehensive framework for creating design principles.

## 2.2. Privacy

Privacy is one of the most enduring social issues associated with information technologies (Nissenbaum, 2004). 'Privacy' has been defined in many different ways from several perspectives. This research addresses the concept from an ethical perspective. The concept of privacy usually occurs within the context of ethical issues involving information about individuals. There is little agreement about the precise meaning and applicability but there is consensus among privacy scholars that privacy is important and that privacy is vague, relative and hard to define (Nissenbaum, 2010; Van den Hoven, 2008; Hirschprung et al., 2016). Privacy is often thought of as freedom from judgement, disturbance, uninvited public attention and the ability of an individual or group to limit its self-expression (Fink et al., 2017). Within VSD literature, privacy is considered to refer to a claim, entitlement or a right of an individual to control what information about himself or herself can be communicated to others (Friedman et al., 2013).

In his unified theory for the framing of online privacy policy, Tavani (2007) based the concept of privacy on four different streams of theory each with their own strong and weak point for application in digital space, indicating once more the difficulty of conceptualizing privacy. According to Tavani (2007), "an individual has privacy in a situation with regard to others if in that situation the individual is protected from intrusion, interference, and information access by others (Tavani, 2007)." Informational privacy is "freedom from epistemic interference" that is achieved when there is a restriction on 'facts' about someone that are unknown, which would include finances (Tavani, 2008). Privacy is also said to include the concepts of appropriate use and protection of information (Nissenbaum, 2004).

Privacy is taken as something desirable, a right or an aspect of human dignity. The United Nations' recognizes privacy as a human right by stating that "no one shall be subjected to arbitrary interference with his privacy" and that "everyone has the right to the protection of the law against such interference or attacks (United Nations, 1948)." However, the concept of privacy is very much dependent on context as is also illustrated in by the inclusion of the word 'arbitrary' in the above quoted section of human rights. Another attempt to conceptualize privacy is done by Huldtgren (2015) who constructs the concept as to be composed of three different aspects; "being left in peace and free from intrusion, being able to control information about oneself, and not being tracked, followed, or watched in private space. However, this construct is relative to personal circumstances (Huldtgren, 2015)."

The concept is both understood as intrinsically valuable as well as deriving its value from the fact that it is favorable to other values, e.g. autonomy or choice (Nissenbaum, 2004; Solove, 2002). Janssen and van den Hoven (2015) recognize this ambiguity by stating that the definition of privacy is "influenced by legislation and policies, culture, societal values and norms, complexity resulting from the involvement of many organizations, processes and procedures, interpretations, organizational structure, and so on (Janssen & van den Hoven, 2015)." They argue that the concept of privacy should therefore be conceptualized as complex, non-dichotomous constructs interrelated with other factors.

Although privacy is intuitively appealing, it is hard to realize in practice due to incorrect conceptualizations. Only by conceptualizing privacy in a complex and composed way, the nature and impact of PSD2 on privacy can be understood, and its levels can be balanced with security, safety, openness and other socially-desirable values (Janssen & van den Hoven, 2015). This view is applicable to this research for the reason that it recognizes that privacy is based upon multiple other values. In order to be able to form a sharply delineated conceptualization, first two things need to be determined: what privacy applies to (i.e. what type of privacy is relevant to this research) and why it is to be considered a value (what reasons would morally justify protecting personal data and what reasons would justify putting limits to the freedom of others to get access to them?).

### 2.2.1. Identity relevant information

What does privacy apply to? It is essential to our research to determine this part of the scope in order to be able to define when an entity is acquiring, storing and processing information about another entity. Perhaps the most intuitive answer is given Malhotra et al. (2004) who use informational privacy. Informational privacy needs to be distinguished from the right 'to be left alone' and 'decisional or constitutional privacy', that is, the right to decide without government interference (Van den Hoven, 2008). Informational privacy refers to "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others (Malhotra, Kim, & Agarwal, 2004)." The unit to which privacy applies is thus 'information about individuals, groups or institutions' or 'personal data'.

EU data protection laws defines 'personal data' as any kind of information concerning an identifiable natural person, which is called a 'data subject'. An 'identifiable natural person' is a person who can be identified, either directly or indirectly, in particular by reference to one or more factors specific to his or her physical, physiological, mental, economic, cultural, social identity or identification number (European Parliament, 1995). This led van den Hoven (2008) to redefine personal data to 'identity-relevant information'. Because even though information may not be about an individual, group or institution, it may still refer to them; the EU data-protection laws protect against referentially used description but could let attributively used descriptions go unprotected. This is the principle of that information may be attributively used and referentially used descriptions as both types help to collect information on people and directly or indirectly help to increase knowledge about them. Van den Hoven and Manders-Huits (2006) argue that instead of defining the object of protection in terms of referentially used descriptions, objects should be defined in terms of the broader notion of 'identity relevant information', as will be done in this research (Manders-Huits & Van den Hoven, 2008).

### 2.2.2. Reasons to protect information

Now that is clear what is to be protected the question naturally following is 'why should we protect identity relevant information?' Or more specifically put, what moral justifications exist that allow for limiting generation, acquisition, processing, and dissemination of identity-relevant information? Van den Hoven (2008) argues that four types of moral reasons are to be distinguished between, that justify limitations to the flow of identity-relevant information. These are 'information-based harm', 'information inequality', 'informational injustice' and 'moral autonomy and moral identification'.

The first one, *information-based harm*, refers to harm that could not have been inflicted without certain information. This includes a broad range of harms to individuals that can be inflicted on the basis of personal information. For example, identity fraud where cybercriminals use databases and the internet to select their targets and prepare for their crimes. "Protecting identifying information, instead of leaving it in the open, diminishes epistemic freedom of all to

know, but also diminishes the likelihood that some will come to harm, analogous to the way in which restricting access to firearms diminishes both freedom and the likelihood that people will get shot in the street (Van den Hoven, 2008)."

Secondly, the *informational inequality* type of moral reason for restriction concerns equality and fairness. It describes the asymmetric position between buyer and seller of identity-relevant information. An individual may have something of worth, e.g. transactional information. Think of an airline company that is able to accumulate an accurate personal profile for targeted advertisement. However, that individual may not always be aware or in a position to benefit from a transparent and fair market environment. The airline does not offer discounts in exchange for the transactional data. As contracts are rarely independent and can therefore not be trusted to provide for a transparent and fair market for identity-relevant information, constraints need to be put in place.

The third type of moral justification for constraining the flow of identity-relevant information is that of *informational injustice*. It constructs the principle of what is often seen as a violation of privacy as "the morally inappropriate transfer of personal data across the boundaries of what we intuitively think of as separate 'spheres of justice' or 'spheres of access'" (Van den Hoven, 2008). The concept of these spheres stem from the work of Walzer (1983), who put forward a construct in which a 'just distribution' of a certain good is relative to what it means to whom it is a good. 'Spheres of justice' or 'spheres of access' are subjective domains where a certain good is considered to have worth and this good is distributed by means of allocation criteria or allocation practices (Walzer, 1983). Informational injustice describes the possibility of identity-relevant information being a currency in another sphere. This could, for example, occur when one's payment information is used to determine the costs of a health insurance scheme. In this case the financial sphere overlaps the healthcare sphere and could thus be perceived as a violation of privacy. Constraints can be put in place in order to prevent informational injustice. A condition for these constraints is, though, that boundaries of spheres should be clearly defined in order to distinct separate and overlapping spheres.

The last moral reason for restricting the flow of identity-relevant information is that of *moral autonomy and moral identification*. It bases its reasoning on the right to "shape our own moral biographies, to present ourselves as we think fit and appropriate […] without the critical gaze and interference of others and without a pressure to conform to the 'normal' or socially desired identities (Van den Hoven, 2008)." However, when information becomes public that affects public opinion about a person, beliefs and judgements are formed outside that individual's influence. This may lead to that person behaving differently than he would have done without that affected public opinion. Moral identification builds forth on the reasoning above to the extent of claiming that the simple identifications made on the basis of data will never be equal to reality. "An outsider's understanding of a person needs to include, ideally, not only the objective representations, but also what he wants or hopes to be, his gratitude or pride or shame or

remorse, and how the person interprets them. These conditions are conditions of the whole person. The very object of the outsider's interpretation ought to aim at representing and understanding the person's second-order as well as first-order attitudes, which is not only difficult, but impossible in principle (Van den Hoven, 2008)." Therefore, in order to prevent false impressions about individuals, identity relevant access to information should be limited.

### 2.2.3. Privacy related values

As stated in the definition of the concept of privacy, privacy should be conceptualized as interrelated with other values. These values are listed and elaborated on in the following section. They are derived from several streams of literature among which Business Ethics, Financial Ethics, Design for Values in ICT, Ethics of Technology and Value Sensitive Design. Also, rules and legislation are considered a stream of literature as they also attempt to protect the value of privacy through enforcing related values (Warnier, Dechesne, & Brazier, 2015).

#### *Transparency*

Transparency is considered as an important societal and democratic value. Transparency is not only about availability of information, but also about how the information is collected and published (Janssen & van den Hoven, 2015). Freier et al. (2011) give a broad and applicable definition of transparency through the principle of informed consent. They argue that informed consent is a combination of awareness and control. Informed consent entails providing mechanisms for user awareness of what information is being collected, how that information will be stored, where that information will be stored, how long the information will be stored, and to whom the information may be transferred. Technologies are said to be invisible if they provide no mechanism for enabling user awareness. Transparent systems are those that disclose the appropriate information to the user in a form that is honest and comprehensible (Freier et al., 2011). Friedman et al. (2013) construct informed consent as a value that entails "accumulating people's agreement, encompassing criteria of disclosure and comprehension (for 'informed') and voluntariness, competence, and agreement (for 'consent') (Friedman, 2013)."

#### *Ownership*

Friedman and Kahn (2003) construct ownership as "the general right to property" which brings several rights which include the right to possession, usage, management, benefit and disposal. This definition, however, is only limitedly applicable to this research as it was meant for physical objects. Many questions about the ownership of intangible data such as online activity or generated data are raised. For example social media content, which in some cases is created by multiple individuals and thus jointly owned (Huldtgren, 2015). A clear definition of ownership is hard to construct because opinions on this matter differ (Marshall & Shipman, 2011). Perhaps a working definition of 'ownership of data' for this research could be the right of an individual to

know what kind of data is stored about them, how it is processed, whom it is being shared with and to save, share, publish or remove data.

### *Openness*

Although openness and transparency are often used as interchangeable terms, the former is more often used within the context of organizations for the willingness to share accurate information, either proactively or upon request. A high degree of openness has been found to increase other values such as accountability and trust (Bertot, Jaeger, & Grimes, 2010). On an individual level, access to accurate information is termed accessibility (Langheinrich, 2002). This entails the ability of users to access their personal data and information about their data (e.g. usage logs) (Kasiyanto, 2016). A form of openness is notice. Notice means communicating data collection practices to users. In the complex environment of digital payments, data flows are often hidden from plain view making it hard for data subjects to recognize that data is being collected. Efficient ways to communicate collection practices to the user is regarded as notice (Langheinrich, 2002).

### *Agency*

Friedman et al (2013) refer to autonomy as an individual's ability to decide plan and act as they see fit in order to achieve his/her goal (Friedman et al., 2013). While autonomy is typically focused on an individual's self-reliance and sufficiency, agency allows for cooperation as well as self-sufficiency (Friedman, Khan, & Howe, 2000). Wilson and Shpall (2012) construct agency as purposeful, goal directed activity (intentional action) while the agent is aware of their physical actions and the purpose of those actions. Agency in thus seen as 'goal directed action' in which an agent initiates a sort of direct control or direction over their own behavior (Wilson & Shpall, 2012). Barad (2003) continues on this line of thought and expands it by saying that agency is the "ability to define one's goals and act upon them", but can take multiple forms, from bargaining and negotiation, to subversion and resistance, as well as the more "intangible, cognitive processes of reflection and analysis (Barad, 2003)". Agency is sometimes found to have a relationship with an individual's subjective well-being through a sequence of adaptive mechanisms that promote human development (Fernandez, Giusta, & Kambhampati, 2015) and generally linked to human well-being (Welzel & Inglehart, 2010). Agency refers to the experience of being in control of both one's own actions and, through those actions, having influence in events in the external world (Haggard & Tsakiris, 2009). A derivative more geared towards ethics is that of moral agency; "agency is an individual's ability to make moral judgments based on some notion of right and wrong and to be held accountable for these actions (Angus, 2003)."

### *Freedom from bias*

Computer technology is considered to be biased if it systematically and unfairly discriminates against certain individuals or groups of individuals in favor of others. A technology discriminates

unfairly if it denies an opportunity or a good, or if it assigns an undesirable outcome to an individual or group of individuals on grounds that are unreasonable or inappropriate (Friedman, Brok, king, & Thomas, 1996). Friedman et al. (2013) define 'bias' as systematic unfairness towards an individual or group which includes "pre-existing social bias, technical bias, and emergent social bias".

### *Security*

The term 'security' comes from Latin roots that mean "without care" and is a quality of systems that enables people to be free of concern. Security is a set of measures to ensure that a system will be able to accomplish its goal as intended, while minimizing unintended negative consequences. Security is therefore construed as the challenges to protect consumer transactions and data against "conventional" crimes such as fraud, theft or hacking (Kasiyanto, 2016). Privacy is often seen as an aspect of security because a secure system should protect the privacy of its users. To security purists, privacy is an expression, or use case, of confidentiality (Macaulay, 2017). At the same time, security may be considered contrary to privacy. For instance, politicians and industry leaders endure reduced privacy to protect the public trust they hold (Fink, Edgar, Rice, MacDonald, & Crawford, 2017). Edgar and Manz (2017) define cyber security as "measures and actions taken to prevent unauthorized access to, manipulation of, or destruction of cyber resources and data" which includes the technologies, rules, and procedures to secure something in cyber space (Edgar & Manz, 2017). The most workable definition of security for the purpose of this research comes from Barker et al. (2013) who define security as "assurance that the confidentiality of, and access to, certain information about an entity is protected (Barker, Smid, Brandstad, & Chokhani, 2013)." "Entity" in this case, can be a corporation or facility as well as an individual person. "Certain information" may refer to any sensitive information, but in the scope of this research could refer to 'identity-relevant information'.

Security is achieved by enforcing integrity and authenticity. Integrity entails that the transaction information will be intact while being processed and cannot be altered (Kasiyanto, 2016). Assets that can be modified only by authorized parties or only in authorized ways (Fink et al., 2017). Digital signatures and secure hashes ensure the integrity of messages sent and received. Authenticity verifies the identity, often as a condition for access. Identities, certificates, passwords, and other mechanisms guarantee only authorized individuals access identity-relevant information (Fink et al., 2017). Closely related to authenticity is confidentiality which indicates the degree to which identity-relevant information is safe against unauthorized access (Kasiyanto, 2016). Computer-related assets can be made accessible only to authorized parties by for example encryption.

