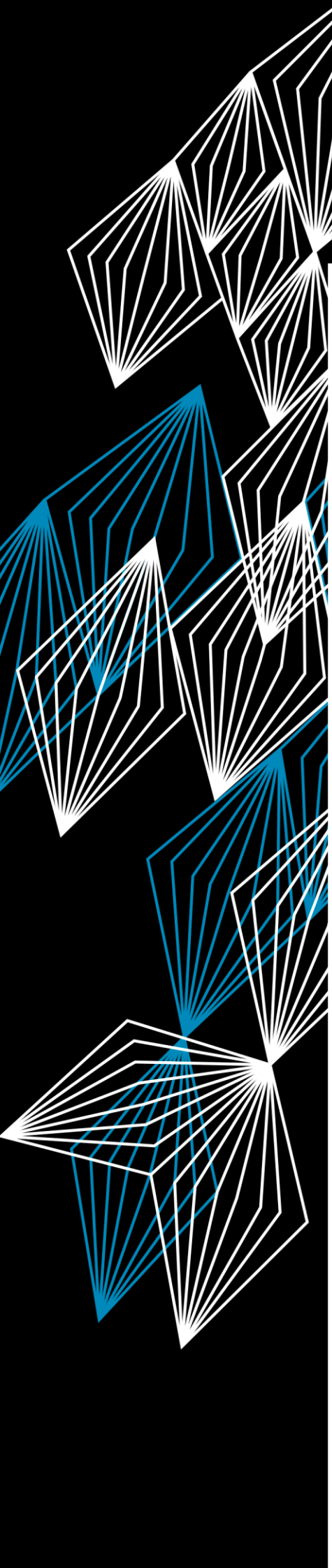


MASTER THESIS

The mediating nature of interfaces on the value and meaning of privacy in the online age

a case study of personal data management

Tanne Francine Ditzel

Faculty of Behavioural, Management and Social Sciences (BMS)

MSc Philosophy of Science, Technology and Society (PSTS)

EXAMINATION COMMITTEE

Dr. K.N.J. Macnish

Prof.dr.ir. P.P.C.C. Verbeek

11th of October 2019

Word count: 19.963

UNIVERSITY OF TWENTE.

Table of Content

Summary

The implementation of the GDPR within Europe has made privacy and personal data a hot topic of debate. As a result, new applications are set up to regain the user's control of his or her personal data. One example is Personal Data Management (PDM). While the intentions of these privacy-enhancing technologies are positive, attention should be paid to their possible unwanted side effects when in use. In this thesis, I investigate the question: "*How are the value and meaning attributed to privacy are mediated through the use of privacy-enhancing technologies such as personal data management (PDM)?"*. First, the definition of privacy is examined through a literature study. I argue that while privacy is correctly defined by limited access theories, the digital age we live in demands more than the concept of privacy can provide. Due to the black-box nature of the Internet, access has become an ungraspable concept for most people unacquainted with its possibilities and restrictions. This, in combination with control focussed technologies like PDM, leads to a shift from access to control as the commonly used interpretation of privacy. The Restricted Access/Limited Control Theory provides a solution by combining the definition based on access and control as tool of privacy. I argue for a layered definition of privacy with a thin core, necessary for political situations, surrounded by the thick cloak, adjusting to the technological environment. PDM interfaces, however, seem to create an illusion of control by provoking the privacy paradox. By reducing the information provided to make the interfaces more "user-friendly" the interface manipulates the users in making unreasoned and subconscious decisions, unknowing what they are consenting to. By looking at the human-PDM-world relation from a post-phenomenological perspective I argue that the interface is key in provoking or fixing the paradox which triggers a reduction in the value of privacy. The PDM interface mediates value attributed to privacy in three ways; 1) The options provided, allowing choice and correction. 2) The amount of information given and reducing the importance of information which is neglected, making users unable to make reasoned and fully informed decisions. 3) The automatic clicking pattern created by the high transparency due to the usability of the interface, which reduces awareness and protection to the possible risk. By designing interfaces with more information on what one is consenting to, guidance, feedback and freedom of choice and correction, the relation is shifted to an alterity relation in which the interface and the importance underlying message is not to be taken as granted. This will break-down the transparency as users are snapped out of their automatic clicking pattern. Three empirically tested PDM pilots proved the existence of these negative effects of the PDM interface. By improving the interface the paradox can also be reduced as suggested. Moreover, it was empirically supported that the meaning of privacy is dependent on technology and context of use.

Introduction

Within our digital age, there is no way around providing your personal data to go about in everyday life. This demand not only stems from official registrations by for instance governmental and private organisations but is the effect of monitoring and storing our behaviour of both online and in the real world. All digitally stored information directly and indirectly concerning an individual can be considered as personal data. Due to the ever-expanding amount of personal data in possession of third parties, the Cambridge analytical scandal and the consequential implementation of the new General Data Protection Regulation (GDPR) within Europe, the privacy of personal data has become a hot topic among the public debate. Due to the new law, people are confronted with their own right to privacy and the previous lack of their ability to control their personal data. The GDPR has enforced the conditions concerning consent, pushing companies to provide easy access to one's data with intelligible terms and conditions using plain language and remove and transfer personal data on the civilian's command (European Commission, 2018).

While these privacy concerning new initiatives seem promising do these actually enhance the online privacy of European citizens? The way to answer this question totally depends on the definition used to describe privacy. Some claim privacy is one of the fundamental rights, an intrinsic value which is needed for other core values such as freedom, democracy, well-being and individuality to be accomplished. However, even after an extensive academic and judicial debate, there is still no consensus of what elements make up the notion of privacy (Solove, 2008). The debate has been split up in predominantly two sides. One attributes the importance of control to secure privacy whereas the second claims that privacy revolves around the concept of access. The control account, most popular within the academic debate, states that one's privacy is violated when one loses control of personal information or space. The access account disagrees as it argues that only by other people actually accessing that same information one experiences a loss of privacy (Macnish, 2018). With the growing digitalisation of our personal information and its vulnerability towards hacking, privacy and control are more essential than ever. It seems as of the digitalisation has shifted the importance of privacy to control. The implementation of the GDPR with its focus on regaining the user's control of his data only confirms this fact. Besides the shift in definition, the value of privacy seemed to have changed over time, with some even arguing about the "death" of privacy (Solove, 2008).

To gain back our "dead" privacy, regulations such as the GDPR have been implemented, which has resulted in the rise of the new initiatives such as Personal data management (PDM). PDM is a movement to restore the user's control over their personal data. The term describes everything related to enhancing the control over the processing of personal data and actual details describing

this data. PDM is often represented as a software tool in which users can access their personal data from an authoritative data source, such as medical and financial documents, and manage which external parties are allowed to have access. The main goal of PDM is to provide the user with ultimate control over their own data. As more and more new technologies will aim for similar results and are very likely to be used on a great scale in the near future, it is of the essence to critically analyse the affordance and constraints surrounding this technology and its impacts on our moral values. For instance, the interface used to enhance one's control over personal data seems at the same time to reinforce the already growing privacy paradox, decreasing the value of privacy. The privacy paradox, a phenomenon which arises in the self-management of privacy, explains the ever more common phenomenon of a significant mismatch between the "individuals' intentions to disclose personal information and their actual personal information disclosure behaviours" (Nordberg, Horne & Horne, 2007, p.100). While people say that they attribute much value to their privacy, in practice there is only little compensation needed for them to give it up. Moreover, one could argue that due to the increased frequency of providing consent due to the GDPR the consent loses its value when it is actually needed (Schermer, Custers & van der Hof, 2014).

The change of course in both the value and the meaning of privacy can be explained by looking at human-world relations and the effect of technology, or in this case how the design of the PDM interface effects this relation and thus change the way we perceive the world. This is done within the philosophical theory of post-phenomenology (Rosenberger & Verbeek, 2015).

Research question & thesis outline

Within this thesis, I answer the following research question; "*How are the value and meaning attributed to privacy mediated through the use of privacy-enhancing technologies such as personal data management (PDM)?"* I will argue that the key lies within the design of the interfaces introduced by PDM. Chapter 1, will largely contain a literature review in which an analytical philosophy approach will be taken. I will first quickly provide an overview of the different conceptions of privacy and explain more thoroughly the control vs. access debate. I will argue in favour of the access account, following the argumentation of Macnish (2018), control is not necessary nor sufficient to secure one's privacy. People can have control over their personal information and space and still have little privacy, as is when allowing intimacy. I will, however, come to the conclusion that in order to describe the case of PDM in its digital context, the access theory falls short. Due to the Internet's black-box nature, the concept of access becomes ungraspable for most people. Moreover, the interface of new digital technologies such as PDM demands a larger focus on the control and self-management side of privacy. The Restricted Access/Limited Control theory (RALC) provides these tools as it expands the access theory by

explaining the management and justification of privacy based on the control account. By analysing the privacy paradox, I will argue that while privacy is indeed best defined as access it does not rule out the significance of the control concept in the context of the digital age. The interface and thus the means of self-managing privacy is essential to which degree the privacy paradox will become present.

Chapter 2 will provide a background in order to better understand the effect of the PDM interface on how the appearance of the privacy paradox leads to the lack of value attributed to privacy in the user's actions. The methodological framework used and described originates from the philosophical background of post-phenomenology. Moreover, it elaborates on how the framework of the value of privacy is affected by PDM and how analytical an continental philosophy can contribute to each other by arguing for a think and thick definition of privacy.

Within chapter 3, the knowledge gained from the two previous chapters will be used and applied to the case study of PDM to test the research question in practice. First, PDM will be explained in more detail, including the two pilot solutions tested. The qualitative method used during the case study will be described and results will be shown. Finally, these results will be discussed in light of the theoretical framework of mediation theory and the definition of privacy established within the previous chapters. As a result of the empirical findings and the discussion an improved interface will be analysed in comparison with the former.

The final chapter will bring the previous three chapters together by attributing the shift in both the meaning and the value of privacy to the design of the PDM interfaces. By going over the implications of our mediated value of privacy I will show the importance of carefully designing interfaces in which amongst others user awareness concerning privacy can easily conflict with the current desire to optimise the usability of the interface. Where interface design has proven to be the origin of the problem, both theoretical and empirical evidence has shown that it is also key in providing a solution.

Chapter 1 Defining Privacy

With the debate on the definition of privacy still going, enriched by multiple disciplines and fields of application, consensus remains out of plain sight. Many have tried to establish comprehensive definitions including scholars from the fields of psychology, legal and behavioural sciences and philosophy. Legal scholar Solove (2008, p. 12-13) argues that all different views found within the debate this far can be arranged under one of the six defined conceptions of privacy; (1) the right to be left alone; (2) limited access to the self, which describes the capability of someone to protect oneself from intruders; (3) secrecy, the ability to keep certain matters inaccessible for others; (4) control over personal information; (5) personhood, which describes the protection of individuality, personality and dignity; and finally (6) intimacy. While the six conceptions do have some similarities and thus overlap they all form a different view on what privacy entails. With numerous definitions out there which all grab little pieces of the whole, one starts to wonder about the necessity of consensus. Macnish (2018), however, argues that now, in a post-Snowden world in which data mining and bulk collection of personal information has become common practice, the need for defining privacy is more of the essence than ever. Due to the limited time and space concerning this thesis, I will not evaluate, compare or criticise the current conceptions of privacy. Instead, I will analyse the two sides of access and control in which the definitions can be categorised. By thoroughly looking at the validity of the access and control account I will argue in favour of the access account as the valid definition of privacy in the context of online information. However, I will also show that the control definition is of better use from a user perspective as limited access can often not be guaranteed when going online. To solve this inconsistency I propose to handle the definition formulated by RALC; the Restricted Access/Limited Control theory of privacy (Tavani, 2007).

1.1 Access versus control

The ongoing debate concerning the definition of privacy can be split into two camps of theories. Dividing the theories into the control account and the access account. Within the debate, the control theories have taken the upper hand and are often favoured by legal scholars. Westin, for instance, takes the control stance by describing privacy as the following; ‘‘claim of individuals . . . to determine for themselves when, how, and to what extent information about them is communicated to others’’ (1967, p.7). There are multiple variations on this definition however all control theorist base their version on one specific criterion for obtaining and remaining one’s privacy: one can only claim to have privacy when the individual in question is in control of their own personal information or space. A loss of privacy is caused by the loss of control over one’s personal information. This definition

seems to correspond with the gut feeling of most people. Because if I cannot control who has access to information about myself, how do I make certain that others are not able to gain insight into things I would like to keep to myself? As Macnish (2018) points out, by losing control one not only feels vulnerable but actually becomes vulnerable due to the increased risk and the inability to secure oneself. As a consequence, one acts as if once's privacy is violated even though this might not even be the case. While no loss of privacy is warranted, a loss of security is. Because privacy protects the right to security, a loss of security often feels similar to an invasion of privacy but is in nature not the same. Moreover, due to the loss of security real harm is caused which in fact might be worse than the harm of losing one's privacy. Macnish provides the example of a diary being left at a public coffee shop by its famous owner. When the owner realises that he is missing his diary he goes back to the coffee shop where he finds the diary in the hands of another customer. There are four possible scenarios which could happen while all having the same condition that control over the personal information in the diary is lost. 1) The customer hands the celebrity back his diary while telling truthfully that she did not open nor has read the diary. In this scenario there is no loss of privacy as she has not read any personal information nor is there a reduction of security as the customer kindly returns the diary. 2) The customer returns the diary however this time, she lies and does not tell the owner about her reading it. This results in a loss of privacy. However, as she has no intentions to follow up on the information read and easily hands over the diary, there is no reduction of the celebrity's security. 3) In this scenario, the customer has read the diary and acknowledges the famous status of the celebrity and the value of his personal information to the press. She blackmails him demanding large pay off to keep her quiet. This time the loss of privacy is not the only harm as the customer's intentions to sell the diary, blackmail and threatens the celebrity causes a large reduction in the celebrity's security. 4) The final scenario describes no loss of actual privacy as the customer did not have the time to read through the diary. However, she acts like she did and threatens to expose the celebrity's secrets with a reduction of security as a result. This example shows that a loss of control does not guarantee a loss of privacy, nor does it necessarily cause a reduction in security even though one might feel that it does.