Another form of authenticity is nonrepudiation, which refers to a state of affairs where the author of a statement will not be able to successfully challenge the authorship of the statement or validity of an associated contract (Zhou, 2001). This protects against an individual's false

denial of having performed a particular action and captures whether a user performed particular actions (i.e. sending or receiving a payment). Automatically collected records and logs may show which user accessed or modified specific parts of a system. When these logs are protected by some integrity mechanism, the result is a system with nonrepudiation (Fink et al., 2017).

#### *Accountability*

Accountability refers to properties that allow for tracing the actions of an individual or organization uniquely to the owner (Friedman et al., 2013). An identity relevant information related definition of accountability is 'recourse' which refers to "the user's ability to hold the recipient of a disclosure accountable for inappropriate use of the user's personal information (Freier et al., 2011)." As accountability requires a ledger of actions coupled to identities, accountability and privacy in some cases can appear mutually exclusive. Naylor et al (2014), however, argue they do necessarily have to be (Naylor, Mukerjee, & Steenkiste, 2014).

#### *Trust*

Schneider (1999) uses 'trust' and 'trustworthy' in the context of "systems that perform as expected along the dimensions of correctness, security, reliability, safety, and survivability (Schneider, 1999)." This technical approach of trust, however, contrasts with the construct of trust as a social value. People trust when they are vulnerable to harm from others, yet believe those others would not harm them even though they could. In turn, trust depends on people's ability to make three types of assessments. One is about the harms they might suffer. The second is about the good will others possess toward them that would keep those others from doing them harm. The third involves whether or not harms that do occur lie outside the parameters of the trust relationship (Friedman et al., 2000; Friedman et al., 2013). When using trust in an online environment, one should distinguish between two contexts: business-to-customer, where it can be hard for customers to judge a company's good will and the risks associated with a transaction, and consumer-to-consumer, for instance, in online social media, in which violations of trust may cause psychological harm (Freier et al., 2011).

### 2.2.4. Ethics in finance

Financial innovation is generally agreed upon to be in need of a more responsible approach (Crouhy, Jarrow, & Turnbull, 2008). Armstrong et al (2013) discuss the potential of responsible innovation in finance. They argue that innovation within the financial industry would benefit from an 'internalized' sense of responsibility by establishing 'New Product Approval Committees' with the purpose of fostering *accountability*, *consensus* and *conscientiousness*. They also mention *precaution* as a value; this 'precautionary principle' is a principle that aims to take into account options besides the main road taken, while explicitly not excluding innovation. "Innovating with care, avoiding excesses, considering proportions and scope of engagement" are part of the precautionary principles. Lastly, the value of *democracy*; refers to inclusive debate and

to the empowerment of stakeholders. A responsible approach is considered to be that discussed and decided upon by all stakeholders. In their view, responsible innovation in finance is fostered by making informed decisions with all concerned parties that assume collective responsibility for a particular issue through their involvement in decision-making, particularly in situations where consequences of a certain act are uncertain (Armstrong et al., 2011).

## 2.3.Conclusion

This chapter reviewed literature in order to answer the first sub-question: *How can privacy in innovation within the financial industry be conceptualized?* Firstly, the Value Sensitive Design approach was reviewed in order to provide a framework for the inclusion of values in innovation. VSD is built on the notion that technologies are intrinsically value-laden and their foremost purpose is translating scientific and technological knowledge into new artefacts and systems to solve certain societal problems. VSD is suited for this research through as it enables technologies designed after PSD2 to promote the relevant values. Secondly, the concept of privacy was defined and conceptualized by reviewing several streams of literature. Janssen and van den Hoven (2015) propose that the concept of privacy is "influenced by legislation and policies, culture, societal values and norms, complexity resulting from the involvement of many organizations, processes and procedures, interpretations, organizational structure, and so on (Janssen & van den Hoven, 2015)." Nissenbaum (2004) argues that the concept of privacy should therefore be conceptualized as complex, non-dichotomous constructs interrelated with other factors. Privacy applies to identity relevant information, which is the principle of that information may be used both attributively and referentially for descriptions as both types help to collect information on people and directly or indirectly help to increase knowledge about them. Furthermore, as the concept of privacy is conceptualized in a complex and composed way, values related to privacy in the case of PSD2 were identified in several literature streams. These were determined to be ownership, openness, agency, freedom from bias, security, accountability and trust. Lastly, this chapter found implications for a responsible approach in financial innovation through reviewing ethics in finance literature.

# 3. Payment Services Directive

In order to create general principles for the inclusion of values in financial innovation, a review of existing literature on the supra-national legislation should be conducted. The following section does so by starting off with an introduction to PSD2's predecessor, PSD1. Subsequently, PSD2 is introduced and thirdly, related privacy and security legislation is explored. Also, the main stakeholders for this research are identified as the case of PSD2 is elaborated on in this section.

## 3.1.PSD1

The first PSD was created out of the necessity for more efficient pan-European payments. In 2002 the political pressure rose to levels sufficient to result in legislation on cross-border payments in euros. It entailed a mandatory standard for fees and handling speed making domestic and European payments uniform. Regardless of the standard, however, a bank's expenses for European payments remained the same as before the introduction of this legislation. This incentivized European banks to develop a Single European Payments Area (SEPA) which would reduce the costs of cross European payments. SEPA entailed reforming the fragmented national euro payments markets to a single 'domestic' market. Because SEPA initiative of the European Union, but is no formal legislation itself, formal steering was only possible to a limited extent. For that reason the European Commission felt the need for establishing a comprehensive legal foundation for the creation for a single European payments market; PSD1. PSD1 is applicable to all payment services in the 28 SEPA countries and has the objective of creating supervision on all parties delivering payment services as well as to increase competition by allowing other non-bank parties to offer payment services (Reijers, 2016).

The intention of PSD1 was to unify rules regarding payments in all SEPA countries. This should have had the effect of making European payments less time and cost consuming. Secondly, the PSD1 provided extra consumer protection regarding refunding and liability on top of national legislation. Thirdly, the fast and affordable uniform payments should have increased intra-European retail competition. Fourthly, increased competition should have also occurred in the payment industry due to the introduction of the Payment Institution (PI); companies other than banks handling payments. No substantial impact was observed on technological innovation or entry of new actors (Deprez, 2013). Before PSD1, only banks and credit institutions could have been seen as PSPs. However, PSPs hold another legal status than banks. Acquiring the legal status of a PI requires amongst others a certain minimum level of capital to guarantee continuity. Fifthly, additional transparency was created by demanding more and clearer information to be conveyed to customers. This way comparison between payment services has less of a threshold (Reijers, 2016). Reijers (2016) identified the unresolved issues of PSD1 to be 1) the limited geographical scope of the Directive (extra-European payments are outside the scope of PSD1 hindering efficient online economic activity), 2) the market heterogeneity (PSD1 allows for discrimination on the national level, e.g. supporting debit card over credit card) and 3) the rise of

third party payment service providers (PSD1 does apply to TPPs as they do not hold any funds at any time).

## 3.2.Introduction to PSD2

Since PSD1 had been implemented in national law in November 2009, several shortcomings came to surface which would have to be resolved in a successor. Also, the trends of changing payments habits needed to be taken into account. With these incentives the EC proposed to revise the PSD. The purpose of the revised Payment Services Directive is mainly to stimulate innovation within the payments markets again which is to be accomplished through legally allowing Payment Account Access Services (PAAS) (PwC, 2016). This aspect is accompanied by an increased security clause (SCA). PSD2 has to be implemented in national legislation by January 2018 and ASPSPs should have complied by November 2018 (European Commission, 2015).

The following section summarizes the most relevant aspects of PSD2 to this research. These are articles from PSD2 related to privacy. By summarizing these, a good understanding of the Directive will add to an accurate analysis of potential issues as explored in the subsequent paragraph. The following articles are derived from Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 (European Commission, 2015).

**Exclusions (Article 3):** the exclusions to PSD2 legislation include most cash-to-cash, paper cheque transactions, transactions directly between payer and payee and transaction without an intermediary.

**Definitions (Article 4):** the legal definitions of entities in PSD2 are set in this article. These are of importance to this research as they bind functionalities to responsibilities. The first party to be defined is the Payment Initiation Services Provider (PISP) or (PIS), which provides services to facilitate payments between merchants and online banking systems. Account Information Services Provider (AISP) or (AIS) is a party providing holistic overview of transactions and balances information of one or more current accounts. The AISP and PISP are both commonly referred to as Third Party Payment Services Provider (TPP). An organization maintaining current accounts under a European banking license is named 'Account Servicing Payment Services Provider' (ASPSP).

**Designation of competent authorities (Article 22):** appoints the European Banking Authority (EBA) as the 'competent' authority for TPP supervision on a European level. It does the same for primary competent authorities in the home member states which are the national banks. Also, all other relevant authorities, if any, are expected to cooperate with each other in order to promote supervision. Reijers (2016) remarks that by legally defining TPPs and assigning the competent authorities to supervise them, TPPs are placed under supervision when the PSD2 comes into effect.

**Supervision (Article 23):** continuing on article 22, this article empowers the competent authorities through legal capabilities to intervene when appropriate or necessary.

**Rules on access to payment account in the case of payment initiation services (Article 66):** the content of this article is the legal basis for Payment Initiation Services. This also entails the obligatory and unconditional cooperation of banks as they will need to work together with PISPs in order to realize the services. Besides certain obligations, this article also states several requirements surrounding confidentiality and security. One of those is that the "payment service user's explicit consent" is required.

**Rules on access to payment account in the case of account information services (Article 67):** the same as in article 66 applies in this article but here it does so for Account Information Services. This also encompasses the confidentiality and security requirements.

**Data protection (Article 94):** PSD2's data protection is covered through the Data protection directive 95/46/EC (European Commission 1995). A TPP in possession of personal data should thus always be in compliance with the Data protection directive (DPD). Amongst others, this means that the customer has to give explicit consent for the processing of personal data and the TPP needs to have a clear purpose for collecting and processing. Fraud monitoring, however, is exempted from this. The PSD2 will legally allow the processing of personal information for the purpose of reducing fraud without the obligation to inform customers or get their consent. A final statement made in this article makes that only data which is relevant to the service in question may be used (Reijers, 2016).

**Management of operational and security risks (article 95):** This article is dedicated to the precautions to be taken by a TPP regarding security of services and systems. This for example, takes the form of the obligation to publish an incident and inform relevant competent authorities. Interesting in particular is the obligation of the competent authority to conduct a yearly security review on the TPP.

**Authentication (Article 97):** A lasting subject of debate is the strong consumer authentication (SCA), or two-factor authentication. Some interviewees stated that SCA was a result of the banks lobbying. Article 97 states that a TPP can either arrange for proper authentications methods itself or rely on the authentication system of the ASPSP. Also, an extra level of authentication is required for PIS (inclusion of the payment amount and beneficiary in payment authorization).

**Regulatory technical standards on authentication and communication (Article 98):** essential to how PSD2 will eventually influence innovation and society is the Regulatory Technical Standard (RTS). It is stated in this article that the EBA, as the competent authority on supra-national level, is responsible for developing the technical policy for security and data protection. This article in the PSD2 sets some guiding principles that outline further standardizations, policies and guidelines on a practical level that will help national supervisors to

develop their control instruments to supervise TPPs on the topics of security and data protection.

In the PSD2, TPPs are considered a specific type of Payment Services Provider and thus are in scope for supervision by the main national supervisor of financial organizations, which is DNB in the Netherlands. As TPPs process personal information they are also subject to the supervision of the AP for data protection. Finally, when TPPs offer services to customers they fall under the supervision of the ACM. On a European level, an important position is given to the EBA. The EBA is primarily tasked with providing guidance to national supervisors on implementing the PSD2. No official supervisor has yet been appointed for information security in general, nor in the PSD2. The absence of an official national supervisor on information security creates a gap in supervision in general. Having a supervisor that can enforce sound security hygiene and force companies to cover the basics, is essential to prevent security incidents and reduce the impact. This gap is partially closed in the Dutch financial sector by DNB as it has made progress on this topic since 2010 (Reijers, 2016).

## 3.3.Regulatory Technical Standards

In accordance with Article 98 of the revised Payment Services Directive (EU) 2015/2366 (PSD2), the EBA has developed, in close cooperation with the European Central Bank (ECB), the draft RTS specifying the requirements of SCA, the exemptions from the application of SCA, the requirements with which security measures have to comply in order to protect the confidentiality and the integrity of the payment service users' personalized security credentials, and the requirements for common and secure open standards of communication (CSC) between ASPSPs, PISPs, AISPs and end-users (European Banking Authority, 2017).

An initial Discussion Paper was published in December 2015 by the EBA to explain its initial ideas and interpretations of the EBA mandates and related provisions in the revised PSD. This publication was assessed externally and formed the basis for the publication of a Consultation Paper in August 2016 containing draft RTS. The EBA, in close cooperation with the ECB, has reviewed and assessed the responses, identifying around 300 different issues or requests for clarification, a small subset of which appeared to be the key issues for respondents. These key issues were (1) the scope and technologically-neutral requirements of the draft RTS; (2) the exemptions, including scope, thresholds and the request of many respondents to add an exemption for transactions identified as low risk as a result of what some respondents referred to as 'transaction-risk analysis', and (3) the access to payment accounts by third party providers and the requirements around information communication (European Banking Authority, 2017).

The general principles ensure that adequate protection to the consumers takes place while the usability of the systems is promoted (Kasiyanto, 2016)." During the assessment of the responses, the EBA has had to make trade-offs between the various, at times competing, objectives of PSD2, including enhancing security, promoting competition, ensuring technology and business-

model neutrality, contributing to the integration of payments in the EU, protecting consumers, facilitating innovation and enhancing customer convenience. For example, the objective of ensuring a high degree of security and safety would suggest that the EBA's technical standards should be rather demanding in terms of authentication, whereas the objective of user-friendliness would suggest that the RTS should be less strict. Also, references to ISO 27001 and specific characteristics for the three elements constituting SCA were removed from the RTS, to ensure technology neutrality and allow for future innovations (European Banking Authority, 2017).

This final draft RTS was submitted to the Commission for adoption. As defined in PSD2, the RTS will be applicable 18 months after its entry into force, which would suggest an application date of the RTS in November 2018 at the earliest. The intervening period provides the industry with time to develop industry standards and/or technological solutions that are compliant with the RTS (European Banking Authority, 2017).

The EU Data Directive legislation is technologically neutral (while certain actors argue otherwise) which means that this legislation does not prescribe one technology over another. This is similar to the idea of 'design principles'; systems design according to the same design principles does not necessarily have to be relying on the same technology. Thus, systems that are designed according to the EU Data Directives should be in compliance with privacy legislation and thus respect the privacy of its users (Warnier et al., 2015).