While most people find the control definition of privacy most intuitive in common use (Inness, 1996), when examining the control theory more closely it appears less intuitive than gained credit for. I, for example, agree with the argument made by Tavani (2007), that it is counterintuitive to our common use of privacy to claim that we can protect our privacy while willingly revealing every piece of information about oneself. According to the control theory, this would, in fact, be possible as long as this choice was controlled by the person in question. This suggests that the control account mistakes privacy for autonomy which certainty is not lesser valued, however not the same as

privacy. Furthermore, the control account does not specify what information one can be expected to have control over and thus is classified as private nor how much control is necessary to keep privacy. Macnish (2018) argues against the assumption made by control theorist Inness (1996) that every personal information is necessarily private. His statement is applicable for both the control and access account. Applied on the former; not every personal information needs to be controlled in order to keep one's privacy intact. Tavani (2007) agrees with this notion as he divides information in "non-public personal information" (NPI) and "public personal information" (PPI). NPI is the information commonly not known to the public and easily considered as private. Sensitive information, for example, one's medical records or financial status can be categorised as NPI. PPI can be described as personal information which can be found out in the open. Examples are: how one looks, where one lives, works or goes to enjoy a meal. According to Tavani, we are able to control the information classified as NPI in contrast to PPI on which control seems to be rather impossible and unrequired to keep one's privacy intact. This distinction between different kinds of personal information is, however, often neglected in control theories.

As argued above, even though it feels similar, control over one's personal information seems not to be equal to maintaining one's privacy over this information. The access account, on the other hand, does describe an accurate definition of privacy. Access or also called limitation theories, argues that privacy is only lost when personal information is actually accessed by others. The example of the diary provided by Macnish shows the validity of this theory. It is not the fact that the customer could have read the diary while the celebrity left it in the coffee shop that caused privacy to be lost. The loss of privacy depends on whether the customer actually read the diary or in other words, accessed the personal information.

1.1.1 The Restricted Access/Limited Control Theory

While the loss of privacy can be correctly defined by the access theory it does not tell us anything about how we can manage or justify the need for privacy. The latter two are needed in order to make the case applicable to the current information technologies and those trying to protect the user's privacy such as PDM. Macnish's example of the diary showed that control is not the concept we are searching for when defining privacy. While this is a convincing argument for the context of the diary, it does not seem to translate to the digital world. Within the analogue world, the information within the diary would be accessed by a human being, violating the privacy of the diary's author. However, this case becomes less clear-cut when changing the situation towards digital information. Instead of the two options of a human eye looking at the information or not, information is increasingly accessed by automated systems or artificial intelligence (AI). In these cases, the information is accessed. However, whether it is also looked at by human eyes remains

uncertain. Within this automatic processing, the link between one's information and the identity of this person often also remains classified as the AI only looks at patterns instead of the individual content. However, whether this really is the case again remains uncertain to the person in question. Moreover, digital information is far more vulnerable to an invasion of privacy as the number of people, or systems, able to access the information through the Internet is far greater than the number of people being able to read the diary found in the restaurant. Besides, since knowledge on the ins and outs of the Internet and its hacking possibilities is scarce and certainly not available to all, a lot of people are left in the dark on how strangers can access their information. Moreover as expressed earlier, the vulnerability caused by the lack of control can cause even more harm to the person in question than the actual loss of privacy. Due to the increasing scale of information being processed without any guidance of human actors and the uncertainty for the user resulted from it, there is an urgent need to protect our fast-growing amount of data in the form of control whether our privacy is potentially violated or not. The digital age thus demands more from privacy than mere access. When looking at access in the context of digital information, it has become an uncertain and ungraspable concept for the common people. From a user perspective, the access theory thus falls short. As the access theory does correctly define privacy, society, or rather the digital age we live in, is by wanting control on their personal data, in fact, asking too much of this particular concept. In order to address the management of privacy, we have to go beyond the concept of privacy. The concept of control, in comparison, is capable of fulfilling these digital needs.

The restricted access/limited control theory (RALC) introduced by Moor (1990, 1997) and expanded by Moor and Tavani (2001) tries to fill in the blanks by combining the definition of privacy provided by the access theory with components of the control theory. RALC theory acknowledges three aspects which are needed to complete an adequate theory of privacy; the concept of privacy, earlier discussed as the definition of privacy, the justification and the management of privacy. I argue that RALC is a suitable theory for describing privacy and its functions in the digital age and provides the tools to protect our growing amount of digital information. RALC theory accomplishes this by excluding control from the definition while still relying on it as a tool to maintain privacy. The definition remains correct while the necessity of control is added to the equation. According to the RALC concept of privacy one experiences privacy: ''in a situation with regard to others [if] in that situation the individual . . . is protected from intrusion, interference, and information access by others'' (Moor 1997, p.30). The context of the situation is in this definition deliberately unspecified, to incorporate a variety of situations in the definition. One situation most relevant for the PDM case is already given by Moor himself: "storage and use of information related to people such as information contained in a computer database" (1990, p.77). Just as the NPI and PPI distinction

made by Tavani, RALC also addresses when information can be controlled. However, contrary to Tavani, Moor argues that it is always the situation, not the kind of information which determines whether or not the information should have norms to protect its privacy. RALC theory distinguishes the situations in which one can have privacy in naturally private and normatively private situations. Naturally private situations are those in which individuals are protected from intrusion, interference or observation by natural obstacles. When one goes on a hiking trip in the woods, for example, this person experiences privacy caused by the natural private situation. According to Tavani and Moor (2001) in naturally private situations privacy can be lost for instance when someone else enters the woods and sees the person in that situation. However, privacy cannot be violated or invaded as there are no conventual, legal or ethical norms to protect one's privacy within this situation. In normative private situations, these norms are set up to preserve privacy from both loss and violation. Take for instance the action of ringing the doorbell to ask permission to enter a house. But besides locations which demand norms so do activities such as voting, certain information and relationships. According to Tavani (2007), these protective norms can be justified to avoid harm to the person in question in the form of embarrassment or even discrimination. Moreover, individuals have the need for control over their life and their data, which includes NPI that, although 'open', need not be shared in some situations. Even though this control might be limited, by providing tools for managing privacy the individual can keep its dignity. These control tools are choice, consent and correction. Choice in which situations one wants others to have access to their presence or information, by choosing to share your personal information on- and offline or staying isolated at home without having social profiles. By providing consent one allows others to access specific personal information in one situation used for a specified purpose. Finally, by correcting earlier provided access individuals need to be able to gain back their privacy when needed. PDM interfaces are one way of providing these management tools.

By providing the case of the Snowden revelations, Macnish (2018) showed the still urgent need to define privacy in a legal context as he does with the diary example. However, I have argued that while access is the correct manner of defining privacy it seems to be a too ungraspable and uncertain concept in the era of the Internet. Where it was previously hard to access secured personal information from for instance paper archives or peek through the window when the curtains were shut, more and more people, companies and institutions have gained the ability to access or hack information due to the digitalisation of personal information. Moreover, especially for the normal citizen, it is harder to detect unwanted access to private information within the digital age. The access part has transformed from a graspable concept in an analogical world to the black box of the digital world we live in today. Due to this black-box nature of the access account and the

ease digital interfaces provide to use the management tools discussed above, the focus is turned to the control side of privacy. While the control theory does not seem to fit the definition of privacy, RALC theory showed that it can contribute to the management and justification of privacy and therefore is a legitimate way of looking at privacy especially in today's digital context. By primarily focussing on control instead of privacy and managing our privacy online these days, the interfaces which are providing the controlling tools in the form of choice, consent and correction have become more important than ever. It is therefore of the essence to analyse these interfaces, to discover how they are being used, what they imply and what kind of behaviour they provoke. Of importance here is the process described as the privacy paradox.

1.2 The privacy paradox

PDM solutions revolve around the management component of RALC's triangle framework. By investigating how people manage their privacy more closely, it might explain more about the user interaction with PDM and its possible reinforcement of the privacy paradox.

1.2.1 Theories behind the privacy paradox

The privacy paradox explains the ever more common phenomenon of a significant mismatch between the "individuals' intentions or attitude to disclose personal information and their actual personal information disclosure behaviours" (Nordberg, Horne & Horne, 2007, p.100). Although people say that they attribute much value to their privacy, in practice there is only little compensation needed for them to give it up. Take for instance the situation in which, providing personal information such as your postal address, e-mail address and date of birth, customers are able to become "member" of a certain retail store. Only a potential 10% discount suffices, to have people give up their privacy.

There has been a number of studies conducted to test the existence of the privacy paradox. The privacy paradox is proven to be present in the context of e-commerce (Acquisti, 2004), social network sites (Barnes, 2006; Hughes-Roberts, 2013; Taddicken, 2014; Reynolds et al., 2011), online shopping (Beresford et al., 2012; Brown, 2001), location data (Lee et al., 2013; Zafeiropoulou et al., 2013), finance services (Norberg et al., 2007) and smartphone applications in general (Egelman et al., 2012). Moreover, there has been a number of attempts coming from different scientific domains trying to explain this growing phenomenon; privacy calculus theory, social theory, cognitive biases and heuristics in decision-making, decision-making under bounded rationality and information asymmetry conditions, and quantum theory homomorphism (Kokolakis, 2017). Cognitive heuristics and biases in decision making are two of the most explored and supported domains. Two examples of these domains are the hyperbolic discounting theory and the affect heuristic.

The former explains the privacy paradox on grounds of the human tendency to attribute less value to future benefits than current ones as preferences change over time. While the intentions of privacy behaviour can be genuine, preferring the benefits of privacy above the benefits of providing personal information, they are future-oriented. At the time of the actual decision making, future benefits are now discounted more than previously was the case, making the person in question value short term benefits of providing the information over the long term benefits of privacy protection. The privacy paradox is thus explained by the human inability to remain consistent in their preferences over time and thus are unable to predict the decisions they will make in the future (Acquisti & Grossklags, 2003). When applied in the case of PDM the ease of control which the tool provides overshadows the actual caring about the exchange of personal data and with that the loss of privacy. Moreover, as I will discuss to more extent in section 1.2.2, there is a significant lack of both short term and long term information to base this short-term decision on. People are not aware nor informed about the possible risks of their decision-making process, letting them make an irrational balancing of their interest instead of escaping the privacy paradox.

Affect heuristic is one of the behavioural biases present in human-decision-making. It describes our fast judgement making due to its associations with things we like or dislike. Resulting in underestimating risks associated with positive affect and overestimating risks with negative affect. The more common a phenomena, the more we tend to associate it with a positive affect (like enjoyment or trust) resulting into providing personal information instead of seeing the actual value of the privacy risk at stake. Therefore interfaces which are specially designed to provide a good feeling and have optimal usability, creating a positive affect due to the ease of usage and familiarity, are more likely to enhance the privacy paradox in which users underestimate the risk of providing their personal information (Slovic et al., 2002; Wakefield, 2013). I argue that this is indeed the case with PDM solutions. They aim to develop a user-friendly interface which provides easy control on the user's personal data and who is allowed to access them. By creating this user-friendly interface which resembles many interfaces which we often use, users associate providing consent with a positive feeling. Due to this positive affect, users underestimating the associated risk of providing their personal data and giving up this part of their privacy.

Both theories show that the privacy paradox leads to the irrational balancing of our interest, underestimating the risks of our decisions and therefore making unreasoned ones. These two theories account for why these unreasoned decisions are made but that does not imply it to be good or acceptable. While the privacy paradox has been around for some time, we should become more concerned about its effects due to the rise of decision making done through uninformed interfaces. Due to the active consent provided through the PDM solution, there is potentially no invasion of

privacy. In fact, there is legitimate access to a specific piece of personal data for the cleared actors. This is where the consequences of the irrational decision made under the influence of the privacy paradox become problematic. Interfaces such as those used on PDM solutions are deliberately manipulating the user in providing consent. Where if the user had enough information to foresee future consequences and events, he or she had not made this unreasoned decision. As the phrase, informed consent already implies, consent needs to inform on its consequences allowing the user to understand the complete process and his own actions. This given information provides the user to take a pause for reflection (Schermer, et al., 2014). This moment of reflection and understanding of what it means to consent is essential in making a reasoned decision, without being persuaded by the biased interface (Dourish & Anderson, 2006). Without this simple pause, users are making a snap decision based on the principles of the privacy paradox such as heuristics and inability to correctly weigh out the short term and long term benefits and risks. Moreover, the Affect Heuristic theory shows how the PDM interface manipulates the user by masking the possible risks of losing one's privacy by its ease of control and its smooth design. In both cases, the issue lies within the design of the interface. By designing an interface in which users are more informed, visualize feedback, promote balanced transparency and are less smooth or conventual designed, users will be snapped out their unreasoned thinking by taking a moment to reflect on their decision making and their trust in the algorithmic interface (Dourish & Anderson, 2006; Kizilcec, 2016). In the following section, I will address this notion further and explain in more debt why notice and consent are not enough to secure an informed, conscious and reasoned decision.

1.2.2 Why notice and consent are not enough to make a reasoned decision

A consent request is a meaningful tool to provide control and awareness: it provides a moment of reflection on the possible consequences as "a consent transaction functions as a warning that a potentially harmful or legally meaningful moral transformation will take place that requires the (undivided) attention of the individual." (Schermer et al., 2014, p.172) While its good intentions the privacy paradox discussed above and another, even more concerning paradox, show the downsides of consent. Hull (2015) refers to second paradox as; "the self-management model of privacy embedded in notice-and-consent pages on websites and other, analogous practices can be readily shown to under protect privacy, even in the economic terms favoured by its advocates." According to Hull the justification of the self-management side of privacy is based on two wrong assumptions. First, it assumes that privacy preferences are based on the rational behaviour of the individual. Second, that this rational behaviour corresponds with the individual's actual preferences. Both assumptions already have been falsified by explaining the theory behind the privacy paradox. However, Hull describes three more reasons why privacy self-management under protects privacy,

which will help to understand the counter effects of tools provided by the digital interface even more: 1. Users do not and cannot have the accurate (both correct and enough) knowledge to know what they are consenting to. 2. Users have difficulties in realising their privacy preferences through the interface. 3. The increasing inability to participate without providing one's private information. Besides, Schermer et al. (2014) warn for a consent transaction overload. Because of these points even when consent and notice are provided, users are still unable to make a reasoned decision. I will explain these notions in more detail.