## 3.4.Related legislation

By introducing the revised Payment Services Directive, the European Union accepts innovative financial services by addressing the legal challenges they bring with. Data protection is an essential challenge in the many challenges stakeholders bring forward during the formation (Fuster, 2016). Article 95 of by the PSD2 states that data protection is covered the Data Protection Directive 95/46/EC (European Commission 1995). The Data Protection Directive was adopted in 1995. It regulates the processing and free movement of personal data within the European Union. It is an important component of EU privacy and human rights law. It forms the basis for the majority of contemporary rules surrounding the topic of storing and processing personal data. The DPD consists of several principles (Warnier et al., 2015):

- **Transparency** entails that it should be clear what information is stored
- **Purpose** means that it should be clear for what purpose the personal data is stored
- **Proportionality** indicates that only relevant data should be stored
- **Access** means that the user should know what personal data about them is stored and they should be able to change errors if any
- **Transfer** entails personal data should only be transferred with explicit permission of the user and the user should be able to request a transfer of personal data.

A General Data Protection Regulation (GDPR, Regulation (EU) 2016/679) is in place to substitute the current Data Protection Directive, which is very much in line with the EU right to personal data protection and EU 2020 Single Digital Market Strategy. The primary objectives of the GDPR are to give citizens and residents back control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. It also addresses the export of personal data outside the EU (Council of the European Union, 2015). In the GDPR, several aspects of the DPD are reviewed in order to strengthen its scope and limits. For example, the GDPR reviews the DPD on how to apply the principles of handling personal data in the context of Big Data and open data and looks at both components of the purpose limitation principle: (1) the condition that processing must be for a specified, explicit and legitimate purpose; and (2) the condition that any further processing of data must be for the same purpose as the original one for which the personal data were collected. The GDPR will take effect as of 25 May 2018 (European Parliment, 2016).

The EU's proactive attitude towards the protection of privacy finds its roots in the EU Charter of Fundamental Rights. It states that "the EU fundamental right to the protection of personal data is granted to "*everyone*", and that it entails that personal data "must be processed ***fairly***" (that is, in compliance with applicable rules determining the exact obligations of those responsible for the processing), always "for *specified* purposes" (in accordance with what is known as the "purpose limitation principle") and "on the basis of the *consent* of the person concerned or some other *legitimate* basis laid down by law" (that is, based on a legitimate ground, which could be the consent or another ground). Additionally, the Charter states that the individuals to whom the data processed relates have a "right of *access*" to such data, as well as "the right to have it *rectified*" when appropriate (Fuster, 2016)."

## 3.5.Conclusion

This chapter was dedicated to reviewing the case of PSD2, its background and related legislation, in order for this research to be able to assess how technologies should be designed to promote the relevant values. Firstly, the original Payment Services Directive was addressed. Research showed the relative high impact of PSD1 with its incentive for more efficient pan-European payments on the one hand, and limited effects on technological innovation or new actors in the payments market. Thereafter, the content of the revised Payment Services Directive (Directive (EU) 2015/2366) has been analyzed. Incentivized by changing payment habits and shortcomings in PSD1, the revised PSD's purpose is to stimulate innovation within the payments markets which should be accomplished through creating new legal statuses (e.g. AISP). The Regulatory Technical Standards as created by the EBA and ECB is of strong influence in the Directive. It determined the level of technology neutrality which affects, for example, the minimum level of data security through strong customer authentication. Lastly, legislation directly relevant to PSD2 was reviewed. The Data Protection Directive, and its successor, the GDPR, provide principles for integrity and responsible possession and processing of identity relevant information. The

GDPR provides the basic limiting principles of (1) the condition that processing must be for a specified, explicit and legitimate purpose; and (2) the condition that any further processing of data must be for the same purpose as the original one for which the personal data were collected, which are highly relevant for privacy in the case of PSD2.

# 4. Methodology

This chapter elaborates on the methods used in this research to data collection and analysis as well as the units of analysis. It presents the development of the interview procedures, design sets and measures taken in order to safeguard an optimal data collection process. These methods provide the methods used to answer research sub-question 2: 'What is the importance of the values to be reflected by technology designed after PSD2 and what are the main ethical privacy related challenges that PSD2 brings to society?' and sub-question 3: 'How can the most important values be included by design?'

## 4.1. Research methods

This thesis is designed as a qualitative, explorative case study. Aim of this research is gaining a deep and complete insight into several processes which, according to Eisenhardt (1989) makes a case study suitable. "A strength of theory building from cases is its likelihood of generating novel theory. Creative insight often arises from the juxtaposition of contradictory or paradoxical evidence (Eisenhardt, 1989)." The characteristics of a case study, provided by Verschuren & Doorewaard (2010) are as follows: (1) a small domain with a small number of research units, (2) intensive data generation, (3) depth focused rather than breadth, (4) a selective sample, (5) an statement about the object as a whole, (6) open observation on site, (7) qualitative data and research methods (Verschuren & Doorewaard, 2010). This thesis is based on the case study design principles as proposed by Yin (2013) and Eisenhardt (1989).

The process of building theory from case study research consists of eight steps, according to Eisenhardt (1989). These are: (1) define a research question, (2) selecting cases, (3) crafting instruments and protocols, (4) collecting data, (5) analysis of data, (6) shaping hypotheses, (7) compare hypothesis with conflicting and similar literature, and lastly (8) theoretical saturation. Theoretical saturation is optional as, especially in the case of this research, the amount of pre-existing theory is fairly thin (Eisenhardt, 1989).

Yin (2013) constructs a case study research design as to consist of five components: (1) research question, (2) propositions, (3) the unit(s) of analysis, (4) logic linking the data to the propositions, and (5) criteria for interpreting the findings. Also, an exploratory research should have a purpose (Yin, 2013). This is why the following sections in this chapter are dedicated to the defining this thesis' purpose, units of analysis and criteria for success.

## 4.2. Purpose

Because this thesis is set up as an exploratory research, no verifiable propositions are produced. Therefore, purpose has to be pre-defined in order to determine whether the research was successful or not. Based on the theoretical concepts, literature review, research objective and questions, the purpose of this research is defined as follows.

The answer to the main research question should give insight in which values should be reflected in the technology made in response to the revised Payment Services Directive. It should lay a foundation for incorporating knowledge of the ethical impact of products and services based upon PSD2 capabilities. The aspects of PSD2 that are to be considered a societal problem should become clear. Also, several principles for addressing identified problems within the effectuation of PSD2 should be proposed.

## 4.3.Unit of analysis

The unit of analysis of this research (the 'what' that is being studied) is a certain group of actors that will be affected by the effectuation of the revised Payment Services Directive; the ASPSP.

The case of PSD2 is generally considered to consist of four parties involved: The first is the society, which is the owners of current accounts and end users of products and services that are developed after PSD2. It is for this population that PSD2 is made; they are supposed to benefit according to the directive. The second groups of actors are TPPs for which PSD2 was called into life to promote innovation processes. These 'entrants' (TPPs, fin-tech, AISP, PISP, etc.) are the actors for whom the reason of existence is primarily granted by the effectuation of the revised payment Services directive. They are the new market entrants with whom the European Commission aimed to increase industry competition. They are mostly relatively young financial technology companies whose business models are data driven. Thirdly, an important group of actors are the public, legislative and monitoring organizations which are tasked with the responsibility of a proper implementation of PSD2 towards society. The last group of stakeholder is that of the incumbent banks, offering current accounts to society and subject to PSD2.

This last group is the unit of analysis addressed in this research. The incumbent bank is also referred to as ASPSPs or traditional financial institutions. They are typically well funded, private and mature organizations. Incumbent banks are essential to national economic prosperity which requires stability to ensure continuity. For this reason vast amounts of regulation has been put in place to regulate them and organizational structures are geared towards diligence rather than agility. PSD2 defines the ASPSP as banks that hold customer accounts.

## 4.4.Case description

As mentioned above, the cases studied in this research are ASPSPs in the Netherlands. More specifically, established financial institutions with a European or Dutch banking license regulated by either the ECB or DNB offering consumer services and products in the Netherlands. Such services can be savings accounts, current accounts, deposits, mortgages, credit cards, etc. Case studies in this research are NIBC Bank N.V., Rabobank Groep N.V. and 'DutchBank N.V.'. On these Dutch ASPSPs is elaborated in paragraph 4.5: Data collection.

## 4.5.Data collection

No documented data or procedures regarding these challenges are currently available. The data for this research therefore needs to be collected in order to be able to answer the main research question. The primary source of data for this research will be obtained through interviews with representatives of the three units of analysis; retail banks, third party providers and agents of society. The interviewees are selected based on their involvement in the retail banking industry and degree to which they are or will be affected by the consequences of PSD2. The interviewees are selected in such a way that an optimal range of perceptions, anticipations and insights are covered. Including many perspectives increases the variety of data which benefits the validity of the qualitative assessment.

The qualitative and explorative character of this research makes semi-structured interviews the best way to gather data. Semi-structured interviews are used to gather systematic information about a set of central topics, while also allowing some exploration when new topics emerge (Wilson, 2014). As opposed to structured interviews, semi-structured interviews entail guiding a conversation rather than following a script. The interview is guided along an interview guide, which is given in Appendix A: Interview guide.

The interviews are structured out of five parts, i.e. 'Introduction and formalities', 'background', 'structured topics', 'complementary' and 'conclusion'. During the introduction and formalities part things such clarification on the research and anonymization are addressed. In the background part, the interviewee is asked about his/her position to and affinity with PSD2. The third part of the interview, structured topics, is the main section during which the majority of the data will be collected. This section focusses on the main subject of this research; ethical challenges regarding privacy in digital environments. The complementary part leaves room for potential question related to this research but not thought of before. Finally, the interview is ended during in the last part.

The topics to be covered during the main section of the interviews are taken from the literature research and are the following:

- Privacy
- Transparency
- Ownership
- Openness
- Agency
- Freedom from bias
- Security
- Accountability
- Trust

The interview will be consisting of two types of questions, i.e. direct questions and probing questions. Direct questions address the research objectives directly while probing questions allow the interviewees to elaborate on their answers to direct questions (Wilson, 2014). Explicitly mentioning the concepts will be avoided to minimize chances of misalignment or incorrect interpretations. The concepts will be derived from interviews during the data analysis phase. Although explicitly mentioning concepts is avoided, they are kept in mind during the interviews to make sure that enough data on the concepts is gathered.

Only the direct questions are structured beforehand. The probing questions are phrased spontaneously during the interview based on the responses of the interviewees. Therefore, the interview guide only states the direct questions. All interviews are conducted in Dutch language and quotes are translated in to English by the researcher.

The interview is structured is such a way that interviewer's intervention and guidance can be kept to a minimum. This is done by asking broad, open question to be filled in by the interviewee. In practice this is done by first asking the interviewee about what he/she sees as the most troublesome aspect of PSD2. The answer to this question is used as a basis for the remainder of the interview. As upfront it is unclear how much overlap the actors have regarding the values they prioritize, the interview is kept uniform along them (no separate interview guides).

The interviews are recorded into audio files and short notes are made to highlight certain elements during the interviews. These recordings are then saved and analyzed as will be elaborated on in the subsequent paragraph.

Interviewees are approached on behalf of NIBC Bank. As NIBC Bank is affected, like any other retail bank, by the effectuation of PSD2, resources are allocated to research and anticipation. Typically this is done through a combination of internal research and collaboration with external actors. This is convenient for this particular research because this means that internal expertise and external connections are available for data collection. The researcher's internship at NIBC Bank contributes to the accessibility to these resources.

A list of interviewees with their function or expertise within the companies and a short description of the companies are given below. For confidentiality reasons, their names are not explicitly mentioned, but a description of their function within company activities are given instead.

- **Rabobank:** The first interviewee (Interviewee #1) is program manager for PSD2 at the 'Cooperative Rabobank U.A.', a Dutch multinational banking and financial services company with its headquarters in Utrecht. Founded in 1972 it now employs approximately 48,000 FTE. Rabobank is considered a bank of systemic importance. The interviewee has extensive experience with payments project, within the Rabobank.
- **'DutchBank'**: two interviewees (Interviewee #2 & Interviewee #3) are employed by 'DutchBank N.V.', a pseudonym for one the systemic three banks within the

Netherlands. DutchBank preferred to remain anonymous because of press sensitive reasons. What can be said is that DutchBank is listed on the Euronext. One interviewee (Interviewee #2) is tasked with managing long term innovation processes within the DutchBank. Long term strategic projects also includes anticipation to PSD2. The other interviewee's (Interviewee #3) position entailed managing experiments and prototyping, for example supervising FinTechs that are developed in collaboration with, or obtained by, the DutchBank.

- **NIBC Bank N.V.**: The interviewee active within NIBC Bank (Interviewee #4) is Vice President of consumer savings and responsible for marketing. NIBC Bank N.V. is a commercial bank headquartered in The Hague with consumer saving activities in The Netherlands, Belgium and Germany. It employs a total of approximately 670 people and reported a 102 million euro profit over the financial year 2016. NIBC Bank N.V. co-hosted this research project, in collaboration with the TU Delft.
- **Enigma consulting**: is an IT consultancy company with a special focus on digital innovation within the payments industry. It has offices in 11 European countries, approximately 3600 employees and 369 million euro turnover in 2015. The interviewee (Interviewee #5) is partner and at the moment of interviewing active within NIBC Bank in an advisory role.
- **'B2Bpay'**: one interviewee (Interviewee #6) is CCO at 'B2Bpay', which is a pseudonym for a FinTech offering a high-tech specialized payments product, licensed and regulated under the FCA and thus currently also subject to PSD1.
- **Synechron**: a digital strategy consultancy company with a special focus on payments. It has offices in 18 countries worldwide, approximately 8000 employees and 500 million dollar turnover. The interviewee (Interviewee #7) is managing consultant at Synechron in the financial services industry currently focusing on PSD2 and other subjects.
- **Innopay**: a payments, e-business and innovation services consultancy company active in The Netherlands and Germany. The interviewee (Interviewee #8) is partner at Innopay since 2003 and has extensive experience in the Dutch payments industry.
- **Cegeka**: an IT consultancy company with a special focus on block chain and IT infrastructure. It has offices in 11 European countries, approximately 4000 employees and 414 million euro turnover in 2016. The interviewee (Interviewee #9) is expert on block chain and PSD2.
- **Authoriteit Consument & Markt (ACM)**: Dutch national authority for independent supervision on fair competition, telecommunication and consumer rights. Interviewee #10 is active in implementation of PSD2 in Dutch national law. Interviewee #11 is specialized in fair competition in the financial sector.

## 4.6.Data analysis

This section describes how the data gathered is processed into information. The results are discussed in Chapter 4. The data in this research are interviews. The purpose of these interviews is to eventually be able to determine what values are of relevance to in the case of PSD2 in order to answer the main research question. This requires a solid qualitative summary. For this purpose, the data is processed as follows. Each interview is recorded with the consent of the

interviewee and the audio file is saved redundantly. From these audio files will be determined which values are relevant to this research the interviewee touches upon. The presence of a value in the interview is considered to be binary; a value is either mentioned as relevant or not. There is no discretion in between. Determining if an interviewee finds a value to be important is done by looking for aspects and keywords in the interview. The main aspects are extracted from the literature review and keywords for each aspect are derived from commonly linked keywords, synonyms or terminology derived from the interviews.