Lack of information

By reading this header "lack of information" people will often counter with the argument that in most situations information can be read in privacy policies. However, there are a few problems which come with that. Hull (2015) argues for example that these policies are often set up to be as vague and long as possible and can be changed to benefit the company wishes. This information overload in combination with the many privacy policies faced when going online makes it impossible for the user to inform themselves (Schermer, et al., 2014; McDonald & Cranor, 2008). And, even if this is changed by the implementation of the GDPR, which demands every policy to be written in clear and understandable language while still keeping the word count short, there still remains a structural information asymmetry. "Despite lengthy and growing terms of service and privacy, consumers enter into trade with online firms with practically no information meaningful enough to provide the consumer with either ex-ante or ex-post bargaining power. In contrast, the firm is aware of its cost structure, technically savvy, often motivated by the high-powered incentives of stock values, and adept at structuring the deal so that more financially valuable assets are procured from consumers than consumers would prefer." (Hoofnagle and Whittington 2014, p.640–641). Moreover, due to the expanding use of data mining, websites themselves do often not even know how likely and in what sense the data will be used at the time of asking consent. It is therefore rather impossible for the user to know what they are consenting to. (Hull, 2015; Schermer et al., 2014). Furthermore, users are often unaware of the value of their data to others, making them assume that their data will not be used. The study by Boyd and Crawford (2012) for instance showed that one 'Like' on Facebook could predict numerous valuable data about an individual. 'Hello Kitty Likes' predicted the individual likely to be emotionally unstable, to score low on conscientiousness, to be open of nature and to have voted on the democratic party in the US. The initial shared data, the 'Hello Kitty like', might in the eyes of the user not seem valuable for others in particular companies. The data generated from the shared like, however, can so be used to benefit companies to a large extent. These lessons can be learned from The Cambridge Analytica scandal. Users thus willingly provide their data without being able to keep the consequences of the derived usages in

mind. This example shows that it is rather impossible for the user to weigh the costs of sharing information online while the benefits are often out in the open, provoking the privacy paradox even more.

Difficulty actualising preferences

When there is good incentive to arrange once's privacy preferences, the act of doing so often seems to take quite some time and effort. Users are often unaware of the ability to change their privacy preferences, and when they are they often lack the information on where to do so. When these privacy preference interfaces are finally found, the interfaces turn out to be hard to get through or require opt-outs for every privacy option or advertising company individually. While this provides the user with more freedom of choice it often functions more like a burden as there is often no opt-out all button available. Too many choices of consent can also work contrary, as it makes it more difficult for the user to effectuate their privacy preferences (Hull, 2015; Schermer et al., 2014).

This issue portraits the importance of how the interface used is designed. Small changes such as aimed for in privacy by design, can make or break the ability of the user to actualise their privacy preference. For example, the interface could be designed to have all the privacy-protective options on instead of off and to have the ability to set them on and off one by one and collectively. Or in the case described in the previous subsection, while not completely fixing the information a-symmetry, clarifying and reducing the information to its essence and providing warnings to make the user more informed. Besides, these little changes in the design of the interface can distinguish between active reinforcement or discouragement of the privacy or self-management paradox.

Impossibility to decline usage

One issue which is faced most often is the inability to participate without providing one's private information. This is most often the case with "free" online services which rely on customer data for their business model (Schermer et al., 2014; Custers, 2001). This makes the unconstrained or uncoerced nature of consent questionable. With almost every website logging, tracking or asking for personal information it becomes impossible to not disclose any private information. Besides the absolute necessity usage of the Internet to go around living there is also tremendous social pressure to use online services and social media. The social costs of not participating are often way too high to even think about preserving one's privacy, making the choice of consent less of a choice (Ellison et al. 2007).

Consent transaction overload

By making explicit consent the standard, the GDPR implementation has resulted in an increased frequency of people encountering consent transactions. Schermer et al. (2014) however argue that this frequent use of explicit consent lowers its value and effectiveness. This creates tremendous

privacy problems for situations in which explicit consent is actually of the essence. They refer to the Jolls and Sunstein study (2006, p. 212) which shows that often showed messages are likely to be tuned out by consumers. Moreover, Böhme and Köpsell (2010) empirically proved that the more consent boxes resemble end user license agreements, on which users are accustomed to clicking without thinking, the easier users provide consent. The implementation of the 'cookie law' provides a good example of these findings. Schermer et al. (2014) therefore argue for a reduction of explicit consent, only to be used when it involves serious risks and consequences, transforming many situations into an implied consent by going online.[1] I would add that it is of the essence to avoid consistency of consent interfaces and in particular between those of high and low importance by adjusting interfaces to the situation at hand.

What is clear is that the privacy paradox is ever-growing and reinforced by the digital technology of today, even within privacy-enhancing technology. While notice and consent tools are put in place to enhance user's control on their personal data it is not sufficient to secure one's privacy. In fact, this gained control through tools such as notice and consent is rather an illusion and creates a false sense of trust (Schermer et al. 2014). While the issues addressed in this section will never be completely solved, changes within the design can come a long way in reducing or shaping these issues of information asymmetry, difficulty in actualising preferences, impossibility to declining usage and consent overload. As details within interfaces and context seem to be crucial to its existence and severity, they need to be taken seriously and reanalysed in order to minimise the paradoxical effect within privacy-enhancing technologies such as PDM.

[1] Schermer et al. (2014): "Consent is implied in those situations where there is no clear expression of consent, but the behaviour of one person may lead another person to (reasonably) believe that consent has been given"

Chapter 2 Theoretical framework: Mediation theory

Chapter one on the definition of privacy and the privacy paradox shows a change of course in both the meaning and the value of privacy due to the digitalization of our personal information and the tools used to manage these. How this shift appeared can be explained by looking at human-world relations and the effect of technology on this relation. In order to analyse the role of the interface in bringing forward the privacy paradox, I will use the post-phenomenology approach established by Ihde (1990) and extended for mediating moral values by Kudina and Verbeek (2018). Within section 2.2 I will firstly investigate the micro-perspective, revealing the potential user-PDM relations and its consequences on the value attributed to privacy by looking at the user-technology interaction. Next, within section 2.3 I will take a step back, examining the macro-perspective of the social shift of privacy and the tension with the established definition explained by limited access and the interpreted meaning developed by the online world.

2.1 Post-phenomenology

Post-phenomenology resulted from a critical evaluation of classical phenomenology and Science and Technology Studies (STS). Classical phenomenology, while appreciated for its philosophical analysis, was criticised on its romantic and abstract way of analysing technology. While the work of phenomenologist Heidegger can tell us a lot about the ways in which technology is capable of alienating human beings from themselves and the world, it falls short when wanting to describe and explain how people experience technology and how they interact based on this experience. And while the empirical approach of STS tries to solve this problem to some extent, it fails to reconnect the empirical answers found with the philosophical questions asked (Rosenberger & Verbeek, 2015). Post-phenomenology combines the strong characteristics of both approaches whilst eliminating the downsides of each. By going beyond classic phenomenology, which focusses on describing the world and technology as an abstract entity, the post approach focusses on the specifics of each technology individually. This allows for careful analysis of its unique interaction patterns and the relation between human beings, the technology and the world we live in. Another important trait of the post-phenomenological approach is its critical attitude towards the subject-object dualism of modernism; the human subject is always interconnected with its objects. Experience in itself cannot exist (Rosenberger & Verbeek, 2015). If there is no content to our thought, there is no meaning in thinking. While objects can exist in themselves to give them real meaning they have to be experienced.

According to post-phenomenology, one must not look at a possible divide between subject and object. Instead, one must focus on how the world is formed by the intentional relationship we as

subjects establish with objects. Ihde (1990), who can be considered as one of the founding fathers of post-phenomenology, has developed a methodological framework in which these intentional relations can be analysed. According to Ihde, these relations between subject and object, that is human beings and the world, are indirect relations shaped by technology or more general, artefacts. Moreover, it is an intentional relation: this form of mediation through technology is attributed as the origin of the specific way the subject and object present themselves in this situation. In analysing these mediated relations Ihde speaks about two different forms of experience; micro- and macroperception. The first, microperception captures the bodily experience through our senses. I, for instance, see my computer screen at this moment. However, there is a second meaning of perception or the verb "to see". The macroperception captures the cultural and anthropological dimensions the experience. It refers to the interpretation of objects within its context. Take for instance the phrase "After knowing her background story I see her completely differently." The word "see" refers here to the interpretation of a girls image which is shaped by information concerning her background. Just as subject and object, micro and macroperception cannot exist without each other. In order to interpret an experience or perception, there needs to be one at hand. Besides, a complete objective perception does not exist. When speaking of an unmediated perception Ihde does not refer to perception without interpretation (micro without macroperception) as this is non-existent. He, however, means a microperception which is not mediated due to the interference of any artefact (Verbeek, 2005).

Post-phenomenological analysis can be done in two separate ways of looking at the human-technology-world relations; either focusing on the experience or on the action. The first approach is called hermeneutic-phenomenological, analyzing the "human-world relation in terms of the way in which the world can present itself to human beings and becomes meaningful."(Verbeek, 2005, p.111). It describes interpretation and meaning, explains the mediation of experience by technological artefacts. The second approach, characterized by its existential-phenomenological perspective, analyses the way in which humans realize themselves in the world. It describes human activity mediated by technologies. Technologies are not neutral, but in fact mediate the relation between the user and their experience and action (Verbeek, 2005).

By analysing these human-technology-world relations one can come to understand how our daily life is shaped by the technologies we use. How do they mediate our actions, experiences, choices, politics and even our moral values? Or more importantly, what actions, experiences or values does this mediated relation reveal into our awareness or conceal into the background? Otherwise put, what consequences do these mediated relations have on our world and the way we live in it? With

this empirical approach, one is able to really zoom in on one specific technological artefact in order to analyse it in its practical environment of use (Rosenberger & Verbeek, 2015).

2.2 Mediating human-world relations

Within this section, the methodological framework of human-technology-world relations developed by Don Ihde will be discussed more thoroughly. Within his initial framework Ihde (1990) distinguishes between four different forms of technological mediation; embodiment, hermeneutic, alterity and background relations. By understanding these different relations one can obtain more insight into the experience and actions the relationship reveals or conceals. By explaining each relation in turn I argue that one of these concealments of the human-world relation mediated by PDM is the privacy paradox. Post-phenomenology does not explain what the privacy paradox is but does help in establishing its manner of presenting itself. In this way the privacy paradox will become visible in practice, showing what triggers the phenomenon in order to gain knowledge on how it can be reduced in the case of PDM.

To analyse the interaction of the user with the artefact and I first have to define the artefact at stake. The PDM software is handled either on a computer or smartphone. However when basing the analysis of the relations on these artefacts one would presuppose that any program used on smartphone or computer would result in the same concealments and revealments due to the mediated relationship between the user and the world. Assuming that Facebook mediates in the same manner as Microsoft Word. This is of course not a reasonable assumption nor conclusion. Moreover, while a laptop or smartphone might serve as a paperweight, its intended use can only be established with the presence of software. So instead of focussing on the hardware, we should take the software into account. Or more specifically, the interface of the software. The interface is namely the main component which creates the distinction between different software programs from a user perspective. The interface imposes certain actions and thus forms of usages by providing the tools to do so. If the interface leaves out certain tools, the use becomes more limited. It is the interface which allows people to use the artefact.

2.2.1 Embodiment

The embodiment relation describes how actions and perceptions with and of the world are shaped through the usage of technology. By using the technological artefact the user becomes one with the technology. Due to this embodiment, the user acts or experiences through the artefact, making it a part of oneself as an extension of one's senses or body.

Instead of a "normal" mediated perception which is schematized as follows:

I-Technology-World

The embodiment relation takes the following shape:

(I-Technology)→World

One famous example of Merleau-Ponty (1962) describes the extension of bodily perception through a blind man's cane. The blind man does not feel the cane itself, it feels the pavement through the cane; the artefact has become transparent. The embodiment of the cane conceals handling it by transferring the action of holding and feeling the pavement with the cane and the cane itself into the background, away from the user's conscious awareness. On the other hand, the relation reveals the new sensation of sight perceived through the cane. Verbeek (2005, p.125-126) describes three conditions to be met for an artefact to become transparent. First, the artefact must be able to serve for the aimed action or perception in order to be embodied. The physical properties thus must allow transparency. Second, the embodied perception requires a skill which must be learned. Only after the habituation process is completed, the perception becomes automated and transparent. The notion of transparency does not function as an on and off switch. Instead, transparency can be described as a context-dependent range of an artefact from being completely in the foreground and thus the full awareness of the user, to becoming fully transparent. Third, the mediated perception should be measurable in comparison to an unmediated perception.

By using the PDM solution the action of providing consent is acted through the tools provided by the interface. The PDM interface invites users to make this choice whether or not to provide the application and third parties with access to their personal data. However, it also inhibits users to edit the characteristics of this data transfer when wanting to make use of the third party's services which are in need of these data to be transferred. Moreover, the interface inhibits the user to make use of these services when no consent is given. Furthermore, the perception of the situation concerning the significance of providing consent and the importance of one's privacy concerning personal data is transformed. The interface reduces the context of the situation and certain moments of reflection which are normally present when deciding whether or not to unclose private data. When providing consent by signing documents, the user is asked to read the provided information and to understand what one is consenting to. Moreover, in more critical situations a notary or anyone else who has the responsibility to make sure that you are making a well informed and voluntary choice is often present. This authority present at the moment of consenting relates to the context of the consent request. In addition, it creates extra pressure for the user to take the case seriously, take his time to read the information and to reflect on this in order to make a conscious and well-informed decision. This informed and reflected context-dependent decision does not seem to be present in the case of the PDM solution.

The main problem lies within the transparency of the interface. Because we use similar interfaces on a daily basis the skill to master the usage of the interface is highly developed resulting in a highly transparent interface. The more ease, comfort and familiarity the interface provides the more transparent the interface becomes. The usability of the interface thus places a tremendous role in making the interface transparent and enforcing the privacy paradox. Users are withdrawn from the actual information provided by the interface, the underlying risks and consequences of their decisions. Instead, they are focussed on the act of using the interface; clicking through the interface to quickly acquire their goal of getting access to the third party's services. Due to the easy and familiar interface, people do not feel the urgency to take a moment to reflect on the decision of providing consent and its possible risks. Only when the usability of the interface is broken down the interface, its detailed information and importance reappear into the awareness of the user. The problem with today's interfaces, however, is the increased focus on making the walkthrough as easy as possible. This implies leaving out long pieces of text, warnings, pop-ups and other inconsistencies which are essential in breaking down the transparency. The trend of enhancing usability is, therefore, reinforcing the privacy paradox, as the mediating nature of the interface shapes the reckless way of acting on one's privacy and therefore the value attributed to privacy.

2.2.2 Hermeneutic

The second relation, the hermeneutic one, also describes the human relationship with the world through technology. However, in this case, the technology itself does not become transparent as it does in the embodiment relation. Instead, it provides a representation of the world.

The hermeneutic relation takes the following shape:

$$I \rightarrow (\text{Technology-World})$$

For instance, by the means of a thermometer, we perceive the temperature while no action of sense is involved. The specific 'language' of the thermometer needs to be interpreted before perception can take place. The skill of reading the display works in the same manner as the transparency described with the embodiment relation; the more common the language is to the user the easier the language is interpreted or 'read'. In the case of the thermometer, the technology mediates the way we interpret the world; instead of sensing a change in weather, we read the change in specific degrees of Celsius or Fahrenheit. Due to this mediated interpretation of the world, we can view the world and the importance of it completely differently. Moreover when the transparency process becomes completely habituated the dependency on the artefact increases. As we rely more and more on degrees Celsius showed upon the thermometer or our smartphone application we rely less on our bodily senses to experience the weather. These days more people check 'Buienalarm' (Rain

shower alert) whether and how dense it is raining instead of looking outside the window to actually see the rain.

Talking about an interface already refers to a hermeneutic relation. The PDM interface is a representation of the choices we can make in the real world concerning the control of our personal data. The interface is, therefore, mediating in what choices are available, reducing unshown options of the user and with that his freedom of choice and control. Moreover as already discussed, the high usability and familiarity of the interface have negative effects on the conscious decision making of the user. Due to the highly developed skill of most people to read and interpret the interface, it easily becomes transparent. The interface will appear as a perceptual *gestalt*, not in need of conscious attention. One could say that due to this lack of need of attention to the interface one will have more attention 'left' to focus on the message put forward by the interface. However, I argue for the opposite. As the interface is interpreted based on its *gestalt* it is classified as familiar, nothing to worry about or give another thought. The interface is perceived as any other interface with the same consequences, through which the user skillfully and quickly clicks through to accomplish its goals. Business as usual, one would say. However, PDM solutions should not become business as usual nor should the consequences and risks be assessed in a similar manner. This urgent moment of reflection is reduced due to the perceived *gestalt* and the snap decision made upon it. The consent transaction overload only stimulates these snap decisions unspecific to the situation. Moreover, to make the interface as easy to interpreted and therefore as easy to use as possible, the designers often try to avoid large pieces of text or additional information. Besides, only so many options, information, warnings or clarifications can be put on in the interface without making it unusable. Due to reduction of information provided by the PDM interface, the user is unable to overcome the information asymmetry and the privacy paradox as without the proper knowledge of what one is consenting to one is unable to make a reasoned decision. As users trust the application in providing them with enough information and options, the hermeneutic relation conceals the importance and awareness of the information and options which are not provided. The representation of the world which is given through the user-friendly, noninformative PDM interface thus reduces the experience of the world by concealing the importance of everything which is not displayed, both options and information. The interface mediates what supposed to be a reasoned and important decision into an everyday swipe without consequences. As PDM solutions soon will become the standard and will be used on a daily basis, it is of great importance that we are aware of these mediating relations and how they reshape the way we see consent from a thoughtful and important decision into an uninformed easy swipe on our mobile phone.

2.2.3 Alterity

The alterity relation describes how humans are related to or with technology, as the technology is seen as a “quasi-other”. The attention and the engagement of the user are with the technology itself, as it is distinctive from himself and the world. The technology comes to the foreground of the attention of the user.

The alterity relation takes the following shape:

$$I \rightarrow \text{Technology (-World)}$$

Interfaces can behave as a quasi-other as they are able to ask direct questions to the user to which the user can answer with multiple options or sometimes even an open answer. Rosenberger & Verbeek (2015) provide the example of the ATM machine: After asking how much the user would like to withdrawal the user is able to type in the exact amount. In this way, the interface is set up to resemble the analogous interaction we have with humans. Voice assistants go even further by copying human speech.

When users are operating the PDM solution, users have an alterity relation with the technology as they are directly engaged with the technology. As the interface is designed in such a way that it moves from a hermeneutic relation toward more of an alterity relation, the importance of the choices made can be amplified. As users see the interface more as a quasi-other resembling, for instance, a notary, the decision of consent is put in a context which resembles more with real life than the hermeneutic relation would provide. By realizing this normative private context as suggested by Moor and Tavani (2001), users will become more aware of the severity of the situation and the risks of violations of privacy. Moreover, this relation towards a notary is far less familiar than a hermeneutic relation provided by a common interface we are using for everyday purposes. Due to the greater autonomy and authority of the interface when shifted towards an alterity relation, the user will make more conscious decisions and take them more seriously. This reduced familiarity and comfort of authority over the interface will result in less positive affect associated with the interface. As established with the Affect heuristic theory, this would imply that the user is will be less automated and unconscious in his actions and feels the authority of the interface. This translates into taking the job and consequences more serious. It will invite people to see the importance of the decision and to make a more careful, informed and reasoned choice. This all will significantly reduce the privacy paradox. However, Schermer et al. (2014) have warned us to keep the explicit consent restricted to the riskful cases and to keep each request specific to its situation.

2.2.4 Background

The last human-technology relation is background relation. It describes how technologies unconsciously can shape the context of our experience. For example In contrast to a thermometer, a thermostat, not only reports the temperature but influences it directly and even operates for itself without active interaction or awareness of the user. It is only when the system shuts down that the user explicitly experiences the role of technology.

The background relation takes the following shape:

I (-Technology/World)

The background relation does not seem to fit the PDM interface right away. However, the characteristics of the background relation can be found within the usage of the PDM interface. The PDM solution always stays active in the background of your mobile environment when not explicitly used. However, it might give notifications when new data transfers need to be approved. Making the PDM solution transfer from the background into the awareness of the user. It is the background relation of many current applications which drives the initiative of PDM. Our phones track our every move without us even knowing. If we become more aware of these background relations by breaking them down through PDM we can become more aware of our data flow. Moreover, when looking at the usage of the PDM interface, the concepts of the background relation might be the solution to the automatic swiping consent. In the previous sections, I have established that the transparent nature of the PDM interface created by the high usability causes the privacy paradox to appear. Because of reasons of usability, the privacy message underlying the PDM solution stays in the background and is not explicitly experienced. By breaking this down, the user will be snapped out of his thoughtless clicking pattern and become aware of the severity of the decision-making process at hand and its consequences. Only by breaking down its normal way of functioning the PDM solution, and more importantly the underlying message concerning the importance of consent and privacy, become meaningful. This breaking down of the usability flow can be done by giving pop-ups, checkboxes or hold-to-confirm-buttons with warnings concerning possible consequences. In this case, the extra information provided by the warning is crucial in making the user aware of the situation. To make certain the user does not continue in their clicking pattern, these pop-ups or checkboxes need to variate according to context as familiar warnings eventually will stimulate the privacy paradox (Schermer et al., 2014).

By analyzing each relation individually, I have argued that to guarantee its usability, concealment of privacy concerns and the underlying thoughts and consequences of the PDM solution are needed in order to function properly. However, one must be aware of this phenomenon and question the

downsides of such. Especially when the things suppressed are fundamental to its goal and the consequences contradictory to the desired aims. In the case of PDM, the usability provided by the solution mediates the awareness of privacy concerns and thus the value of privacy in a negative sense.

2.3 Mediating moral values

In the previous sections, we have seen that the use of technology can mediate the decision-making process of people and their followed moral behaviour. However, by looking at chapter 1, which shows the changing interpretation of privacy beyond its own boundaries to the distinct concept of control, the mediating nature of technology does not stop at the moral behaviour of its users and the value attributed to privacy. While I have argued for the limited access to be the basis of the "correct" definition of privacy, I have also shown that due to the arrival of new technologies, this might be inconsistent with what people actually mean when speaking of privacy. This is where the two approaches used within this thesis, analytical (chapter 1) and continental (chapter 2) philosophy, clash with each other. I will address the definitions as a result of these approaches as respectively the thin and the thick definition of privacy. Before going into this tension and its implications more elaborately, I will first discuss the thick definition in more detail.

Mediating moral values go beyond the established post-phenomenological theory. However, recent research of Olya Kudina (2019) has established an extending theory based on the concept of value dynamism. The concept of value dynamism suggests that besides the mediated moral decisions and its underlying perceptions, technology also changes the infrastructure of this decision-making process and thereby co-shaping the meaning we attribute to values. This theory is based on the assumption derived from Dewey, that in contrary to many dictionaries and moral theory definitions of value, states that values are not "normative ends but ends in view" (Kudina, 2019, p.59). Suggesting that values are not objective and universal entities immune to contextual shaping. Instead, our daily lives and experiences shape and co-shape our interpretation and meaning of values, making the concept dynamic and never set in stone. However, how must we assess emerging technologies, such as PDM, if these normative frameworks are shaped by these technologies? Kudina and Verbeek (2018) argue that by empirically looking at the technical mediation one can overcome this ethical variant of the Collingridge Dilemma. By taking into account the impact of the technology itself on its normative framework one is still able to stir the direction of the development and assess the impact of PDM. To understand how this mediation occurs, Kudina focusses on the concept of appropriation. This concept, used within the field of domestication studies and post-phenomenology, describes the process of how people actively make sense of and relate to technologies while interacting with the technology in its particular context. It is during this process

of sense-making of technologies and placing them in existing and evolving interpretation frameworks that the meaning of values and it's framework can be subject to change. The process of appropriation is highly dependent on three ever-changing entities; the user with its available knowledge and beliefs, the technology within its dynamic frameworks of understanding and the world or context in which it is used. To examine appropriation, one must look at the actual technology in use, which suggest empirical qualitative research. By empirically analysing *YouTube* comments on *Google Glass* as one of her case studies, Kudina showed "that what people mean with the value of privacy changes in relation to this technology. A connection does indeed exist between technologies and values, whereby values are not stable backgrounds but are flexible and responsive to the sociotechnical practice at hand. Such empirical observations, however preliminary, push the boundaries of the moral mediation account further, for they show that moral mediation includes this dynamism in the value frameworks." (2019, p.45).

Kudina's study suggests that also in the PDM case, an empirical study can provide more insight into the change in what people mean with privacy due to the usage of PDM. Chapter 1.1 has argued for a shift in the meaning of privacy from the analytical correct definition of access, or what I will call from now on the thin definition, towards another concept beyond privacy, the more practical concept of control. This shift is mainly caused by the large influences of digital technology in our daily lives, transforming most of our personal information into digitally stored data. With our private information digitally stored the normal civilian loses grip on who is able to access his or her personal information as for most people the Internet and the possibilities provided by it remain a black box. By this insecurity on the side of access, the common interpretation of privacy starts to shift to a more graspable concept for the many; control. The increasing number of technologies focussing on controlling data and privacy confirms the change in the meaning of privacy even more. We see that this new thick definition established by society and the technology we use provokes tension with the thin definition of privacy. And with that the two approaches used within this thesis. I, however, argue that these two versions are both needed, can coexist and even add to each other. The thin version goes back to the essential core of privacy. A stable basis needed in a legal or political context as proven by Macnish (2018). The thick version forms a dynamic cloak around this rigid core. This more elaborate thick definition shows how privacy is used within daily life, as it is vulnerable to contextual shaping and is no lesser than the thin version. The thin core remains constant while over time technology and society influence the ever-changing thick cloak. The right to privacy, how we manage privacy, what and to what extent we want things to keep private all have been changed by history and its corresponding technologies and culture. As a result, the implications of these changes will differ. For example, the more we are able and nudged to share information online by the sharing

culture created by social media, the less personal information will be considered as private. Or the more technology can provide unwanted access to personal information, the more control becomes of the essence in the thick definition. But what does this implication imply? It looks like a vicious cycle; more information online due to technology, more technology needed to provide control. Which in turn will only increase our online activity and storage of information, which results in a higher need for control. As I argue throughout this thesis, due to this increased use of privacy controlling technologies in everyday life we must not lose track of its embedded context importance and the thin definition of privacy underneath. While these changes in interpretation and implications are inevitable and also needed to fit the situation, the consistent core of the thin definition needs to be kept in place for political reasons. We thus have to make sure that for situations which demand a concrete definition the thin version stays reachable under the layered cloak of the thick one.

By combining analytical with continental philosophy one could say that my solution to the meaning of privacy remains somewhat vague and with too much tension. However, I think that it kept me critical towards the methodologies used and let me look outside the lines of their established frameworks. By using the best of both worlds I have found a way to go back to the core of the problem; the mismatch in definition between analytical and continental philosophy is namely also present within the public debate. It provided me to structurally go back to the essence of privacy needed in a legal or political context that was not subject to time or change. And come to the conclusion that what was considered privacy is not in line with how society uses the value. By combining them as a thin core and a thick cloak as described above I am able to keep this essential thin definition while acknowledging the influence of technology and place in history on the way privacy is perceived. The coexistence of both a thin stable and a thick dynamic definition also demands people to be explicit on what they mean with privacy. If this is done, this reflection enables us to get back in touch with the core of privacy and expand it to the situation at hand. However, it can also stimulate miscommunication when parties are not explicit on their used meaning of privacy. When this occurs more often, society can lose its touch with the thin definition, which can be catastrophic in a political and legal context. However, by combing these two approaches the need for the explicitness of definition used became apparent. As technology is key in changing the thick definition of privacy, I argue that this reflection on what users mean when talking about privacy must be provoked by technologies such as PDM. When technologies concerning privacy are not explicit what they mean with privacy how must we make reasoned decisions through them without having the risks of miscommunication?