If a value is found to be mentioned as relevant, it is marked so through the coding analysis. The number of times a value is mentioned as relevant in an interview is converted to indicators indicating the degree to which an interviewee conveyed insights regarding a value. These indicators are presented per case in Table#. A '-' shows that the value was either mentioned as unimportant in the interview or that the value was present in the interview, but no stance or opinion towards the value was observed. A '+' represents the interviewee found the value to be important.

To minimize potential ambiguity during the interpretation of keywords and aspects, claims are supported by quotes where possible. After having mapped which interviewee mentioned what values as relevant, the values will be translated into design principles through the value hierarchy method as proposed by Van de Poel (2014). Further analysis will be conducted by interpreting the results along the knowledge from the literature review and will form the basis for the value sensitive design.

## 4.7.Conclusion

This section delineated the methodologies to find the main ethical challenges that PSD2 brings, validate what values are relevant to technology developed after PSD2 and evaluate the importance of the values. The first iteration is to gain a deep and complete insight into the main ethical privacy related challenges that PSD2 brings to society. The research should therefore be set up as a qualitative explorative case study. Data is collected through semi-structured interviews with eleven experts from three of the four types of stakeholders. The unit of analysis is the ASPSP as defined by the revised Payments Services Directive. Dutch consumer banks in the Netherlands are suited as a case because Dutch payment traffic is one of the most efficient in Europe making the Dutch ASPSPs experienced in digital innovation in finance. The semi-structured interviews are analyzed in a qualitative way, identifying the ethical privacy related issues. Thereafter, the second step is to qualitatively validate the values that were identified in literature. This provides the basis for a part of sub question 2; the relative importance among the values. This is done by scoring the importance of every value mentioned as important in an interview and weighing the scores against each other in a qualitative way.

# 5. Results

In this chapter the results of the ten interviews are presented. The results are given per issue that came up in the interviews, because the interviews had a significant amount of overlap. Each paragraph addresses one issue. Together these answer sub-question two: "What is the importance of the values to be reflected by technology designed after PSD2 and what are the main ethical privacy related challenges that PSD2 brings to society?"

## 5.1. Ethical issues to referential data: control, discrimination, harm

One of the most pressing and at the same time ethical issue is that of the possession of referential data. Information on a current account, transactional data, is per definition always in possession of two or more parties. A transaction may contain several types of identity relevant information. If one of the parties in possession of the particular transaction decides to opt in on sharing that transaction with a third party, the other owner(s) have not given their consent while their information is in the hands of a third party. It may even be the case that if they had known the recipient of the transaction would share the transaction in question, one of the parties in the transaction would not have wanted the transaction in the first place. Theoretically seen it should be possible to completely identify a certain current account's transactions without the owner having given any consent.

"The risks are huge, such as discrimination. If this really happens on large scale than our society will stop functioning because our society is built on the idea that some people are in luck and some are not and a minimum standard of quality in life is for everybody. If transparency increases, the weak of our society may be discriminated, which is an unwanted state (Interviewee #2)." In the latter, interviewee #2 is referring to the situation when organizations such as health care insurance and creditors base their assessment of risk or creditworthiness on an transparent market where the 'weak' customers pay a high premium for their services. The customer is not in control of his/her own reputation anymore. The risk of informational harm however, goes further than discrimination alone. The ethical issue of referential data encompasses all risks that follow from parties without an individual's consent still forming a 'user profile' and acting upon that.

"The DPD offers some of the solution to the referential data problem (Interviewee #8)." Interviewee #8 refers to the main principles of DPD; purpose, transparency, proportionality, access and transfer. The DPD states that information may not be transferred from one storage location to another unless it is for the same purpose as it was stored for in first place. This would imply that referential information in a transaction owned by someone else than that is consenting to the sharing of information may be transferred without the consent of the other owner of the information. In the case of PSD2 this would mean that information owned by more than one party may be transferred to TPPs if a TPP is using it for banking purposes. This however does not directly solve the issue of external parties being able to produce profiles of individuals who

did not give their consent to a certain TPP. Legally this problem is even more complicated as the following quote indicates: "From a legal perspective PSD2 has an inherent problem because payment data almost always has more than one owner. Legally seen, a customer's data on a current account is not even his (Interviewee #1)." How exactly the DPD, its successor, the GDPR, and other legislation will legally affect this ethical dilemma of privacy is outside the scope of this research.

## 5.2. The principle of informed consent

"A challenge to PSD2 is knowing when an informed consent was really informed (Interviewee #5)." Multiple interviewees repeatedly addressed the subject of informed consent. "We know for a fact that informed consent in some situation is a false hypothesis (Interviewee #1)." Deep in the principles of PSD2 is rooted the condition that everything given in the directive is only applicable after an end-user 'opted in', i.e. gave informed consent. If an end-user chooses to 'opt out', under no condition can data be shared with TPPs. Informed consent, as has been defined in the literature review, entails disclosure and comprehension for 'informed' and voluntariness, competence, and agreement for 'consent'. However, several interviewees questioned the validity of informed consent as a way to justify a breach in privacy.

PSD2 stimulates privacy to be traded for benefits. Many contemporary information systems contain implicit tradeoffs between disclosing identity relevant information and receiving some form of benefit (Hirschprung, Toch, Bolton, & Maimon, 2016). "A customer does not ask itself if it is wise to give his or her information to a certain party. Rather, a customer asks itself if he or she wants to use the service or products. Consumers have historically proven that their choice is not based upon if it is morally wise but on if a product is attractive enough (Interviewee #6)." With this statement interviewee #6 was referring to users of Google and Facebook, trading their information for services such as social media, email and mobile operation system (Android). The user gains social benefits through disclosing information but is also exposed to a loss of privacy. One could perhaps rely on the end-users rationality which would entail "maximizing their expected benefits against the possible cost of disclosing identity relevant information if it were not for the intangibility of the concept of privacy, the inherent uncertainty in privacy decisions its context-dependence, and its sensitivity to various biases that make it a challenge to understand the utility and cost of privacy. In this context, uncertainty is prevalent due to limited transparency and the fact that users do not always know how their data will be used, or even how authentic the electronic service is (Hirschprung et al., 2016)." Another concern is the lack of interest of end-users to get familiar with risks; "Privacy is not a customer's priority because negative consequences are not directly evident (Interviewee #1)."

"Giving consent is too easy for it to be the only safeguard. It has proven ineffective in the past. Also, the implications of disclosing payment information are too complex for one to disclose with a single click of the button (Interviewee #3)." However, some interviewees do expect the

principle of informed consent to provide enough of a safeguard for privacy. "We expect customers to be relatively risk averse (Interviewee #4)" interviewee #4 said about their averagely high aged customer base. This implicitly entails the belief that customers are rational; that they understand the risks involved and weigh those against benefits before making the decision to share identity relevant information. "I think the trend will be that data will become increasingly the property of the customer and that it will become up to them if they want to share it and with whom. PSD2 is the start of that trend with the opt-in principle build in (Interviewee #7)."

When asked if PSD2 would change customers' attitude towards sharing identity relevant information, interviewee #6 replied: "My position is that end-users will not change their behavior with PSD2. They have been used to giving away their very sensitive, very valuable data for years now (Interviewee #6)." This is based on the belief that in the perception of the consumer, financial information is not significantly different from information customers are currently used to sharing, i.e. addresses, photos, etc. But not all interviewees share that opinion. For example, "With PSD2 called into life I expect a public debate to rise about who should educate the customer about the use of financial services. That task will likely be allocated to incumbent banks (Interviewee #7)." With 'educating the customer' is meant that end-users should be explained to what an informed consent precisely entails and what the risks are. This brings together the elements of transparency and agency. An individual should have access to the relevant information before making a decision about his/her identity relevant information. Within the debate about the duty of care, retail banks feel like they are responsible for educating the customer about risks to opting in while certainly an argument can be made that it is the government's role to do so. This notion of retail bank's sense of responsibility comes from the expectation that they are the ones whose reputation will be damaged in case of financial damage, as has been defined in PSD2. Government organizations are responsible for onboarding TPPs and licensing them. However, the incentive for ASPSPs to 'educate' the consumer is amongst others the lowered deductible excess (part of financial damage to be paid by the victim) which makes the ASPSP liable for fraud.

Interviewee #2 generally agrees with the researcher's statement that end-users are inclined to overlook long term risks to privacy for short benefits, but shows a different perspective on that. "I think TPPs are far more capable to innovate to the advantage of clients than we [ASPSPs] are and PSD2 takes a good step in that direction. But if we want PSD2 to impact society as hoped for, we should get rid of our 'stay-away-from-my-data' mentality and foster the idea of open innovation (Interviewee #2)." This statement could be interpreted as the notion that limited rationality ultimately benefits innovation and thus the end-user. Interviewee #2 continues with the following statement: "With legislation like the GDPR, people start being aware of privacy issues and things like what the business models of companies like Facebook are based on (Interviewee #2)." The general awareness of privacy related questions might be more effective than the awareness of short term consequences.

TPPs should provide a comprehensible and complete summary of what their services entail through which data in order to promote the value of transparency. ASPSPs should provide their customers with a real-time overview that summarizes which TPPs the customer gave consent. "I think most of all doubts surrounding PSD2 can be solved with transparency. It fosters the realization of what a customer's data is worth and thus who to trust with it (Interviewee #7)."

## 5.3.Sensitivity differences in types of information

The current state of legislation does not distinguish between different types of information. "There are strong differences between the types of data clients use; some are worth more than others (Interviewee #6)." i.e. there can be distinguished between the sensitivity of a type of information. Reijers (2016) dedicated an experiment to finding the most common types of identity relevant information in current accounts. The findings identified the following types of information: names, addresses, social security numbers, credit card numbers, license plate numbers, income/wage, spending categories (preferences and dedicated worth), medical, religious, location, behavioral (events) and social (contacts) (Reijers, 2016). These types differ strongly in nature, sensitivity and situational risk. Information referring to a religion, for example, is likely to be relevant in fewer cases than income.

Also, with the DPD's principle of purpose, a third party cannot ever be in the possession of data which is not used for the purpose of their service/product. This means that the TPP that extracts data through API technology probably will tread carefully with which information to ask consent for. But, it is practically unreasonable to assume that asking for certain data will not ever contain data that has more sensitivity than wanted. Therefore, with the current version of the revised PSD and RTS not addressing the differentiation between types of data, the responsibility of 'cleaning' data will fall to the TPP. Hence, the following quote: "A bank that simply complies to PSD2 will give all information, which certainly does not benefit privacy (Interviewee #5)."

Even though filtering out data is technologically very feasible, some interviewees still propose that end-users should be the ones to have the option to choose between what data they do and do not share due to the ethical aspect of filtering data. "Consumers should have the choice to control the level of abstraction of the data they share. For example, an AIS does not always need to know that I went to the 'Albert Heijn' but may have plenty by just knowing I went to a supermarket (Interviewee #6)." Interviewee #6 speaks about a negotiation-like situation where TPPs ask information and end-users choose which variables to share and to what abstraction those are accessible. For example, instead of giving information to the location and amount of cash withdrawal in an ATM, an end-user could have the option of giving the information that cash was withdrawn at an ATM in a certain timeslot. ASPSPs should provide interfaces that allow for end-users to choose what data to share to a high level of detail in order to promote the value of agency. "There is a difference between giving consent to sharing everything and giving consent to share only certain aspects of your data (Interviewee #7)."

## 5.4.Unregulated forms of data abuse

"Some types of data abuse are not regulated, neither in PSD2 nor GDPR (Interviewee #9)." Interviewee #9 was referring to an indirect risk on sharing data; bankruptcy, mergers and acquisitions. Even though not directly related to PSD2, it does seem to apply in its case. When a business or TPP goes bankrupt, all assets of financial value will be wholesaled to settle the residual debts. In the case of such a whole sale, user data could even be the most valuable asset to be sold. Thus, a company can ensure the integrity of customer data protection practices but in certain exceptional circumstances control over customer data and thus the ability to ensure integrity can be compromised.

A generally accepted notion is that the introduction of PSD2 will foster young, small companies as new entrants in the market to offer PIS and AIS. A well-established business model in startups is creating a large customer base in small amounts of time through superior user experience. However, the fail rate of such young companies is known to be very high. These two traits could thus jeopardize customer's identity relevant data. Another known business model is for a parent company to let a small, legally unrelated spin-off company into the market in order to prove a certain concept or gain experience in a market. These spin-offs are limitedly funded as they have not been created with the purpose of profit in mind and are thus more than average likely to fail. Accountability may be limited due to complex legal structures. Depending on the service/product of such spin-off company, identity relevant data may thus at risk of exposure.

## 5.5.Licensing and supervising of TPPs and ASPSPs

A recurring theme in interviews was the supervision of new entrants and incumbent banks. The uncertainty over the supervision is threefold. Firstly, uncertainty arises from the fact that PSD2 has not been completely finalized yet at the moment of interviews giving room for a discussion about legislation on licensing and supervising of TPPs being necessary at all. Secondly, the legislation regarding onboarding and licensing that has been created until this point is of ambiguous nature. Lastly, roles on supervision of TPPs and their behavior are undefined or suboptimal.

The question if regulation on the onboarding, licensing and supervision of TPPs is necessary arises from the current absence of clear cut standards. At this point in time it is clear that onboarding and licensing for PISPs are the responsibility of the competent national organization which is the national central bank. This legislation however does not originate from PSD2[1]. AISPs are therefore not regulated. To some actors this seems reasonable; "Regulating the integrity of managing end-user data is superfluous because a mechanism of natural selection will

[1] As of the 11th of July 2017, the EBA published its final guidelines on the information to be provided by applicants intending to obtain licensing as PISP, electronic money institutions and AISP under the revised Payment Service Directive. The implications of the final guidelines could however not be included in this research as interviews were conducted before the publishing of this document (European Banking Authority, 2017).

lead to only players taking integrity serious being accepted by the end-user (Interviewee #6)." However, most interviewees agree upon the need for a regulated TPPs market. "Self-regulation in the financial sector has proven quite inapt. Formal regulation is necessary (Interviewee #9)." This together leads to the notion that TPPs have to be supervised, but also ASPSPs; "The general perception of the current situation is that incumbent banks are the ones that know how to properly handle data and PSD2 introduces 'cowboys' into the playing field who get to go wild with your data. Now I do not say the latter is not true, but I do say the former is not (Interviewee #6)."

The second ambiguity in PSD2 is the onboarding and licensing process. "In the end, some kind of onboarding of a TPP should take place, even if it is only a very simple one, but if this should be done by an ASPSP or a regulator, is still unclear (Interviewee #2)." The onboarding process would entail checking for specific variables before giving a license to operate in the EU financial market. For a payment institution (PISP) these are already defined and operational. Requirements for PISPs are amongst others capital adequacy, minimum own funds and ethical conduct of business. Both onboarding and licensing of payment institutions is done by the national central bank. However, legislation does not address the requirements for an AISPs license. Because of the different nature of a PISP and an AISP, requirements for a license should be different. Requirements for an AISP license could be its server location (EU based or not; due to privacy legislation etc.), history of integrity or minimal cyber security measures.

Another aspect of the second ambiguity in PSD2 originates from the responsibilities of licensing and liability of fraud, illustrated by the following quote. "If the competent financial supervisory organization tells us [ASPSP] that we can fully trust the licenses they have granted to TPPs, to what extent are we still responsible for the duty-of-care? We are the first ones that customers come to when something went wrong, while we are expected to hand over data if consent was given (Interviewee #1)." The uncertainty arises from the contradiction that ASPSPs are liable for fraud if a licensed TPP transgresses laws while the onboarding of TPPs is done by the competent national organization, emphasized by the lowered excess deductibles from €150 to €50. Also, ASPSPs are concerned about differences in onboarding and licensing processes between EU members. If licensing requirements differ between members of the EU, TPPs will go to the one with least resistance and discrepancies between the level of ethical conduct of EU member states will come into play. A standardized EU-wide onboarding process for TPP licensing could offer a solution.

The third aspect of ambiguity in the handling of third parties is the supervision. In the case of the Netherlands, for example, the right competent organizations are already in place to supervise TPPs and ASPSPs (DNB, AP, ACM and AFM), but specific tasks and responsibilities have not yet been appointed. Also, some interviewees expect that the number of new entrants will exponentially increase with respect to the current situation making scalable processes within these organizations necessary. The 'open banking culture' in the United Kingdom is fostered by

a sandbox approach of the competent regulatory organization, which entails that new entrants are given a 'light version' of a financial license under strict supervision but this is not a scalable solution. Moreover, ASPSPs are in most situations the first to be notified about fraud and misconduct. Some ASPSPs might even engage in active misconduct investigations of TPPs. However, up until this point in time no protocols for reporting fraudulent activities of TPPs and ASPSPs have not been established.

## 5.6.Rating of values

Table 2 gives the results from the coding analysis as explained in chapter 4. From each interview was determined which values were relevant to the interviewee. If an interviewee mentioned a value as relevant, it is marked so through the coding analysis. The number of times a value is mentioned as relevant in an interview is converted to indicators indicating the degree to which an interviewee conveyed insights regarding a value. These indicators are presented per case in Table#. A '-' shows that the value was either mentioned as unimportant in the interview or that the value was present in the interview, but no stance or opinion towards the value was observed. A '+' represents the interviewee found the value to be important.

Table 2: coding results from interviews.

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | sum |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Privacy** | + | + | + | + | + | + | + | + | + | + | **10** |
| **Transparency** | + | + | - | + | + | + | + | + | + | + | **9** |
| **Ownership** | - | + | + | - | + | + | + | + | + | + | **8** |
| **Openness** | + | + | + | + | - | - | - | - | - | - | **4** |
| **Agency** | + | + | + | - | + | - | - | + | + | + | **7** |
| **Freedom from bias** | - | - | - | - | - | - | - | - | + | + | **2** |
| **Security** | + | + | - | + | - | + | + | - | + | - | **6** |
| **Accountability** | + | + | - | - | + | - | - | + | + | - | **5** |
| **Trust** | + | - | - | + | - | - | - | - | - | + | **3** |

Table 2 shows which interviews reflected certain values, with the outer right column giving the total number of interviewees that have mentioned the row's value as important. The more interviewees mentioned a value as important, the more important the value is considered to be in this research. The 'sum' row thus represents the importance of a certain value.

Table 2 shows that, based on the findings in this research, privacy, transparency and ownership are the three most important values for innovation in the financial industry in the case of PSD2. Privacy was found to be the foremost concern in PSD2, transparency almost as important followed by ownership. The value 'freedom from bias' is the least reflected in interviews but also trust was underexposed. Also noticeable is that openness is solely a priority with ASPSPs.

## 5.7.Conclusion

Chapter 5 answered sub-question 2: What is the importance of the values to be reflected by technology designed after PSD2 and what are the main ethical privacy related challenges that PSD2 brings to society? Through a qualitative validation, the final set of values to be reflected by technology designed after PSD2 is determined. The results of the validation are given in Table 2 and show that privacy is the value of greatest importance to be reflected in technology developed after the revised Payment Services Directive. Furthermore, based on the insights experts brought forward during the interviews, five ethical challenges that come with the implementation of PSD2 were identified. The first is the ethical issue of referential data which entails the unconsented disclosing of a third party's information (current account information on the counter part of a transaction). The second issue is that the principle of informed consent is utilized to justify the trade of privacy for benefits while in some situation this principle may be compromised. The third ethical challenge comes from the fact that PSD2 does not distinguish between different types of data on a current account while some are more privacy sensitive than others. Fourthly, some types of data abuse are unregulated under the current state of legislation such as information transfer in the case of bankruptcy. The fifth and last challenge is the limited legislation for the licensing, responsibility and supervision of TPPs and ASPSPs.

# 6. Value hierarchy

In order to answer sub-question three, "How can the most important value tensions be translated to design requirements?" this chapter is dedicated to the translation of values into design requirements. This is done through the value hierarchy method as proposed by Van de Poel (2014). Firstly, the method will be elaborated on after which it will be applied to the values as determined to be important in chapter 4. This chapter demonstrates the translation of a value to design requirements based upon this method. This also includes addressing the implications to formulate design requirements based upon a limited amount of values that can conflict with other values.

## 6.1. Explaining the method

When a value is found to be important, VSD argues it should be taken into account in the design of the technology in question. This logically leads to the translation of values into design requirements. Because VSD does not include this translation, Van de Poel (2014) proposes the notion of 'values hierarchy'. The process of transforming values into norms and design requirements is a form of specification. This research applies specification because it has determined the important values in previous chapters.

In order to translate values into design requirements, three different levels are distinguished between in a values hierarchy (Van de Poel, 2014). At the highest and most abstract level, there are the fundamental values a person may hold principal such as safety, privacy or autonomy. Disagreements rarely ever come from what institutes a value because abstract values like safety, privacy, and autonomy are likely to be approved. Rather, disagreement comes from how the value is specified into norms. Norms are located at the second level of hierarchy and come in the form of a prescription for or restriction on certain actions. Such norms may include objectives (such as 'maximize safety' or 'safeguard privacy' without a specific target), goals that specify a more tangible target, and constraints that set boundaries or minimum conditions. The bottom level of a value hierarchy, which is also the most concrete one, indicates the technical and institutional design requirements that are derived from the norms. Figure 1 depicts Van de Poel's value hierarchy.

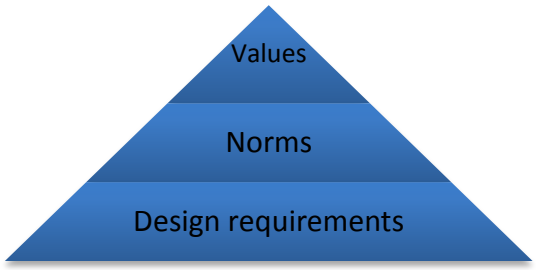


**Figure 1: a schematic representation of the three basic levels of value hierarchy (Van de Poel, Translating Values into Design Requirements, 2014).**

The value hierarchy can be used both as a tool for analysis and design. As an analytical tool, it can help to analyze why, or for what, something is preferred. It can help to explain the values that underlie certain decisions or characteristics in a design. As a design tool, which is the way it is used in this research, the value hierarchy can be used to come up with a design that can bring together divergent values and norms into a coherent set of ex ante design requirements. Insofar possible, stakeholders should be able to confirm that their values are reflected in a service or product, evaluate and judge its validity, and develop an appropriate level of confidence in its output (Friedman, Kahn, & Borning, 2002).

The value hierarchy is chosen for this research because of its top-down character, which is essentially a practice of specification: translating higher level elements to lower levels. This method is applied because the in previous chapter determined values are high level elements to be translated to lower level elements.

## 6.2. Translating privacy into design principles for PSD2

This section combines both results from literature and empirical research; the results of the interviews are combined with the conceptualization of values. The results in chapter 4 indicated that privacy in digital environments was the value of greatest importance to innovation in the financial industry in the case of PSD2. Therefore, this section will work through a value hierarchy to demonstrate the translation of the value 'privacy' into design requirements.

The first step in the value hierarchy is to form a norm out of the relevant value. A norm is defined as prescriptions for, and restrictions on, actions. A norm refers to an end to be achieved or strived for. The end can be a state-of-affairs, capability or an activity. Norms in technical artefacts may refer to properties, attributes or capabilities that should be reflected. This may include objectives, goals and constraints (Van de Poel, 2014). In this section, norms are derived from the analysis of privacy both in literature and empirical research. Some norms also promote privacy-related values. Successively, a design requirement is formed from a norm. Design requirements constitute the most concrete layer of a value hierarchy. These typically state a specific attribute, capability, characteristic, or quality. The design principles formed in this research should be applicable through time and technology development, for the same reasons as the PSD2 is aimed to be technology neutral.

**Norm 1: end-users should be able to make an informed decision and have options in selecting the data's level of abstraction**

The principle of informed consent is strongly reflected in PSD2, proving its importance in the environment of financial innovation. However, the results have pointed out concerns regarding the validity of the principle when an end-user opts-in for a PSD2 related product. The threshold for digital consent could be insufficient for consumers to understand the complex products, procedures, stakeholders and consequences. Friedman et al. (2013) state that in order for consent

to be 'informed', the criteria of disclosure and comprehension have to be met and according to Freier et al. (2011) transparent systems are those that disclose the appropriate information to the user in a form that is honest and comprehensible.. Hence, society would benefit from norms that promote the comprehensibility of consequences that come with informed consent. Furthermore, financial information is in the highest categories of privacy sensitivity (Reijers, 2016). This type of information enables detailed personalized analysis of end-users' behavior and traits in private spheres. Because privacy is conceptualized as, amongst others, the protection from intrusion, interference, and information access by third parties, the disclosure of information should be, at least to a certain extent, in control of the end-user. Hence, society would benefit from norms addressing the end-user's ability to have choice regarding the level of abstraction and variables in the data disclosed. These two notions together lead to the first norm **(Norm 1)**. Norm 1 reflects the value of privacy through the privacy-related value transparency.

The revised PSD and RTS lead to the problem of how to comply in practice with the requirements for informed consent. For instance in the context of emerging flows of information, where AISPs might develop complicated forms of analyses, the end-user is unlikely to comprehend any consequences. The RTS and PSD2 are unclear about how the data subjects should be fully and specifically informed about the complex data processing practices specific to financial (information) transaction. In order to ensure effective protection of the data subject through informed consent, end-users should be informed in a complete, un-biased, transparent and comprehensible way about the data's destination, traits and potential consequences of disclosing giving users the opportunity to opt out or adjust terms. This could be accomplished by showing a summary of certain relevant facts about the content and potential consequences before a data subject is asked for consent. Which variables a data subject should be informed about is subject to discussion and largely dependent on further developments in legislation. Variables that could be relevant are server location (because servers outside the EU might fall under different legislative climates), details on which variables will be disclosed and a TPP's reputation as addressed in Design Requirement 5. In order to avoid unfair competition, ASPSPs could standardize such an informed consent interface across the EU. This together leads to the first design requirement: **systems disclosing data should inform end-users about the consequences, procedures before consenting, preferably in a standardized format throughout the EU (Design Requirement 1, Figure 2)**. An example of what such an informed consent interface could look like is given in Appendix C: Pre-consent information standard.

Results showed a lack of end-user's autonomy reflected in PSD2 legislation in the form of choice regarding which variables to disclose to a TPP. Current accounts contain a vast amount of data each with different characteristics and thus different implications upon disclosure. Variables may differ in time dimension versus static and financial transactions can both be disclosed with and without recipients' accounts enclosed. An ASPSP that does not distinguish between these levels

of privacy does not properly value privacy. For example, a request for disclosure of a static balance at one point in time should be different from a request for balance for each point in time in the last 90 days. ASPSPs should provide end-users of their systems with a flexible 'data disclosing system' that allows them to choose which specific data to disclose. This mechanism for selection should provide the means for end-users to leave out data up level of detail of single fields. The second design requirement is therefore stated as follows. **End-users should be provided with the possibility to select and leave out data they are about to disclose regarding the exact variables and dimension, to a high level of detail (Design Requirement 2, Figure 2)**.

**Norm 2: ex ante privacy assessments should be conducted**

Another notion for including privacy is assess privacy based upon prediction before a service or product reaches the market rather than based upon empirical results. Kizhakenath (2015) proposed ex ante privacy assessment to advance privacy prior to legislative proposals in the case of smart meters in the Netherlands. The norm proposed in this research adds that ex ante privacy assessments, besides legislative proposal, should also add to accountability in products and systems designed after PSD2. Accordingly, the second norm is stated: ex ante privacy assessments should be conducted in order to identify privacy issues before the product or system is implemented and issues are found in practice **(Norm 2)**. In the case of PSD2, most room for implications for legislation by ex-ante privacy assessments are expected in the implementation of the EU directive in national law. Other privacy assessments are proposed in the form of standardized licensing procedures for TPPs and a shared database for those licenses. Norm 2 promotes the value of privacy through the privacy-related values transparency, openness and accountability.

When executing an ex ante privacy assessment for a product or system, guidelines for privacy should be maintained. These could be guidelines in the form of legislation or rules such as the GDPR or the notion of by privacy by design. These are imperatives to analyze and address privacy concerns before they surface. Besides these institutionalized guidelines, society would benefit from actors -especially ASPSPs and TPPs- taking a proactive stance in ensuring privacy of users (Friedman et al. 2013). Hence, the third design requirement: **privacy assessments on designs along established and relevant guidelines and legislation should be utilized (Design Requirement 3, Figure 2)**.

The revised Payment Services Directive recognizes the existence of the PISP and AISP by stating that those TPPs have to obtain a license with the national competent authority. However, results showed that PSD2 relies on existing legislation for the licensing process of Payment Institutions which does not specify requirements for AISPs intending to obtain authorization. When national competent authorities define rules individually, this could potentially lead to AISPs being licensed under different requirements. If this would be the case, AISPs would obtain a license at the least stringent EU member and operate in the entire EU. Therefore the

fourth design requirement addresses this gap in legislation, so that ASPSPs can assume a uniform level of integrity across all licensed third parties: **TPPs should be licensed through standardized requirements across the EU (Design Requirement 4, Figure 2)**[2].