By gathering empirical evidence on PDM through the technical mediation framework, I will investigate whether PDM is provoking the privacy paradox and show how PDM mediates the way we value privacy and how we act on it. An advantage of the case of PDM in comparison with the Glass study is the availability of two pilot versions of PDM applications. While available for me, the PDM solutions are still beta versions unavailable for the public and still developing. Where Kudina had to work with textual conversations provided by *YouTube*, I am able to conduct in-depth interviews with people after they were for the first time introduced to a PDM solution. As Kudina already suggests, "in-depth interviews would better reflect the nuanced nature of value interpretation in relation to different case studies" (p.47). In addition, this first-time usage can make a valuable contribution to the authenticity of the appropriation process. Furthermore, by observing how people use the PDM solution, asking them to speak out their thoughts while using the interface and to go back to that interaction by asking more in-depth post questions, the observer can capture the implicit and explicit sense-making of the technology and see the human-technology-world interaction. One should, however, keep in mind that by using an observing method another dimension of hermeneutics comes into play. The interpretation of the answers and observed behaviour by the observer is a subjective entity and remains vulnerable reliability issues such as experimenter bias, especially when it comes to interpreting the implicit answers underlying speech and behaviour. Another advantage of testing and analysing this technology on possible negative consequences mid-stream, in its development stage, is that it is still capable of change. Any conclusions or recommendations made upon the analysed user-PDM interaction can be taken into account when improving its design of the interface. On the counter side, the famous Collingridge dilemma (Collingridge, 1980) also suggest that this up or mid-stream interference is troublesome as we cannot with guarantee predict the way in which these technologies will interfere with consisting value frameworks. The mediation approach will tackle this by also analysing the technological influence on the value of privacy as discussed above.

Chapter 3 Case study: Personal data management

Throughout this thesis, I have spoken a lot about PDM and the implications for our interpretation of the meaning of privacy and the value we attribute to it. While introduced shortly in the introduction, I will provide a more theoretical explanation of PDM in this section. Next, I will describe my qualitative empirical research on both the mediated meaning as the value attributed to privacy, going through the method used and results found. I have done this by testing two PDM pilots on their privacy experience and usability through observation and in-depth interviews. After applying these results to a new version of the interface I will examine the interface again in a similar manner, which will provide insights into whether changes in interfaces indeed can promote or discourage the mediating nature of the interface and thereby the privacy paradox.

3.1 Personal data management

PDM is a movement to restore the user's control over their personal data. The term describes everything related to enhancing the control over the processing of personal data and actual details describing this data. Besides providing more control, PDM also involves providing the user with more insight into the data flow and how it is processed. PDM ultimately could provide the tools to the user to access, remove and share and “unshare” personal data. Furthermore, it aims to provide a structured overview of the shared data and its receivers and the ability to enter self-asserted data.

Figure 1 sketches an overview of the basic principles of PDM described above. It also shows the possible areas of application and kind of data shared through PDM. For now, the concept of PDM is very attractive to governmental institutions who want to safely share the person’s data for the person’s purposes while retaining its authenticity. On the other hand, data consumers such as banking corporations who accommodate mortgages or medical personal want to ease and fasten the process of their customers, i.e. the person, in providing them with the authenticated data they need to accurately do their job. Finally, the PDM construction is meant to please the person as s/he gains easily insight and control into his personal data.

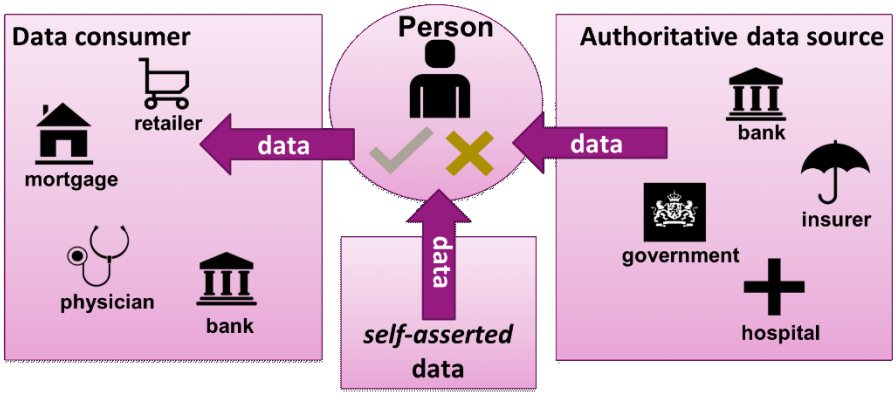


Figure 1. Basic principles of PDM (InnoValor, 2019)

While PDM is an up and coming movement, there are already multiple PDM solutions being tested for implementation. The main core of all these solutions is often based on the four different roles within PDM. Firstly, its role for the person or user operating the PDM solution, controlling their personal data and with whom they are shared. Secondly, the data source gathers and distributes the personal data with the person, operator and data using service on behalf of the person's wishes. Thirdly, the data using services to whom the data can be transferred using the operator on the person's command. And finally, the operator providing a secure platform or service with which the person is able to access and control the personal data and its flow between the data source and the data using service. These connections are mapped out in figure 2.

There are two variations of the PDM structure. The push-model in which the person himself takes the place of the operator, managing the data flow and access between the source and service directly. And pull-model in which the operator is an external party as sketched in figure 2. In the latter case, the operator claims not to be using the data itself but is providing a secure sharing service mediating between the different roles in the PDM structure. In my empirical research I will test both a Push and a Pull-model, respectively the case study of the 'Blauwe Knop' and of ' Schluss'.

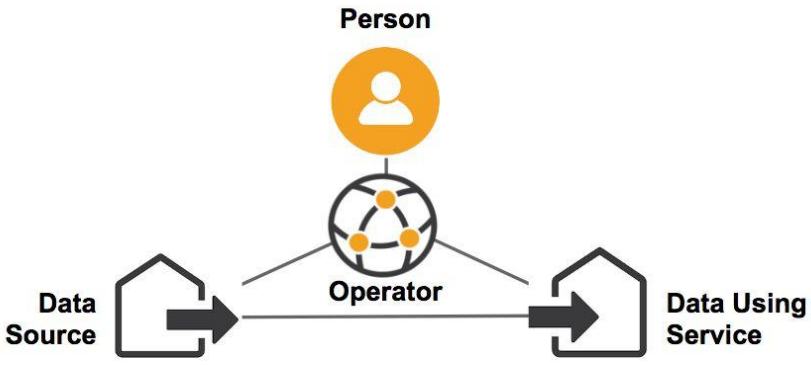


Figure 2. Roles in PDM solutions (MyData declaration, www.mydata.org)

In order to make the connection between the four roles, the PDM solution has to function properly. This is done through the eight functional components of the operator called the *PDM commons*:

- Consent management – managing (temporary) consents for sharing specific personal data between data sources and data consumers. Includes an overview of consent and the possibility to revoke and adopt consents given.
- Authorization management – translates consent to access to data, allowing data using services to access the data at a certain source.
- Authentication – authenticating the user to ensure the right personal data are accessed or shared. For example DigiD in the Netherlands.
- Service management - enables connecting data sources and data consumers. Similar data can be at different sources and can be used by different data consumers.
- Data management – storage of (self-asserted) data.
- Value-adding services – the PDM solution adds value to data by filtering, analysing or aggregating data, or translating data.
- Logging – keeping track of all information exchanges taking place, creating transparency in who accessed what and when.
- Information exchange – interface to allow for data exchange between data source, data consumer and operator in a standardized and secure manner. This can take different forms: structured data, supporting automated transactions or unstructured data, such as a pdf. Information can flow through the PDM solution, but can also function as a pull or push model (InnoValor, 2019, p.8).

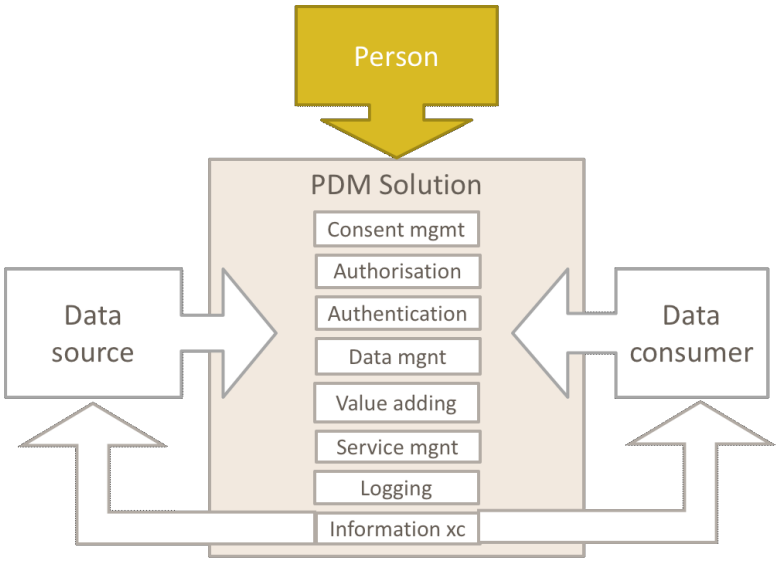


Figure 3. PDM model roles and commons (InnoValor, 2019).

While there are a number of PDM solutions up and coming, there are still in their pilot phase and have difficulties scaling up. These pilots often remain stuck with one or two data sources and consumers. Examples in the Netherlands are Ockto, Dappre, Schluss, Financieel Paspoort, Tippiq and Blauwe Knop. Moreover, they are often not "complete" according to the eight essential commons. The ultimate goal behind the PDM movement is to eventually have one dominant operator, in which persons are able to manage their entire data flow from one central digital place. This central place would provide a clear overview of which personal data is available at data sources and whether or not they are shared with data consumers/using services (InnoValor, 2019). Within my empirical research on the mediating nature of PDM solutions, I tested two PDM pilots which I will now introduce shortly.

3.1.1 Schluss

The first pilot application is called Schluss, which needs to impose the nature of the application; a vault. Within this pilot study, Schluss is used by the data consumer, the Volksbank, to arrange consent management and easy data flow from student debts stored by data source DUO. By using this data transfer of student debts, the operator Schluss enables the person to quickly apply for a mortgage. As a third party, Schluss tries to aim for user-centred design in which the user has more transparency and control on the data flow. Moreover, this data transfer is much quicker than the paper version used nowadays, which can take up to six workdays. Schluss asks the user to provide consent to access the student debt data from DUO and again asks consent to share this data with the Volksbank. Meanwhile, the data is stored within Schluss. Users are able to create a vault which can be accessed later on with the use of a pin code. In the future, Schluss can also be used to store and transfer data to other parties but now remains limited to the data source of DUO and the data customer of the Volksbank. Within the future vault, users can overview which parties have access to what kind of information undue any prior consent arrangements.

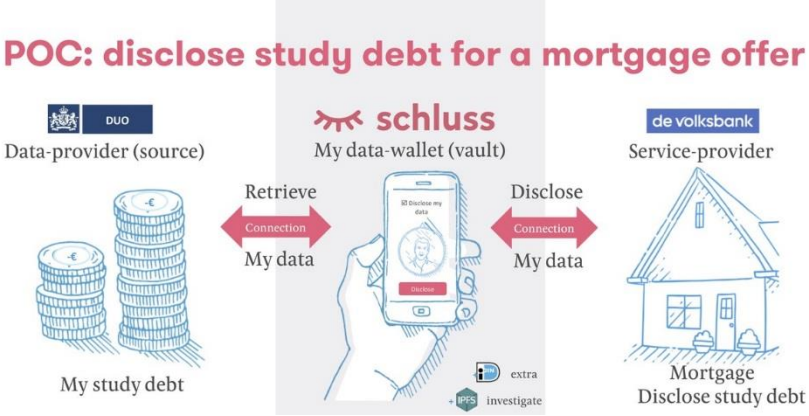


Figure 4. Model of Schluss proof of concept (POC) (InnoValor, flyer, 2019)

3.1.2 DUO Blauwe Knop (Blue Button)

Even though DUO is part of the Schluss pilot, it also has its own PDM system, called de Blauwe Knop (Blue Button). Instead of using a pull-model such as Schluss the Blauwe Knop usage a push-model. This means that the user personally retrieves the information from DUO when needed instead of providing consent for another party to pull this data from DUO as in the case of Schluss. Within Blauwe Knop the user is provided with information through three drop-down menus about downloading, security and privacy. With the Blauwe Knop users remain totally in control over their data as it is downloaded onto their own personal computer in a PDF or XML format. The data can when needed to be digitally sent to parties of choice. This needs to be done manually by the user themselves. When the data is printed the authorization stamp of DUO expires. The Blauwe Knop is currently also working to develop a '++ variant' in which the people are also able to directly send the data to the desired data customer, transforming the push into a pull-model. The PDM is set up for current and former students to provide easy access and overview of their student debt data from their own personal laptop.

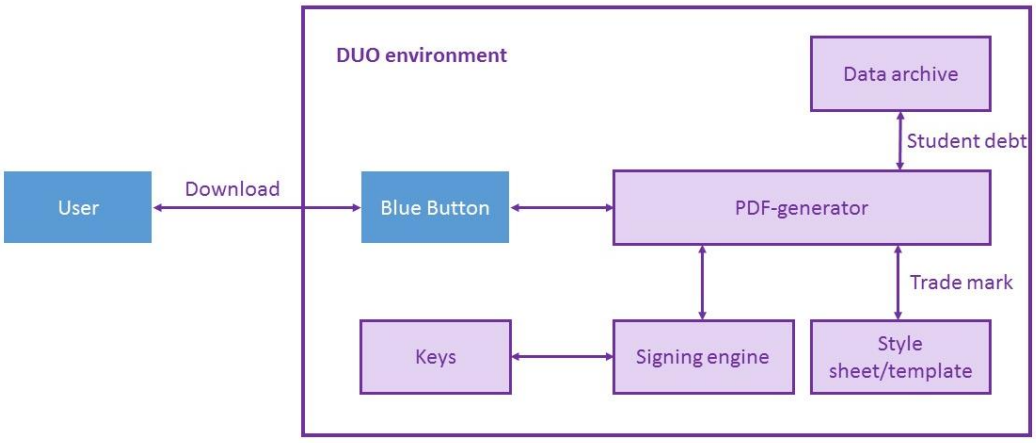


Figure 5. The architecture of Blauwe Knop

3.2 Qualitative analysis PDM

3.2.1 Method[2]

To find empirical evidence to support my argument that PDM solutions are mediating the way we interpret privacy and the value we attribute to it, user studies of two PDM platforms were done. Following the 'thinking aloud method' (Lewis, 1982) the participant used the PDM solution and spoke clearly and elaborate on what he/she was doing, on what is clear and what unclear and why he/she is taking certain actions. In the meantime, the experimenter is carefully observing while not

[2] The complete methodology and results of this case study can be found in the Appendix

interfering with the participant. Due to this observational method, I was able to perceive the behavioural patterns of the participant while using the PDM solution and see whether or not the usability of the interface mediated into an automatic clicking response. An in-depth post-interview gave me the opportunity to together with my participant, reflect on the interaction with the software and to ask follow up questions concerning the consciousness and rationality of the decision-making process. Moreover, the interview revealed the appropriation of the PDM solution and the mediating effects on the value dynamism. In order to foresee interpersonal differences in the concerns around privacy, I used the famous Westin privacy concern index (1991) and the additional Buchanan technical capability scale (2007), measuring the participant's behaviour aimed at securing their online privacy, to explain different outcomes per group. For both studies, four participants were recruited, (eight in total) with a similar profile as the end-user of the PDM solution. For Schluss, invited were starters on the housing market, in the phase of applying for a mortgage and who are or previously were students using services provided by DUO. For Blauwe Knop, the main inclusion criterium was that participants were current students or were so in the past. For both studies, the participants needed to have a remaining study debt at DUO. Both studies aimed to create a realistic environment which matches the actual usage environment.

Conclusions for design recommendations were drawn on the basis of thinking aloud analysis, which included the time taken to complete the walkthrough and the time to provide consent, in combination with the interview data. In this way, both the explicit and implicit answers of the participants, as well as their actual behaviour, were captured in order to find mediating effects of the PDM interface on the value and meaning attributed to privacy. These design recommendations were implemented in an improved interface which was tested with the use of the same method, again with four participants. Comparing the results from the original and improved interface will show whether or not design recommendations such as the implementation of more information on what one is consenting to, will reduce the privacy paradox and therefore the negative consequences of the mediating nature of the interface.

3.2.2 Results

Within both studies all Westin privacy classifications were represented and distributed the same; 2 unconcerned, 1 pragmatists and 1 fundamentalist. In the Schluss case, these classifications were obviously mirrored within the in-dept interview through the experienced privacy, the trust level and the number and kinds of recommendations made to improve the application. Overall there was a relationship found between how much people are concerned about their privacy and how capable they were to secure their privacy online. While the observation is only based on eight participants, it is quite obvious that the behaviour and attitude concerning privacy are in line with each other;

people who have more technical capabilities to secure their online privacy and are doing so are more concerned about their privacy.

How PDM interfaces mediate the value of privacy

All participants in both case studies were very quick to go through the applications as they only spend around two minutes completing the data request. When observing their behaviour it was obvious that nearly all participants clicked out of automatic unreflective behaviour instead of taking a second time to think about the consequences of their actions. For instance, only one of the participants opened one of the three drop-down menus within the Blauwe Knop application providing critical information concerning downloading, security and privacy. Moreover, only one of the Schluss participants noticed the button leading to the elaborate terms and conditions. This shows that critical information must not be provided as an option to inform oneself. Instead, the designer of the interface must make certain that users will inform themselves. Within the Schluss applications, participants had to provide their final consent by holding a button for 3 seconds to make sure the consent was made intentionally. However, this good example of design interface to deconstruct the mediating effect of the application only proofed its existence. Only one participant correctly held the button, others became frustrated and confused as they did not understand why it did not function. Note that the notification of the 3-second rule was placed underneath the button in question. The fact that this was ignored proofed that most participants did not even bother to scan the whole screen before pushing the final consent button, let alone think of its consequences. The pressing action was a responsive one. The fundamentalists, participants who greatly concern about their privacy, in both case studies stood out as they took remarkedly more time to provide consent than the other participants while still having the lowest overall time to complete the application.

From the observations in combination with the in-depth interview, we learn that participants claim that behaviour would be altered when small changes in the interface help reduce this unreflective clicking behaviour and so reduce the negative mediation from the interface. Participants recommend the implementation of a mediating screen showing the content to be downloaded before the actual act and mandatory reading of privacy information by conventual ticking boxes instead of new design features such as the 3-second button.

When being asked to prioritize, low privacy classified participants quickly chose ease and usability above privacy. The higher the classification the harder the confession seemed to be. However, at the end of the interview, every participant explicit or in some cases implicitly confessed to choosing ease over privacy and thus supporting the privacy paradox. The most common reason to favour ease and usability proved the argument made that people do not think their personal information is of any

value to others. All but one participant, who was classified as privacy unconcerned, mentioned that they indeed went very fast through the application without explicitly thinking about the consequences of consent. They all stated that this was indeed due to the ease and usability of the user interface and the flow of the application, proving my initial argument on the mediating nature of the interface on the value of privacy especially where usability is concerned.

"The button was so big, so present that I just pressed it because it screamed to be clicked." (Blauwe Knop participant)

"Ehm… Yes. Yes, you are right… I did indeed click without thinking, how terrible… I feel ashamed." (Schluss participant)

The privacy unconcerned participant mentioned that she knew she had to provide consent already at the beginning of the application for a mortgage, so it did not matter in which way she was asked to do this, even though it was indeed easy.

Finally, all but two Schluss participants, both classified as unconcerned, stated that when these PDM solutions will become the standard and are used on daily basis on a large scale, they can cause tremendous problems due to the thoughtless thinking of people which is reinforced by the ease and usability of the interface. Providing consent will become an automated action as it is done so frequently. Managing one's consents on data flows all together will only enhance this automated unconscious behaviour due to the lack of diversity and the disconnection of the request with its context. In accordance with what was described in 1.2.2, another problem stated by the participants is the inability to access the service provided when no consent provided. The two privacy unconcerned participants however stated that on the contrary, when PDM solutions become more common in use and are used for different data transfers, people will become more aware of issues around providing consent. This opinion was mostly based on the fact that participants saw how users gain more control and a better overview of the data flow and the parties involved due to the application. Both the unconcerned participants however do mention that this opinion possibly only counts for themselves as being higher educated. They do feel that other people, for example, people with less education, are more vulnerable and give in to the ease of providing consent without actively thinking about the decision and being aware of the consequences. They state that, in this way, that automatic response can become a big problem which needs to be foreseen.

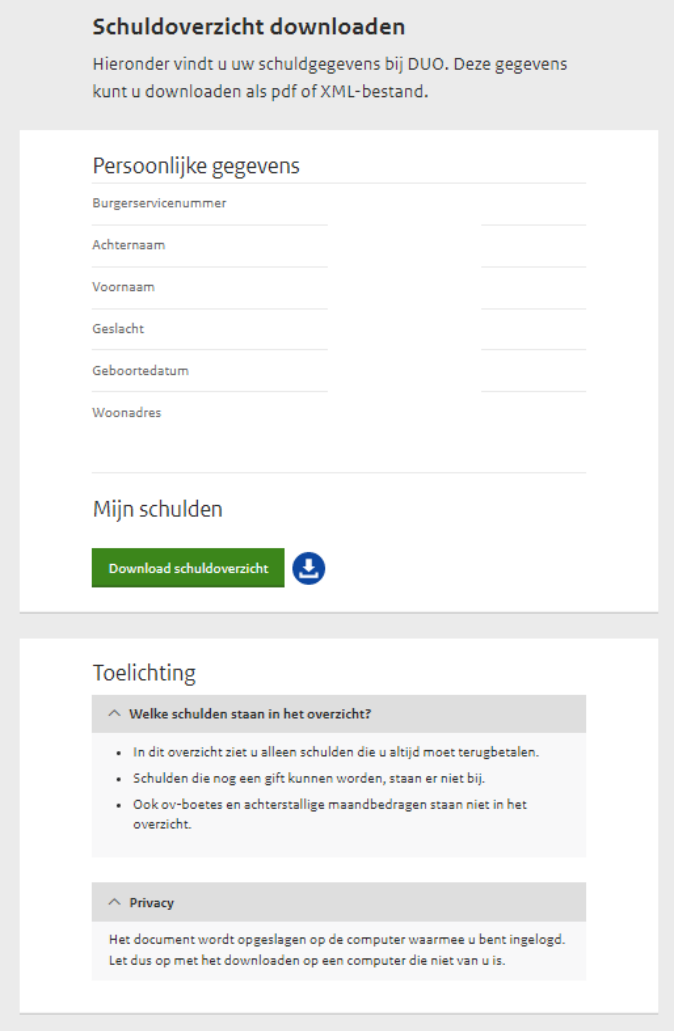


Figure 5. The interface of Blauwe Knop; the data to download is not displayed before the action is taken, critical information is stated in drop-down menus which actively need to be opened

How PDM solutions mediate the meaning of privacy

In our studies, the degree of privacy experienced provided by the PDM solutions depended on both the privacy classification as well as on the definition described to privacy. Every Schluss participant defined privacy as control. Blauwe Knop participants were equally divided between the control and access camps. This difference in outcome can be explained by looking at the nature of the two PDM solutions. In the case of Schluss, the whole process revolved around controlling one's own data in order to transfer it to the bank. Blauwe Knop, however, did not include this transfer option which made the task at hand revolve around accessing the data yourself instead of controlling it to transfer. This difference in attributed meaning to privacy shows that the thin and thick layer can coexist and that the different setups of technology user characteristics and context determine how users define privacy in each situation.

Within the Schluss study, participants had very different opinions about the control Schluss provided them, opinions which correlated with their assigned privacy classification. The two privacy

unconcerned participants mentioned that they had gained more control due to the Schluss application. They mentioned that due to this enhanced control, it was easier to get insight into the flow of data and to be sure no unwanted parties were involved. Moreover, they noted that only specific information was transferred. This provided a feeling of more safety. However, the other two participants, higher ranked within the privacy concern index, experienced less control due to Schluss. They both considered Schluss as a third person on which they had no certainty hence no control. However, all participants agreed that they as users had no control or freedom in what to share. This path is restricted due to the fact that what is transferred and how is already laid out by Schluss. All participant wanted more options to choose from, both in what to share and for how long. These findings confirm the mediating nature of the interface on the freedom of action of the user. Within the Blauwe Knop study, most of the participants experienced more control over their personal data due to the set-up of the application. They appreciated the fact that they were able to access their personal data and to manage who they send it to when needed. And most importantly, that this was all done on their demand and by themselves. The storage on their own laptop also provided a sense of control as they felt like they now 'owned' the data. More insight, understanding and more freedom thus granted a better feeling of control.

For the Blauwe Knop study, two participants, both low on the technical capability score, noted that they did not feel secure when sending the document digitally. The Internet is seen as a big black box of which participants have little understanding and thus the feel not secure about who is accessing their personal data. Moreover, although enhancing the feeling of control, the storage on one's own laptop did negatively contribute to the feeling of security for half of the participants. These participants experienced their own laptop as unsafe and easily hackable. This result confirms the arguments made within chapter 1 that due to the ungraspable nature of the Internet and other's hacking capabilities, the user loses sight of who has access to their personal data. Therefore the meaning of privacy among users will shift beyond privacy to control. The other half of the participants did not feel like anyone would bother to hack their laptop and did not experience their laptop as unsafe. This confirms the argument on information asymmetry: the participants are unaware of the value of their data to others.

3.3 Mediating privacy

These outcomes show that specifics of the PDM solution determine whether the user perceives privacy as access or control. This confirms the dynamic nature of values which is highly depended on the socio-material context and technology used as argued for in chapter 2.3. Blauwe Knop, which did not provoke privacy as control completely, is only in its first stages. The future prospects are that it will become more similar to Schluss, that is, creating the immediate data flow from the data source

to the data consumer by the hands of the person operating the PDM platform. This development shows that this pull-model of PDM is the functionality desired by the PDM community. As established by examining Schluss, this would suggest that future PDM solutions, which are managing multiple consent flows and thus access permissions between multiple data sources and consumers, will mediate its users into perceiving privacy less as access and more as control. The more common PDM becomes in our daily life, the more effect this mediation will have on this thick version of the definition of privacy. Supporting the argument made that the digitalization of our personal information and tools to manage these shift the interpretation beyond the thin definition of privacy towards a thick version based on control.

The empirical evidence also showed that both Schluss and Blauwe Knop, and, if representative, thus likely all PDM solutions, are at high risk of reinforcing the privacy paradox due to the mediating nature of the user-friendly interface. The observed automatic, unreflective consents facilitated through the user-friendly device support my argument made in chapter 2.2. I argue specific design recommendations will reduce these unwanted consequences. These changes need to make certain that critical information on privacy is read, for instance by getting rid of drop-down menus, that users are aware of the content they consenting to before the action takes place and that they are snapped out of their unconscious clicking pattern by pop-up warnings and ticking boxes. Moreover, the interface must make clear what definition of privacy they are using to prevent miscommunication and to provide the user with room to reflect on their own used meaning of privacy. These improvements create a more calm user flow in which the user is nudged to consciously think about what he or she is doing and to be informed about the possible consequences. Instead of becoming a zombie following the intended user flow without being conscious of the actions taken. In this manner, there will be a higher consistency between the intention or attitude about privacy and the actual behaviour, or at least make more informed and deliberate decisions and actions. Moreover, the reflection on their own meaning of privacy as discussed in 2.3 provides the means to get back in touch with the thin version an adapt it to the context at hand.

3.3.1 The improved PDM interface

Based on my design recommendations a new interface was designed for the Blauwe Knop. The most critical improvements are shown in figure 5 and 6. In testing, the only difference compared to the method used with the previous two PDM solutions was the context in which the interface was implemented. While Blauwe Knop for DUO was focussed on student debts, the new Blauwe Knop was developed for municipalities and is focused on civilians who have multiple debts. These users are often lower educated and less familiar with digital technology than the students using the DUO

interface. The qualitative research showed that participants were more conscious in providing their consent and had less of an automized clicking pattern than those using the earlier interface. The former was mainly caused by the implementation of a screen clearly showing the debt overview and an explanation text on the functionality and purposes of the Blauwe Knop. This all was done before the consent request was shown. This created a more informed decision-making process in which the users were aware of the importance of the task and its consequences. The reduction of the automatic clicking through the application was obtained by the extra information given and extra warnings considering the privacy implications which were mandatory in order to proceed to the download. This was done through inactivating the download button until the warnings were read and ticked by its boxes. The observation showed that when participants wanted to fall back on the clicking pattern and continue downloading before reading the information, they were snapped out of this trance due to the red notification stating that they needed to first understand the consequences of the consent. This pop-up warning created the important moment of reflection, in which they actively read the consequences and inform themselves before consenting. The post-interview also showed that participants were content with the way they were educated and informed, both by the data shown before the consent and the warnings given. This all gave a feeling of protection and participants felt as they were taken seriously, guided to a good extent and therefore treated as human beings instead of being patronised. The reflective moments and warnings concerning privacy made the participants actively think about the privacy at stake and were the building blocks of their attributed meaning of privacy. Due to the focus on the security provided by DigiD, some participants defined their privacy as the thin version of access. While others referred to the privacy warning to be aware that the document will be saved on the used computer. Because they all read this warning before continuing they had the control to remove the document when wanted, defining privacy as a thick version of privacy based on control. Here again, the meaning of privacy is influenced by technology and its used phrases. Overall, the design recommendations proved to be a success in reducing the negative mediation of the interface on the conscious decision-making process in providing consent and made users shape their meaning of privacy to the context at hand. The interface, however, would even more benefit by providing an explicit definition of privacy used. Whether this is the thin or thick version, by providing this transparency it will allow people to engage in a personal reflection of their meaning of privacy and whether this is consistent with the interface avoiding miscommunication and loss of the thin definition.