PSD2 requires TPPs to obtain a license in order to operate in the EU market. Once a TPP has obtained a license, an ASPSP is obliged to give automated access to data and payment initiation through the dedicated interface. A suggestion of how these licenses should be kept and made accessible is lacking. Interviewees generally assumed that the responsibility of creating and maintaining a license database logically falls with the competent authorities that are already responsible for the licensing process but this research proposes that that does not necessarily have to be the case. The fifth design requirement proposes that ASPSPs organize, maintain and keep up to date a register for the licenses granted by competent authorities. As ASPSPs should have instant access to the licenses for authorization purposes, a database system set up by them will most likely yield the most effective system with highest compatibility across industry.

Furthermore, such a database could also keep track of a TPPs' privacy and integrity related incidents in order to document a history of integrity. A 'TPP reputation register' could either be integrated in de license database or be set-up as a separate database maintained by ASPSPs. This would enable ASPSPs to do an automated privacy assessment along with automated access to current accounts. Collaboration with the competent supervising authorities across the EU would greatly benefit from such a 'reputation ledger' because of the increased transparency. Also, end-users should have access to a TPP's reputation which adds to the validity of the informed consent principle and transparency. This would also make the fifth design principle an incentive for a TPP's integrity. A reputation shown to end-users upon consent could take the form of a number between 1 and 5 in which 1 means 'barely met the minimum requirements' and 5 means 'amply passed all requirements'. Altogether, the fifth design requirement is: **a database for TPP licenses should be created and maintained by a collective of ASPSPs that includes reputational history and ratings (Design Requirement 5, Figure 2)**. Multiple possibilities exist for the design of such a database, such as centralized through an independent organization representing ASPSPs and TPPs or a closed form of block chain.

**Norm 3: an ASPSP should anonymize data upon disclosing if no consent has been given by all owners of a transaction.**

One of the most pressing issues found in the interviews was that of the ethical issue regarding referential data; the possibility that a data set disclosed with the current account owner's consent contains information that refers to individuals that did not give consent. Multiple interviewees

[2] The EBA's final guidelines on the licensing of TPPs under PSD2 have been published. They state which information should be provided to which competent authority in order to obtain the license for PISP, AISP or e-money institution (European Banking Authority, 2017). However, due to the release of this document after the data collection phase of this research had finished, this document is not included in the results and remaining section of this thesis.

said this conundrum is one that is inherent to the principle of PSD2 because a financial transaction per definition has two or more owners and sharing a ledger with the consent of only one therefore leads to moral issues. The third norm in the value hierarchy of privacy thus concerns restrictions on certain forms of identity relevant information. Warnier et al. (2015) describe the perfect privacy preserving system as one that does not collect, store or process any personal data but also recognize that in the majority of systems this is implausible (Warnier, Dechesne, & Brazier, 2015). In the case of PSD2, systems disclosing data from current accounts should minimize the impact of the information being disclosed on the privacy of non-consenting thirds by anonymizing data. This leads to the third norm: an ASPSP should anonymize data upon disclosing if no consent has been given by all owners of a transaction **(Norm 3)**. Norm 3 reflects the value of privacy through the privacy-related value agency, ownership and privacy.

The corresponding design requirement builds forth on the notion of norm 3. In order to minimize the impact of identity relevant information being released by owners who did not consent for disclosure on privacy, the sixth design requirement states that every owner of a transaction should be able to either consent to the disclosure of its information to third parties or not. ASPSPs should provide end-users with the possibility to indicate which information they allow the recipient of the transaction to disclose to TPPs. The end-user should be able to at least leave out the description and its own bank account number in the financial transaction (shown as option# in informed consent interface Appendix B: Banking environment privacy interface). This together leads to the design requirement formulated as follows: **datasets disclosed by an ASPSP cannot contain data directly referring to a private consumer current account unless both owners have given consent (Design Requirement 6, Figure 2)**.

The practical implications for this design requirement are more or less on parallel with those of design requirement 5. It would require the automated communication of user consent in between ASPSPs. Also, the threshold that will indicate if a 'double consent' is necessary is up for discussion. Intuitively, consumer current accounts are more privacy sensitive than business current account and might thus be eligible for a higher consent threshold, payments amounting to a certain limit might be considered not privacy related and the description given to a payment might be considered more or less imposing to one's privacy depending on culture across the EU. Lastly, which should be the standard setting in a current account is a choice with consequences to privacy. The standard setting could either be 'allowed to be shared' or the most privacy friendly option, 'I do not allow the receiving party of my transactions to share my information to third parties'. The former option promotes a more liberal stance towards privacy perhaps beneficial to innovation and user-friendliness while the latter preserves privacy possibly at the cost of the initial philosophy of PSD2.

Figure 2 visualizes the value hierarchy as formed in the latter sections. The highest level contains the value at stake: privacy. The middle section entails the three norms that were determined to be of importance in the case of PSD2 and their connection with some specific privacy-related

values. The lowest level contains the design requirements as should be applied in systems and products of ASPSPs in the case of PSD2.

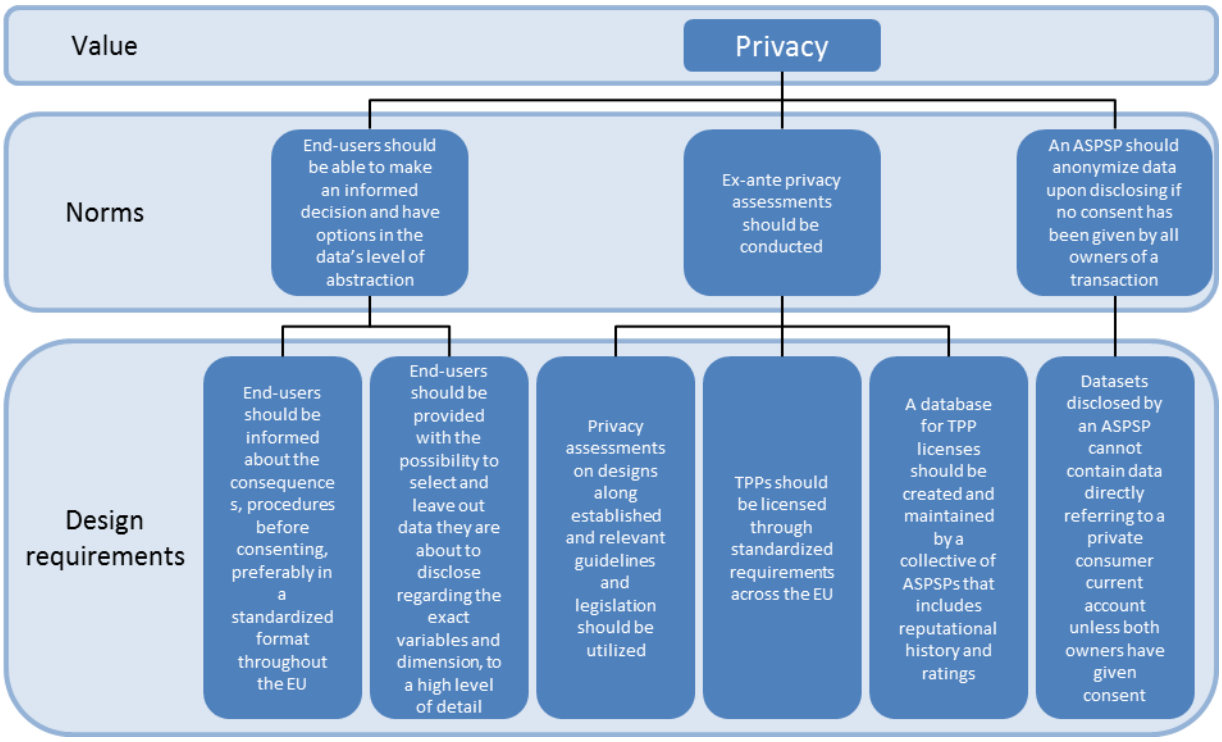


Figure 2: Value hierarchy for privacy in innovation in the financial industry in the case of PSD2.

Aldewereld et al. (2014) have created norms based upon privacy for cookies for internet browsers comparable to the value hierarchy as created in this research. Their results also recognized the importance for consent by the end user and anonymized personal data. The research of Kizhakenath (2015) also concluded that end-users should be informed about the purpose and consequences of the information they disclose though applying the value hierarchy method in the case of privacy for the social acceptance of smart meters in households. Friedman et al. (2006) proposed to promote informed consent by giving users the option on what information is stored and transparency by telling users which information is stored about them through utilizing the VSD approach in designing information systems.

## 6.3.Conclusion

Chapter six answered sub-question 3 as well as sub question 4. Sub-question 3: "How can the most important values be included by design?" was answered by the value hierarchy methodology. The method is used to translate values to design requirements. It is a form of specification in order to promote a relevant value in a technology by design. The applicability of the value hierarchy method to translate values was evaluated. It was assessed with the requirements of Friedman et al. (2015). Concluded was that the value hierarchy method is applicable to measure the importance of values. Therefore, sub-question 3 can be answered with the value hierarchy method.

The answer to sub-question 4: "What recommendations can be made regarding the inclusion of values by design in innovation with respect to PSD2?" was given by demonstrating the value hierarchy method by applying it to the value of privacy in which it turned out to be applicable in the case of systems developed by ASPSPs for PSD2. Six design requirements were formulated based upon three norms for the value of privacy in digital space. These design requirements were formulated through the value hierarchy method in order to promote the relevant value into technologies developed after PSD2. The six design requirements addressed the end-user's ability to make an informed decision for consent, ex-ante privacy assessment through standardized licensing procedures and a shared license database, the possibility for end-users to manage information disclosed through APIs and the limitation of information referring to transaction's counterpart that did not consent.

# 7. Conclusions & Discussion

To conclude this thesis, this final chapter summarizes the results by answering the sub-questions and main research question. Also, the contribution of this research to theory is given and the limitations are addressed. Lastly, recommendations for future research are made.

## 7.1.Conclusion

This thesis has addressed the privacy aspects of the revised Payment Services Directive. It conducted an exploratory study on a selection of incumbent financial institutions in the case of PSD2. Analyzing the case of PSD2 showed issues in the inclusion of values in the design stage of the legislation and moral overload. Therefore, we set our research objective to address the moral residue and find implications to reduce the moral overload.

A main research question was formulated in order to address the moral residue:

**"What general principles for the inclusion of values in innovation within incumbent financial organizations can be derived from the values of stakeholders to optimize the anticipated effects of PSD2 on society?"**

A set of four sub-questions was formulated in order to systematically build to answering the main research question.

Sub question 1: **How can privacy in innovation within the financial industry be conceptualized?**

Several streams of literature were reviewed which yielded multiple literatures (Nissenbaum, 2010; Hirschprung et al., 2016; Van den Hoven, 2008; Nissenbaum, 2004) stating that an interrelated value such as privacy can only be conceptualized in a complex and composed way. This research used the concept of privacy as proposed by Nissenbaum (2004). As privacy is considered a composed concept, related values were identified. These were determined to be ownership, openness, agency, freedom from bias, security, accountability and trust. Also, four reasons justifying the protection of information were found and motivation to implement a responsible approach in innovation within the financial industry were identified.

The Value Sensitive Design method was utilized to redefine the values derived from literature. This approach disclosed the social and moral aspects of the values, which is important for the technologies to promote the relevant values. Gathering the literature and analyzing the legislation and supporting documents enabled us to identify the stakeholders involved. The separation that the Directive makes between stakeholders' intentions turned out to be suitable for grouping stakeholders for the purposes of this research, i.e. government, ASPSP, TPP and each of them also represented society, the fourth stakeholder.

Sub question 2: **What is the importance of the values to be reflected by technology designed after PSD2 and what are the main ethical privacy related challenges that PSD2 brings to society?**

After having redefined the values according to literature and VSD, a qualitative validation of the values to analyze whether these values are applicable and the relative importance between them was conducted. The validation was based on semi-structured interviews with eleven experts on PSD2 from every group of stakeholders. The results of the validation are given in FIGURE# and show that privacy is the value of greatest importance to be reflected in technology developed after the revised Payment Services Directive.

Based on the insights experts brought forward during the interviews, five ethical challenges that come with the implementation of PSD2 were identified. The first is the ethical issue of referential data which entails the unconsented disclosing of a third party's information (current account information on the counter part of a transaction). The second issue is that the principle of informed is utilized to justify the trade of privacy for benefits while in some situation this principle may be compromised. The third ethical challenge comes from the fact that PSD2 does not distinguish between different types of data on a current account while some are more privacy sensitive than others. Fourthly, some types of data abuse are unregulated under the current state of legislation such as information transfer in the case of bankruptcy. The fifth and last challenge is the lacking prescriptions in legislation for the licensing, responsibility and supervision of TPPs and ASPSPs.

Sub question 3: **How can the most important values be included by design?**

The method used to translate values to design requirements is that of the value hierarchy. This method is a form of specification in order to promote a relevant value in a technology by design. This research demonstrated the value hierarchy method by applying it to the value of privacy in which it turned out to be applicable in the case of systems developed by ASPSPs for PSD2. However, because a technology rarely ever depends on the value of privacy alone, the value hierarchy method should also be used to translate other relevant values into design requirements and test for value tensions before implementing the technology into society.

Sub question 4: **What recommendations can be made regarding the inclusion of values by design in innovation with respect to PSD2?**

Six design requirements were formulated based upon three norms for the value of privacy in digital space. These design requirements were formulated through the value hierarchy method in order to promote the relevant value into technologies developed after PSD2. The six design requirements addressed the end-user's ability to make an informed decision for consent, ex-ante privacy assessment through standardized licensing procedures and a shared license database, the

possibility for end-users to manage information disclosed through APIs and the limitation of information referring to transaction's counterpart that did not consent.

The aim of applying the value hierarchy to the value of privacy was to demonstrate how design requirements could be formulated based on important values of PSD2; therefore, the design requirements should be analyzed and evaluated by the relevant group of stakeholders before they are implemented. The design requirements as mentioned above should foster technology that promotes privacy as a value, although they are limited due to the possible, but in this research unconfirmed conflict with other important values.

Answer to the main research question is that privacy is the most relevant value that should be promoted in technology developed by ASPSPs after PSD2 and six design requirements for the inclusion of privacy by design are formed for technology to promote the relevant values for PSD2 to impact society as wished for.

## 7.2.Recommendations

This research used experts from different backgrounds as a source of information to derive, verify and determine the importance of values related to PSD2. However, even though expert of differing backgrounds from every type of stakeholder were utilized, this research might still be biased regarding the priority of values by the choosing this source of data. Highly experienced and often technically well-educated insiders may not strive for the same values as the public at large would. Therefore, research on the values as held by the public at large towards PSD2 should be conducted. For example, a research as proposed by Dignum et al. (2016) who observe that the public debate on a new technology often addresses values or norms in the form of arguments, which are put forward in the public debate. As such the identification of arguments can be used to identify also the values that are specified outside of the circle of insiders (Dignum et al., 2016).

European supra-national legislation is ever evolving. As such, also is the legislation of the revised PSD. The EBA published the final guidelines on the licensing of TPPs under PSD2 after this research finished collecting data. They state which information should be provided to which competent authority in order to obtain the license for PISP, AISP or e-money institution (European Banking Authority, 2017). However, due to the release of this document after the data collection phase of this research had finished, this document is not included in the results. Further research should be conducted in order to determine the implications of this document on the conclusions of this thesis.

Moreover, the revised Directive on Payment Services is only one of several European legislative pieces that have been revised. The Data Protection Directive for example will be superseded by the General Data Protection Regulation, effective simultaneous with PSD2. The GDPR and PSD2 have a large tangent plane on privacy and transparency but this was out of the scope of

this research. Therefore, further research should be conducted on the implications of the GDPR and other legislation on the findings of this research and PSD2 in general. Is the GDPR a solution to the privacy related ethical challenges that the implementation of PSD2 brings?

Lastly, as was already suggested in 6.2, the design requirements as given recommend several fairly complex, cross organization and international systems to be organized. For example, the database for TPP licenses that should be created and maintained by a collective of ASPSPs and includes reputational history and ratings as stated in design requirement 5. A system as this would require instant access by ASPSPs as well as competent governmental organizations and real-time maintenance of content. Furthermore, the system could be set up as a centralized database but does also qualify for an application in block chain. Therefore, further research should be conducted into the practical applicability of the design requirements and what a viable set-up would look like.

## References


Angus, T. (2003). Animals & Ethics: An Overview of the Philosophical Debate. *Broadview press*, 20.

Armstrong, M., Cornut, G., Delacote, S., Lenglet, M., Millo, Y., Muniesa, F., . . . Tadjeddine, Y. (2011). Towards a practical approach to responsible innovation in finance: New Product Committees revisited. *Observatory for Responsible Innovation*.

Barad, K. (2003). Posthumanist performativity: Toward an understanding of how matter comes to matter. *Journal of women in culture and society, 28*(3), 801-831.

Barker, E., Smid, M., Brandstad, D., & Chokhani, S. (2013). A Framework for Designing Cryptographic Key Management Systems. *NIST Special Publication*.

Bertot, J. C., Jaeger, P. T., & Grimes, J. M. (2010). Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. *Government Information Quarterly, 27*, 264–271.

Borning, A., & Muller, M. (2012). Next Steps for Value Sensitive Design. *ACM annual conference on human factors in computing systems* (pp. 1125-1134). New York: ACM.

Council of the European Union. (2015). *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).* Retrieved from http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf

Crouhy, M. G., Jarrow, R. A., & Turnbull, S. M. (2008). The Subprime Credit Crisis of 2007. *The Journal of Derivatives, 16*(1), 81-110. doi:10.3905/jod.2008.710899

Davis, J., & Nathan, L. P. (2015). Value Sensitive Design: Applications, Adaptations, and Critiques. In J. van den Hoven, P. E. Vermaas, & I. van de Poel, *Handbook of Ethics, Values, and Technological Design* (pp. 11-40). Dordrecht: Springer. doi:10.1007/978-94-007-6970-0

Deprez, C. (2013). *Study on the impact of Directive 2007/64/EC on payment services in the internal market and on the application of regulation (EC) no. 924/2009 on cross-border payments in the community.* London Economics. Retrieved from http://ec.europa.eu/internal_market/payments/docs/framework/130724_study-impact-psd_en.pdf

Dignum, M., Correljé, A., Cuppen, E., Pesch, U., & Taebi, B. (2016). Contested Technologies and Design for Values: The Case of Shale Gas. *Science and Engineering Ethics, 22*(4), 1171–1191.

Edgar, T., & Manz, D. (2017). Science and Cyber Security. In T. Edgar, & D. Manz, *Research Methods for Cyber Security* (p. 37). Cambridge: Elsevier. doi:https://doi.org/10.1016/B978-0-12-805349-2.00017-0

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. *The Academy of Management Review, 14*(4), 532-550. Retrieved from http://links.jstor.org/sici?sici=0363-7425%28198910%2914%3A4%3C532%3ABTFCSR%3E2.0.CO%3B2-R

European Banking Authority. (2017). *Final Report in the EBA Guidelines under Directive (EU) 2015/2366 (PSD2) on the information to be provided for the authorisation of payment institutions and e-money institutions and for the registration of account information service providers.* Retrieved from https://www.eba.europa.eu/documents/10180/1904583/Final+Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29.pdf

European Banking Authority. (2017). *Final Report On Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2).* Retrieved from https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf

European Commission. (2010). *Europe 2020 in a nutshell.* Retrieved from eu.europa.eu: http://ec.europa.eu/europe2020/europe-2020-in-a-nutshell/index_en.htm

European Commission. (2015). *Directive (EU) 2015/2366: revised Payment Services Directive.* Official Journal of the European Union.

European Commission. (2015). *Payment Services Directive (EU) 2015/2366.* Official Journal of the European Union.

European Parliament. (1995). *Directive 95/46/EC on The protection of individuals with regard to the processing of personal data and the free movement of such data, adopted October 24 1995.* Brussels: Official Journal.

European Parliment. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).* Brussels: Official Journal of the European Union. Retrieved from http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

Fernandez, A., Giusta, M. D., & Kambhampati, U. (2015). The Intrinsic Value of Agency: The Case of Indonesia. *World Development, 70*, 92-107. doi:http://dx.doi.org/10.1016/j.worlddev.2014.12.020

Fink, G., Edgar, T., Rice, T., MacDonald, D., & Crawford, C. (2017). Security and Privacy in Cyber-Physical Systems. In H. Song, D. B. Rawat, S. Jeschke, & C. Brecher, *Cyber-Physical Systems: Foundations, Principles and Applications* (pp. 129-141). London: Elsevier. doi:http://doi.org/10.1016/B978-0-12-803801-7.09993-4

Freier, N. G., Consolvo, S., Kahn, P. H., Smith, I., & Friedman, B. (2011). A Value Sensitive Design Investigation of Privacy for Location-Enhanced Computing.

Friedman, B., Brok, E., king, S., & Thomas, J. (1996). *Minimizing Bias in Computer Systems.* vsddesign.org.

Friedman, B., Kahn, P. H., & Boring, A. (2013). Value Sensitive Design and Information Systems. In P. Zhang, & D. Galletta, *Human-Computer Interaction and Management Information Systems: Foundations* (pp. 348-375). Londen: M.E. Sharpe.

Friedman, B., Kahn, P. J., & Borning, A. (2006). Value Sensitive Design and Informtion Systems. In P. Zhang, & D. Galletta, *Human-computer interaction in management information systems: foundations* (pp. 348-372). M.E. Sharpe.

Friedman, B., Kahn, P., & Borning, A. (2002). *Value sensitive design: Theory and methods.* Washington: University of Washington technical report.

Friedman, B., Khan, P. H., & Howe, D. C. (2000). Trust online. *Communications of the ACM, 43*(12), 34-40.

Fuster, G. G. (2016). EU Data Protection and Future Payment Services. In G. Gimigliano, *Bitcoin and Mobile Payments* (pp. 181-201). Rome: Springer. doi:10.1057/978-1-137-57512-8_8

Giambelluca, G., & Masi, P. (2016). The regulatory Machine: An Institutional Approach to Innovative Payments in Europe. In G. Gimigliano, *Bitcoin and Mobile Payments* (pp. 3-25).

Gimigliano, G. (2016). *Bitcoin and Mobile Payments: Constructing a European Union Framework.* Siena: Springer.

Haataja, L.-M. (2015). *Payment Service Directive II: Effects on Business Models and Strategies.* School of Science. Espoo: Aalto University.

Haggard, P., & Tsakiris, M. (2009). The Experience of Agency. *Current Directions in Psychological Science, 18*(4).

Halbac, R. (2015). *Digitization of the payment Value-Added Services in the Netherlands.* Delft: Delft University of Technology. Retrieved from https://repository.tudelft.nl/islandora/object/uuid:dd5c0952-89e0-4d5a-818e-fbdbf5d7d32e/datastream/OBJ/download

Heisenberg, D. (2005). *Negotiating privacy: The European Union, the United States, and personal data protection.* Lynne Rienner Publishers.

Hirschprung, R., Toch, E., Bolton, F., & Maimon, O. (2016). A methodology for estimating the value of privacy in information disclosure systems. *Computers in Human Behavior, 61*, 443-453.

Huldtgren, A. (2015). Design for Values in ICT. In J. van den Hoven, P. E. Vermaas, & I. van de Poel, *Handbook of Ethics, Values, and Technological Design: Sources, Theory, Values and Application Domains* (pp. 739-763).

Janssen, M., & van den Hoven, J. (2015). Big and Open Linked Data (BOLD) in government: A challenge to transparency and privacy? *Government Information Quarterly, 32*, 363-368.

Jordaan, Y., & Heerden, G. V. (2017). Online privacy-related predictors of Facebook usage intensity. *Computers in Human Behavior, 70*, 90-96. doi:http://dx.doi.org/10.1016/j.chb.2016.12.048

Kasiyanto, S. (2016). Security Issues of New Innovative Payments and Their Regulatory Challenges. In G. Gimigliano, *Bitcoin And Mobile Payments: Constructing a European Union Framework* (pp. 145-180). Palgrave Macmillan. doi:10.1057/978-1-137-57512-8_7

Kizhakenath, A. (2016). *Social acceptance of smart meters.* Delft: Delft University of Technology. Retrieved from https://repository.tudelft.nl/islandora/object/uuid:570ab4dc-4697-47b8-8363-6c53500b62b1/datastream/OBJ/download

Kleijnen, M., Wetzels, M., & De Ruyter, K. (2004). Consumer acceptance of wireless finance. *Journal of financial services marketing, 8*(3), 206-217.

Kroes, P., & van de Poel, I. (2015). Design for Values and the Definition, Specification and Operationalization of Values. *Handbook of Ethics, Values, and Technological Design*, 151-178. Retrieved from http://doi.org/10.1007/978--94--007-6970-0

Langheinrich, M. (2002). A privacy awareness system for ubiquitous computing environments. *international conference on Ubiquitous Computing*, 237-245.

Le Dantec, C., Poole, E., & Wyche, S. (2009). Values As Lived Experience: evolving value sensitive design in support of value discovery. *27th international ACM, SIGCHI conference on human factors in computing systems*, (pp. 1141-1150). Boston.

Lee, R. G., Petts, J., & Heintz, M. (2013). Adaptive Governance for Responsible Innovation. In R. Owen, & J. Bessant, *Responsible Innovation: Managing the Responsible Emergence of Science and Innovation in Society* (pp. 143-163).

Ligtvoet, A., van de Kaa, G., Fens, T., van Beers, C., Herder, P., & van den Hoven, J. (2015). Value Sensitive Design of Complex Product Systems. *Policy Practice and Digital Science*, 157-176.

Macaulay, T. (2017). Confidentiality and Integrety and Privacy Requirements in the IoT. In T. Macaulay, *Understanding and Managing Risks and the Internet of Things* (pp. 125–139). London: Morgan Kaufmann. doi:http://doi.org/10.1016/B978-0-12-419971-2.00007-8

Malhotra, N., Kim, S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research, 15*(4), 336-355.

Manders-Huits, N. (2011). What Values in Design? The Challenge of Incorporating Moral Values Into Design. *Sci Eng Eth, 17*(2), 271-287.

Manders-Huits, N., & Van den Hoven, J. (2008). Moral identification in Identity Management Systems. *The Future of Identity in the Information Society. 262*, pp. 77-91. Boston: Springer. doi:10.1007/978-0-387-79026-8_6

Marshall, C. C., & Shipman, F. M. (2011). Social media ownership: using twitter as a window onto current attitudes and beliefs. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1081-1090). ACM.

Moody's Analytics. (2013). *The Impact of Electronic Payments on Economic Growth.* Retrieved from https://usa.visa.com/dam/VCOM/download/corporate/media/moodys-economy-white-paper-feb-2013.pdf

Naylor, D., Mukerjee, M. K., & Steenkiste, P. (2014). Balancing Accountability and Privacy in the Network. *SIGCOMM* (pp. 75-86). Chicago: ACM New York. doi:10.1145/2740070.2626306

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Wash. L. Rev.*, 79-119. Retrieved from http://www.kentlaw.edu/faculty/rwarner/classes/internetlaw/2011/materials/nissenbaum_norms.pdf

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy and the Integrity of Social Life.* Standford, California: Stanford University Press. Retrieved from http://www.sup.org/book.cgi?id=8862

Owen, R., Stilgoe, J., Macnaghten, P., Gorman, M., Fisher, E., & Guston, D. (2013). A Framework for Responsible Innovation. In R. Owen, J. Bessant, & M. Heintz, *Responsible Innovation: managing the responsible emergence of science and innovation in society* (p. Chapter 2). John Wiley & Sons.

Pesch, U. (2015). Engineers and Active Responsibility. *Science and Engineering Ethics*, 925–939. doi:10.1007/s11948-014-9571-7

Pesch, U. (2016). *Mapping Sociotechnical Publics for Responsible Innovation.* doi:10.13140/RG.2.1.4050.6480

PwC. (2016). *The strategic implications of PSD2 for Europe's banks.* Strategy&. Retrieved from https://www.strategyand.pwc.com/media/file/Catalyst-or-threat.pdf

Rao, N. (2017). Assets, Agency and Legitimacy: Towards a Relational Understanding of Gender Equality Policy and Practice. *World Development, 95*, 43-54.

Reijers, J. (2016). *Payment Service Directive 2: Dutch supervision on the security and data protection of third party access.* Faculty of Science. Nijmegen: Radboud University Nijmegen.

Schneider, F. (1999). *Trust in cyberspace* . Washington, DC: National Academy Press.

Solove, D. (2002). Conceptualizing privacy. *California Law Review*, 1087-1155.

Tavani, H. (2007). Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy. *Metaphilosophy, 38*.

Tavani, H. (2008). Informational Privacy: Concepts, Theories, and Controversies. In K. Himma, & H. Tavani, *The Handbook of Information and Computer Ethics* (pp. 131-164). Hoboken, New Jersey: John Wiley & Sons, Inc. doi:978-0-471-79959-7

United Nations. (1948). Universal Declaration of Human Rights. Retrieved from http://www.un.org/en/universal-declaration-human-rights/

Van de Kaa, G. (2014). Responsible Innovation and Standard Selection. In K. Jakobs, *Modern Trends Surrounding Information Technology Standards and Standardization within Organizations* (p. 24). Hershey: Information Science Reference.

Van de Poel, I. (2014). Translating Values into Design Requirements. In D. Michelfelder, *Philosophy and Engineering: Reflections on Practice, Principles and Process* (pp. 253-266). Dordrecht: Springer Netherlands.

Van de Poel, I., & Royakkers, L. (2011). *Ethics, technology, and engineering: An introduction.* Oxford: John Wiley & Sons.

van den Hoven, J. (2005). Design for values and values for design. *Information Age*, 4-7.