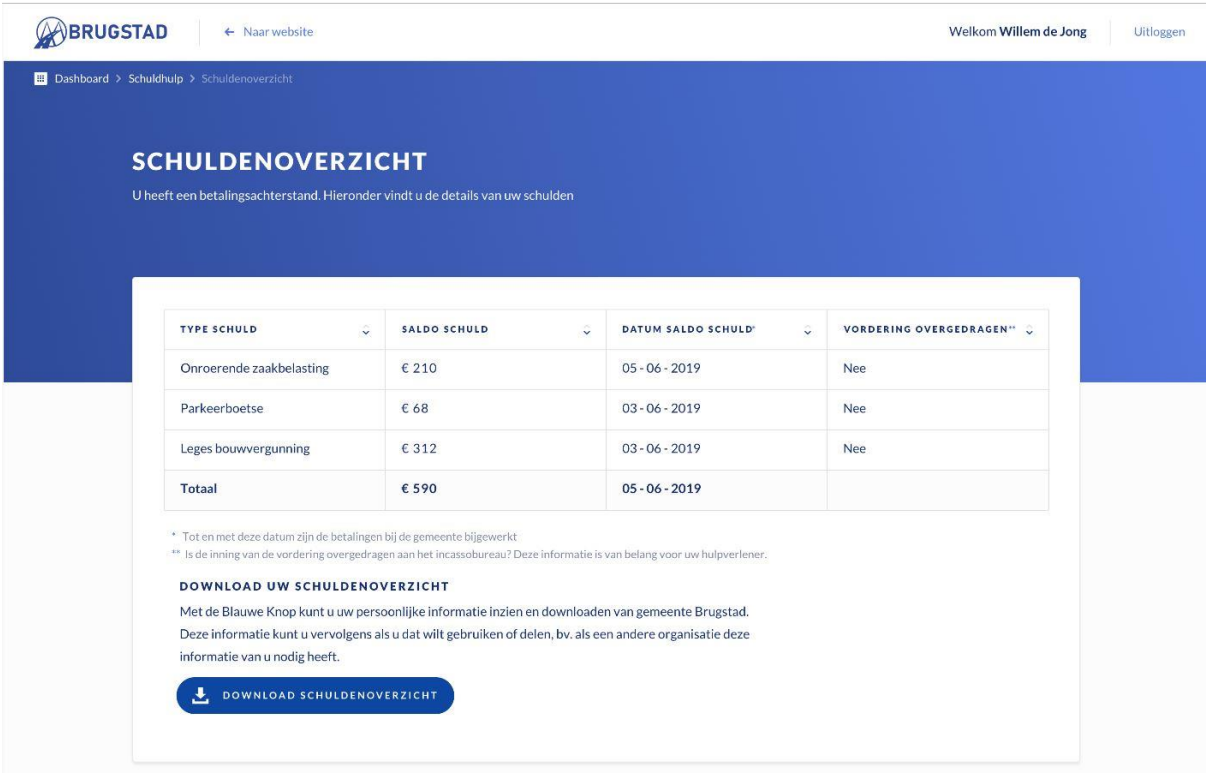


Figure 5. Improved interface; Debt overview is shown before the download, including information on the Blauwe Knop's purpose.

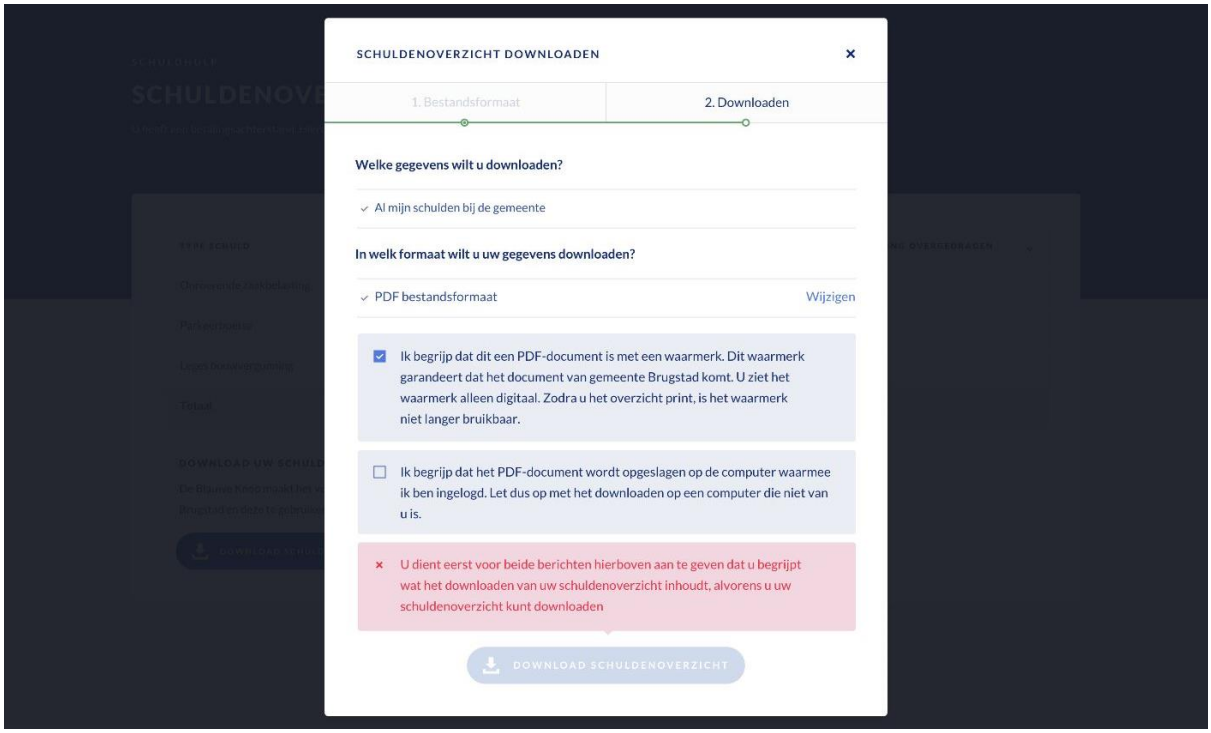


Figure 6. The improved interface: warning pup-up when consequences are not read.

3.3.2 In defence of libertarian paternalism

While analysing these improvements above one could argue that by wanting to reduce the persuasive nature of the interface it is still paternalizing its users. Users are guided in making an

active and reasoned decision. However, I consider this a helping hand necessary to provide room for users to think about what they mean with privacy, whether that is consistent with the definition of the interface and what they consenting to. Where the previous interface was persuading users in behaving in favour of the request, the interface is now persuading users for their own good. Ihde has taught us that technology always shapes human behaviour, making some kind of paternalism inevitable. I, therefore, argue for a libertarian paternalistic approach, which influences users is in making decisions to promote their welfare, without any form of coercion, preserving freedom of choice and which is more attractive than other forms of paternalism by avoiding harmful or random effects (Sunstein & Thaler 2003). So while this new setup does interfere with users right to be left alone, designers do claim responsibility in providing users with their right to be educated and to make their decision explicit. Yes, users are patronised in informing themselves. However, this knowledge on what they are consenting to makes their decision on providing consent even more their own choice, as without it they were forced in harming themselves. Moreover, by providing more guidance, information and feedback participants experienced more dignity and less patronised than in the previous interfaces. In order to keep this from harming one's welfare by overburdening them, unurgent consent requests must be brought back to implied consent as proposed by Schermer et al. (2014). Libertarian paternalism thus tries to weigh out the costs and benefits of assigned choices on the user's welfare.

Chapter 4 The interface: both problem and solution

Throughout this thesis, I argued that the interface of digital technologies, in particular ones concerning privacy such as PDM, are the cause of certain shifts in behaviour and interpretation when it comes to privacy. The analysis of the meaning of privacy in chapter 1.1 showed that due to the digitalisation of our personal data, the thin definition of privacy, the access or limitation theory, is not sufficient for most people or uses. The ignorance of what goes on through the Internet and the uncertainty which comes with that seems to be the driving factor in this shift. This obscurity for the common people can be captured in the following: who is accessing the data, who being human or systems? How the data is accessed, is this only in general terms, in patterns or tracible to the individual? And what is the intensity in which this accessing is done? While access remains ungraspable, as we have become dependent on the Internet as the source to make data accessible, control provided by the interfaces of privacy managing systems seems to offer a solution. The empirical analysis showed that, as suggested in the theoretical analysis, the arrival of control technologies such as PDM also help to shift this interpretation of privacy to the thick definition since the way people appropriate privacy is through these technologies. The thin definition might in this way start to differ from the thick common used definition. While the concept of value dynamism shows that this shift in interpretation is not uncommon or undesirable, I argue that we must be aware that we do not lose touch with the thin definition of privacy for political reasons. I argue that the design of the interface must be explicit on what definition is used and provoke the user's reflection on one's own meaning of privacy. Besides the change in the meaning of privacy, the interface is also key to which degree shift in the value attributed to privacy takes place.

First, the interface provides the means to the three c's of control according to the RALC theory; choice, consent and correction. Chapter 1 showed that these three tools of control are needed to provide the basis of control and protection of privacy. However if the interface does not provide one or more of them to a sufficient extent, the control offered by the PDM solution remains an illusion. Chapter 1.2.2 has shown that while consent and notice are often present, this is far less the case for choice or correction. Forcing the user in providing consent as there is an inability not to and inhibiting the possibility to realize one's privacy preferences and edit characteristics of the data transfer. This manipulation by the interface is the first step in enforcing the privacy paradox and underlining the meditative nature of the interface on the value of privacy. By simply making the choice and correction available the interface would solve its own problems.

Secondly, the privacy paradox comes forward out of a human inability to remain consistent in their preferences over time and context. This is grounded in the absence of information of both short and

long term consequences to base this decision on. Moreover, interfaces are often not specific what they mean when talking about privacy. In short, users are not able to know what they are consenting to, unaware of its consequences and implications and undervalue their own data especially in the current context of data mining. By not giving full disclosure and reducing this information, the interface is concealing the importance of everything which is not displayed, both in the form of information, the significance of the consent, definitions used and options of action. If the interface allowed this information to be provided, more reasoned decision making could take place. Users would then be able to rationally weigh out the costs of sharing information online to the provided benefits. Moreover, if the information is provided users are given a moment of reflection as they are snapped out of their clicking pattern to read. Reducing the chance of an appearing privacy paradox and conflicting definitions.

Thirdly, the affect heuristic theory showed that the conventual design and thus the ease and familiarity of the interface associated with the decision-making process also strengthens the privacy paradox. This is supported by the mediation theory as the high usability creates the highly transparent nature of the PDM interface. Small changes such as warning pop-ups, short but informative text which is explicit on the used meaning of privacy and checkboxes which are only clickable after a period of time needed to read the warning, will help in reducing this transparency by visualizing feedback and consequences of one's actions. Understanding the process is needed to regain the importance of the one's privacy concerning personal data, as the interface now transforms this perception into business as usual (Dourish & Anderson, 2006). By breaking down usability and reconnecting the request with its context, the user will become more aware of the privacy consequences and any possible inconsistency between user's and interface's version of privacy. In result, users are snapped out of their automatic clicking pattern. By the small changes described above, little moments of reflection will reappear which are normally present when deciding whether or not to unclose data and reveal formerly concealed privacy risks.

These arguments show that while the interface is the cause of all the trouble it is also key in solving them. This is also substantiated by the empirical evidence; the difference between the results of the initial and the improved design show once again that the design of the interface is the key factor in establishing or discouraging the mediating nature of the value of privacy and the way in which people give it meaning. It shows that the improvement of little design features can reduce the privacy paradox and increase conscious and reasoned decision making. The main message is to reduce the transparency of the interface. One way to achieve this is to shift the hermeneutic or embodiment relation towards an alterity one. This can be done by taking the user more seriously and educating them as equal. Implementing more guidance, information on what they are

consenting to, room to reflect on one's decisions and freedom of choice and correction will make sure of this. By doing so the interface is seen as an autonomous quasi-other with authority. Creating more significance to privacy issues, its context and stressing the importance of the decision and to make a more careful, informed and reasoned choice. On the counter side, we must make sure that this does not result in information or consent overload by providing too many options and irrelevant information. The key is to apply informed and explicit consent with these recommendations in cases of need and reducing all other to implied consent. Adjusting the request to its context can come a long way in preventing similarity and therefore the paradox.

Becoming aware of the problem and how to foresee them is important as this moral issue of manipulating interfaces is overshadowed by the absence of a legal one. With the more important decisions made on interfaces, also more decisions will be manipulated through the interface. Users will make a different, more conscious and reasoned decision if the interface provides them with more choice and options for correction, more information on short and long term consequences, and more reflection time in comparison with the absence of these features. The control gained through PDM is only an illusion, making people even more vulnerable and less secured. It is likely that PDM interfaces will become part of our everyday life, diminishing the importance of consent and privacy risks as swiping consent will be done in the same manner as liking a Facebook post. In addition, the increased focus on control can make us lose touch with the thin version of privacy needed in political situations. Moreover, the envisioned path of the PDM movement is to move beyond the low scale pilot applications we encountered in the qualitative analysis towards one central application managing all our data transfers in life. In the process of centralizing different kinds of data to one application, specific context will be lost. Provoking the meditative nature even more as the importance of the data becomes even more concealed without its surrounding context. Furthermore, when everything is put in one application there might be simply no room for information specific to each set of data. Thus, creating the inability to properly inform its users and strengthen the privacy paradox, and the loss of value attributed to privacy. We are in need to act now while the PDM solutions are still in their development state. That these PDM solutions will develop is set in stone, how they develop on the contrary can still be shaped. We have to reveal the paradoxical nature of these "privacy-protecting" solutions. Make their meaning of privacy clear and change their interface design to reduce the negative effects on the value of privacy and our reasoned decision making to a minimum.