Van den Hoven, J. (2008). Information Technology, Privacy, and the Protection of Personal Data. In J. van den Hoven, & J. Weckert, *Information Technology and Moral Philosophy* (pp. 301-321). Cambridge: Cambridge University Press.

Van den Hoven, J., Lokhorst, G., & Van de Poel, I. (2012). Engineering and the Problem of Moral Overload. *Science and Engineering Ethics, 18*(1), 143-155. doi:10.1007/s11948-011-9277-z

Van den Hoven, J., Vermaas, P. E., & Van de Poel, I. (2015). *Handbook of Ethics, Values, and Technological Design.* Dordrecht: Springer.

Verschuren, P., & Doorewaard, H. (2010). *Designing a research project* (2 ed.). The Hague: Eleven International Publishing.

Von Schomberg, R. (2011). *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields.* Office of the European Union. doi:10.2777/58723

Waagmeester, F. (2016). *Responsible Innovation in Platform Based FinTech Start-Ups: an explorative study.* Master Thesis, Delft University of Technology, Delft.

Walzer, M. (1983). *Spheres of Justice: A Defense of Pluralism and Equality.* Basic Books. doi:9780465081905

Warnier, M., Dechesne, F., & Brazier, F. (2015). Design for the Value of Privacy. In J. van den Hoven, P. E. Vermaas, & I. van de Poel, *Handbook of Ethics, Values, and Technological Design* (pp. 431-446). Dordrecht: Springer.

Welzel, C., & Inglehart, R. (2010). Agency, Values, and Well-Being: A Human Development Model. *Soc Indic Res, 97*, 43-63. doi:10.1007/s11205-009-9557-z

Wilson, C. (2014). Chapter 2 - Semi-Structured Interviews. In C. Wilson, *Interview Techniques for UX Practitioners* (pp. 23-41). Morgan Kaufmann. Retrieved from http://www.sciencedirect.com/science/article/pii/B9780124103931000028

Wilson, G., & Shpall, S. (2012, April 4). Action. *Stanford Encyclopedia of Philosophy*.

Yin, R. K. (2013). *Case study research: Design and methods.* Sage publications.

Zhou, J. (2001). *Non-repudiation in Electronic Commerce.* Singapore: Artech House. doi:9781580532471

# Appendices

## Appendix A: Interview guide

This appendix contains the protocol followed during the semi-structured interviews as mentioned in Chapter 4: Methodology. The broad layout was derived from the work of Berg (2007). The questions in the protocol questions were derived from the research questions and sub-research questions in collaboration with the first and external supervisor.

**Part 1: introduction and formalities**

1. Introduce self.
2. Introduce the research topic and goals of interview.
3. Ask for permission to record conversation.
4. Inform the interviewee that by continuing he/she gives consent for the data to be used in the research and that their name and company will not be anonymized.

**Part 2: background**

1. Shortly describe your current position and activities.
2. Shortly describe your relation to PSD2.

**Part 3: structured topics**

1. To which of the following values should PSD2 systems/products be designed to?

   **Probe**:

2. Transparency
3. Ownership/property
4. Control
5. Openness
6. Agency
7. Freedom from bias
8. Security
9. Universal usability
10. Accountability
11. Trust
12. Identity

**Part 4: complementary**

1. Ask the interviewee about his/her general opinion on PSD2.

**Part 5: concluding**

1. Ask if the interviewee has any more questions.

2. End interview by thanking for his/her time and cooperation.

The following questions could function as example questions to start a specific line of questioning or to follow up on one above stated main question to keep the conversation going (in Dutch).

- **Wat betekent PSD2 voor uw organisatie?**
- **Welke acties heeft uw organisatie al ondernomen richting PSD2?**
- Wanneer iemand zijn betalingsgegevens afgeeft bevat dit data die refereert aan anderen, zonder dat die daar toestemming voor hebben gegeven.
  **Hoe denkt u dat zou moeten worden omgegaan met dit ethisch dilemma?**
  **Wie is in dit geval de eigenaar van de data?**
  **Tot in hoeverre hoort iemand controle over zijn data te hebben?**
- ING heeft in 2014 plannen gedeeld om klanten data beschikbaar te maken voor derden. Toen werd dit plan op de lange baan geschoven vanwege publieke discussie.
  **Zou uw organisatie vergelijkbare weerstand kunnen verwachten?**
- Data reuzen als Google zien transparantie richting klanten als een steeds belangrijker onderdeel van hun beleid. (rondleidingen door data centra en uitleg over verwerking van data)
  **Hoe belangrijk hoort transparantie over het gebruik van klanten data in uw organisatie te zijn?**
- PSD2 is in het leven geroepen om innovatie te bevorderen. Nieuwe technologie kan nieuw gedrag en verwachtingspatronen creëren.
  **Hoe denkt u dat de publieke perceptie richting privacy zal veranderen met de invoering van PSD2? (ownership, accesibility, transperancy)**
- Wat denkt u dat de belangrijkste [privacy gerelateerde] gevolgen van PSD2 zullen zijn?
- Is er iets wat PSD2 inhoudelijk mist?

- **Wat zijn de voornaamste kansen van PSD2 voor uw organisatie?**
- **Wat zijn de voornaamste bedreigingen van PSD2 voor uw organisatie?**

## Appendix B: Banking environment privacy interface

Figure 3 is an example of what a dedicated privacy environment could look like. This example is designed to represent a privacy tab in a personal online banking environment. It shows to which TPPs the end-user has given consent. Of every TPP that has received consent, information is given in a comprehensive manner.

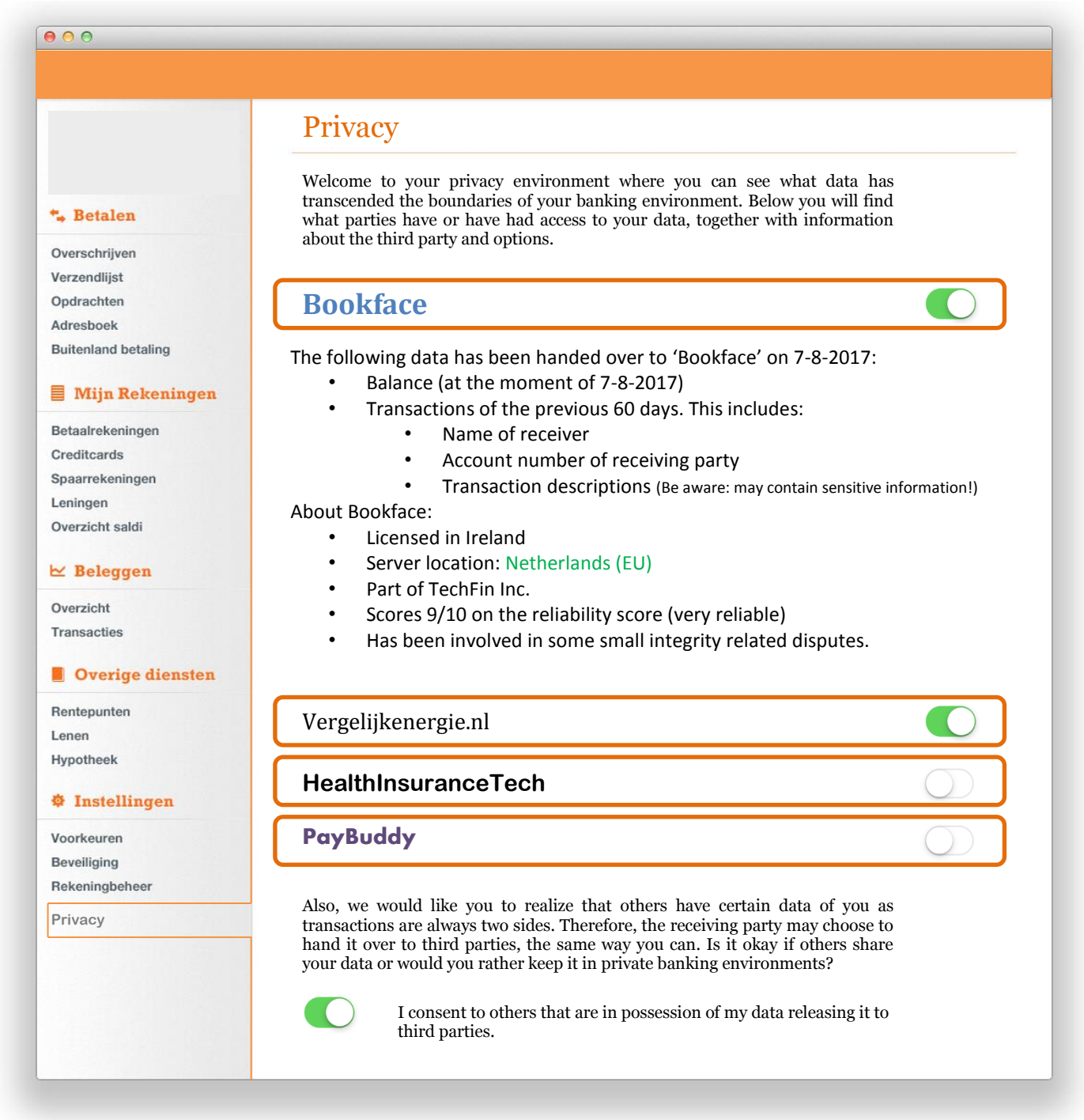


Figure 3: sub menu dedicated to privacy in digital space.

If the period of access to the account is still active, the slider shows green. If the access of the TPP is inactive for any reason, the slider shows grey. The information about the TPP in Figure 3 serves as an example but does reflect in what direction a summary should be designed. The summary of the TPP should contain which variables have been handed over to a certain degree of detail. The end-users should be informed about a decision not only before consent has been given but also after. Also, when variables that are likely to contain exceptionally privacy sensitive information have been handed over to TPPs, a warning should be given after the variable.

Also, on the very bottom of the financial privacy environment, there is a slider that lets the end-user choose if his/her sensitive information may be shared by individuals that have been involved in transactions with the end-user of this interface and are thus in possession of information. To what extent this option should function requires further investigation, but preliminary results have shown that account numbers, names and descriptions could be left out in sharing as the remaining data (amount, date and time of transaction) are in a majority of cases sufficient for the end-goal of which the data was being shared. In order for this option to be possible, a central database containing privacy preferences accessible for all ASPSPs should be put in place. Such collaboration would be complex and costly because of the vast amount of stakeholders in such a system. The design of such database should therefore be researched before recommendations are finalized.

## Appendix C: Pre-consent information standard

Figure 4 shows what an interface for an end-user could look like to be able to make an informed decision. Also, the interface could serve as a platform for the end-user to determine what data will be shared. This interface would be presented to the end-user as a final warning before handing over data to a TPP. Preferably, such a window shown before the data is transferred is standardized throughout the EU.

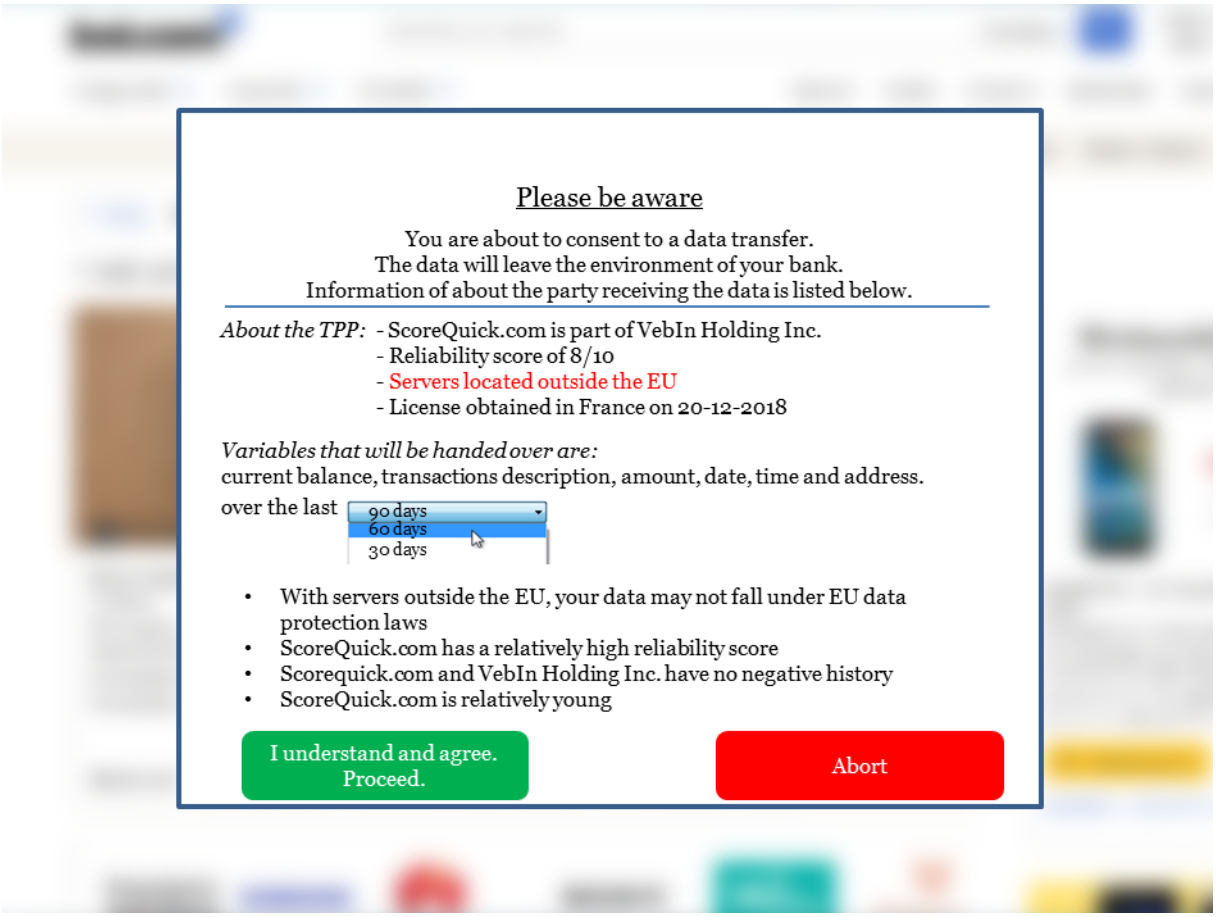


Figure 4: Interface with brief information before client consent to hand over financial data.

As was proposed by design requirement 2, the end-user should have a choice in the data to be shared. The choice in this example is rather limited but it does show the principle of a simple way for the end-user to choose to a detailed level what data to share. More detailed variables, such as transaction descriptions, could perhaps be altered or left out of the exported data set.

Information about the TPP is given, similar to the financial privacy environment as shown in Figure 3: comprehensive and complete. The exact variables shown are indicative and require further investigation but do form an example to what direction such a pre-consent interface should look like.