Conclusion

Within this thesis, I argued that the online age and, with it, the arrival of new privacy-enhancing technologies such as PDM create a shift in the interpretation of privacy and reduction in its attributed value. I have done this by first diving into the concept of privacy. I have shown while the analytical definition of privacy is proven by the access theory, our online age demands more than the concept provides. Because of the black-box nature of the Internet, people need a more graspable concept than access. Therefore, one has to go beyond privacy and reach for the concept of control. While remaining a distinctive concept from privacy, RALC theory shows that control provides the tools for handling privacy in a digital context. But with it comes large responsibilities for the interface and its designer. The privacy paradox shows that by neglecting what users are consenting to, interfaces manipulate users into behaviour conflicting with their initial attitude. While notice and consent cover the legal issue a moral issue rises. Through applying the theoretical framework of post-phenomenology to the case of PDM, I have shown that the main problem underlying the privacy paradox and its reduction in value is the transparency of the PDM interface provoked by an embodiment or hermeneutic relation. Moreover, the definitions of access and control can coexist and even add on each other by referring them as the thin core necessary for political situations surrounded by the thick cloak adjusting to the technological environment. Design changes in the interface can shift this human-PDM-world relation to an alterity relation and break down this transparency. For users to make reasoned decisions, interfaces should provide more information on what one is consenting to, guidance and freedom of choice and correction and reconnect with its context. In addition, as the interface is key in changing the thick definition of privacy, I argue that this reflection on what one means when talking about privacy must be provoked by technologies such as PDM. Users will snap out of their automatic clicking pattern and perceive the interface and the importance of the underlying message as an autonomous entity which is not taken for granted.

By analysing two PDM pilots and seeing the privacy paradox and value mediation in practice, an improved interface was designed in order to achieve the previously set goals. The difference in results between the former and the improved interface show that little design features can reduce the privacy paradox of the interface. Within chapter 4 I showed how every argument made is underlined by the interface and how this interface can serve as a solution. Moreover, I showed the future prospects and the significance of addressing the problem of mediating interfaces in the context of privacy. Even though I found supporting evidence in my design changes for the paradox, more research can be done on what design characteristics are critical in reducing irrational behaviour. Besides, more elaborate research can be done on what influences design changes have

on the mediation of the value of privacy. For instance, privacy by design should be examined whether or not it can hold back the paradox and whether a change in the value of privacy has implications on the categorization of normative and naturally private situations. Implicating more loss of privacy instead of violations of privacy. However, in the end, only the future will tell whether centralized and scaled up PDM solutions will indeed provoke the reduced value of privacy in the way I have argued for.

Bibliography

Acquisti, A. (2004), Privacy in electronic commerce and the economics of immediate gratification. In: *Proceedings of the 5th ACM conference on Electronic commerce*, May 17-20, 2004, New York, USA.

Acquisti, A., and Grossklags, J. (2003), Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. In: *Proceedings of the 2nd Annual Workshop on Economics and Information Security* (WEIS 2003), May 29-30, 2003, Maryland, USA.

Barnes, S.B. (2006), A privacy paradox: Social networking in the United States. *First Monday*, **11**(9).

Beresford, A. R., Kübler, D., and Preibusch, S. (2012), Unwillingness to pay for privacy: A field experiment. *Economics Letters*, **117**(1), 25-27.

Böhme, R., & Köpsell, S. (2010). Trained to accept?: a field experiment on consent dialogs. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 2403-2406). ACM.

Boyd, D., & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, communication & society*, *15*(5), 662-679.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American society for information science and technology*, *58*(2), 157-165.

Brown, B. (2001), Studying the internet experience. *HP Laboratories Technical Report (HPL-2001-49).*

Collingridge, D. (1980). The dilemma of control. *The Social Control of Technology*, 13-22.

Custers, B. (2001). Data mining and group profiling on the Internet. *Custers BHM (2001), Data Mining and Group Profiling on the Internet. In: Vedder A (red.) Ethics and the Internet. Antwerpen: Intersentia*, 87-104.

Dourish, P., & Anderson, K. (2006). Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human-computer interaction*, *21*(3), 319-342.

Egelman, S., Felt, A. P., and Wagner, D. (2012), Choice architecture and smartphone privacy: There's a price for that. In: *Proceedings of the 11th Annual Workshop on the Economics of Information Security* (WEIS2012), June 25-26, Berlin, Germany.

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. *Journal of computer-mediated communication*, *12*(4), 1143-1168.

European Commission. (2018). "A new era for data protection in the EU, What changes after May 2018" retrieved from https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

Hoofnagle, C. J., & Whittington, J. (2014). Free: accounting for the costs of the internet's most popular price. *UCLA Law Review*, *61*, 606-670.

Hughes-Roberts, T. (2013), Privacy and Social Networks: Is Concern a Valid Indicator of Intention and Behaviour? In: *Proceeding of the International Conference on Social Computing* (SocialCom 2013), September 8-14, 2013, Washington, USA.

Hull, G. (2015). Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data. *Ethics and Information Technology*, *17*(2), 89-101.

Ihde, D. (1990). *Technology and the Lifeworld*. Bloomington: Indiana University Press.

Inness, J. C. (1996). *Privacy, intimacy, and isolation*. Oxford University Press on Demand.

Innovalor (2019). *Personal data management, views from digital We*

Jolls, C., & Sunstein, C. R. (2006). Debiasing through law. *The Journal of Legal Studies*, *35*(1), 199-242.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security*, *64*, 122-134.

Kizilcec, R. F. (2016). How much information?: Effects of transparency on trust in an algorithmic interface. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 2390-2395). ACM.

Kudina, O. (2019). The technological mediation of morality: value dynamism, and the complex interaction between ethics and technology.

Lee, H., Park, H. and Kim, J. (2013), Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human-Computer Studies*, **71**(9), 862-877.

Lewis, C. H. (1982). *Using the "Thinking Aloud" Method In Cognitive Interface Design* (Technical report). IBM. RC-9265.

Maurice, M. P. (1962). Phenomenology of perception. *Trans. Colin Smith. London, New York: Routledge & Kegan Paul*.

McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *Isjlp*, *4*, 543.

Moor, J. H. (1990). The ethics of privacy protection. *Library Trends, 39(2), 69-82*

Moor, J. H. (1997). Towards a theory of privacy in the information age. *Acm Sigcas Computers and Society*, *27*(3), 27-32.

Macnish, K. (2018). Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World. *Journal of Applied Philosophy*, *35*(2), 417-432.

MyData declaration, www.mydata.org

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviours. *Journal of Consumer Affairs*, *41*(1), 100-126.

Reynolds, B., Venkatanathan, J., Gonçalves, J., and Kostakos, V. (2011), Sharing ephemeral information in online social networks: privacy perceptions and behaviours. In: *Proceedings of the 13th IFIP TC13 Conference on Human-Computer Interaction* (INTERACT 2011), September 5-9, Lisbon, Portugal.

Rosenberger, R., & Verbeek, P. P. (2015). A field guide to postphenomenology. *Postphenomenological investigations: Essays on human-technology relations*, (p.9-42) London: Lexington Books, 2015, ISBN 978-0-7391-9436-2.

Taddicken, M. (2014), The 'Privacy Paradox'in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. *Journal of Computer-Mediated Communication*, **19**(2), 248-273.

Tavani, H. T., & Moor, J. T. (2001). *Privacy protection, control of information, and privacy-enhancing technologies* (pp. 378-391). Sudbury, MA: Jones and Bartlett.

Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy*, *38*(1), 1-22.

Verbeek, P. P. (2005). *What things do: Philosophical reflections on technology, agency, and design.* Penn State: Penn State University Press, ISBN 0-271-02539-5 (264 pp.)

Wakefield, R. (2013), The influence of user affect in online information disclosure. *The Journal of Strategic Information Systems*, **22**(2), 157-174.

Westin, A. F., (1967). *Privacy and freedom* (Vol. 1). New York: Atheneum.

Westin, A. F., (1991). *Harris Louis & Associates. Harris-Equifax Consumer Privacy Survey*. Tech. rep, Conducted for Equifax Inc. 1,255 adults of the US public.

Schermer, B. W., Custers, B., & van der Hof, S. (2014). The crisis of consent: How stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology*, *16*(2), 171-182.

Slovic, P., Finucane, M., Peters, E. and MacGregor, D.G. (2002). The Affect Heuristic. In: Gilovich, T., Griffin, D.W. and Kahneman, D. (eds), *Heuristics and Biases* (pp. 397-420), Cambridge University Press.

Solove, D. (2008). Understanding privacy.

Sunstein, C. R., & Thaler, R. (2003). Libertarian paternalism. *American Economic Review*.

Zafeiropoulou, A. M., Millard, D. E., Webber, C. and O'Hara, K. (2013), Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions? In: *Proceedings of the 5th Annual ACM Web Science Conference*, May 2-4, Paris, France.

Appendix: Case study Methodology & Results

Method

Design

Within this short study two Personal Data Management platforms, Schluss and Blauwe Knop were tested on usability, privacy experience and consent management. For the former and the latter, thinking aloud experiment was conducted in order to perceive the behavioural patterns of the participant. This behavioural and quantitative data was completed with a semi-structured indebt interview consisting of intentional and attitudinal data. The interview also went in debt on the privacy experience of the participants. Conclusions were drawn in combination with a privacy profile, categorizing the behavioural and attitudinal concern for privacy. Resulting in Design recommendations for each platform individually.

Schluss

The first pilot study is called Schluss, which needs to impose the nature of the application; a vault. Within this pilot study, Schluss is used by the Volksbank to arrange consent management and easy data flow from student debts stored by DUO in order to apply for a mortgage. Schluss is a third party organisation which the user can use to retrieve personal data and transfer this to the desired party. Schluss tries to aim for user-centred design in which the user has more transparency and control on the data flow. Moreover, this data transfer is much quicker than the paper version used nowadays, which can take up to six workdays. Schluss asks the user to provide consent to access the student debt data from DUO and again asks consent to share this data with the Volksbank. Meanwhile, the data is stored within Schluss. Users are able to create a vault which can be accessed later on with a pin code. In the future, Schluss can also be used to store and transfer data to other parties. Within the vault, users can overview which parties have access to what kind of information undue any prior consent arrangements.

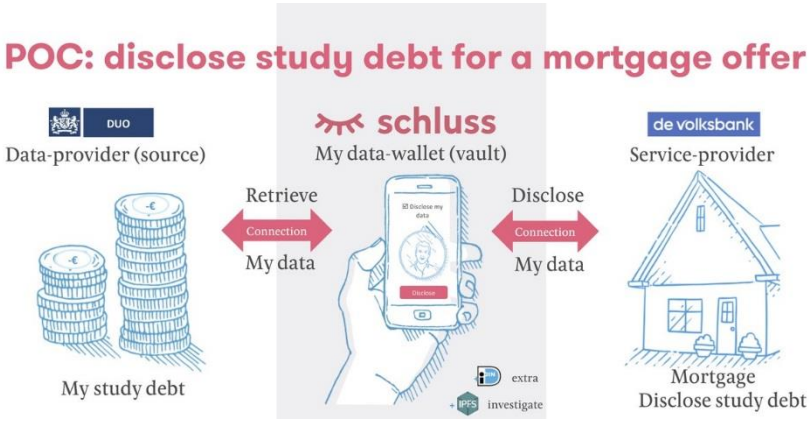


Figure 5. Model of Schluss POC

Participants

Within the case of Schluss, PDM is used to transfer financial data in the context of a mortgage application. The main option now available on Schluss is the transfer of student debts from the governmental organization of DUO towards the mortgage provider, the Volksbank. To match this environment the criteria of recruiting the participants was aimed at getting starters on the housing market, in the phase of applying for a mortgage and who are or previously were students using services provided by DUO. After the cancellations of the male participants, only female participants remained. Participants ranged in age from 24 to 28 years old (M=25.75 SD=1.11).

Setting and apparatus

The user study for the Schluss case was done in a small office resembling an office of a mortgage broker. This reconstruction needed to take place as there was no opportunity to make the user study a part of an actual mortgage application meeting, as this would interfere too much with the actual purpose of the meeting. Within the small room, one table with and two chairs were available, one for the supposed mortgage broker and one for the participant. The experimenter or observer was sitting in the corner of the room, looking over the shoulder of the participant.

During all phases of the user study audio recording was used. This was done on an iPhone 8. The participants were asked to bring their own smartphone. The mortgage broker provided a QR-code on his smartphone which the participant needed to scan through the use of their smartphone camera. To access the student debt the participant needs to log in with their DigiD. However, within the pilot study, this was still not available. Instead, the participants got the same login screen but a standardized DigiD account.

Measurements

Thinking Aloud

The first part of the user study consists of a walk through the Schluss application. During the actual use off the Schluss application, the participant is asked to think out loud and to be very elaborate and clear on what he/she is doing, what is unclear and why he/she is taking certain actions. Within this thinking aloud method the experimenter is not to interfere too much with the actual usage of the application. The experimenter is only allowed to stimulate the aloud thinking and the elaboration of reasoning (Lewis, 1982). The whole walkthrough is audio-recorded and the experimenter makes notes on the performed behaviour of the participant while using the application. The experimenter will especially pay attention to the time to complete the whole walkthrough, the number of errors and hesitations made, the kinds of errors or hesitations made and the time taken to provide consent. The participant is asked to act as if the setting is a real-life mortgage application with the Volksbank. The mortgage broker will get out his smartphone showing a QR-code to the participant who then is asked to scan the QR-code with his smartphone camera which will open a link. The dashboard of Schluss is shown on the participant's phone. It states that the Volksbank is doing a data request in favour of the mortgage application and would like to have insights into the participant's student debt stored in DUO. The dashboard also shows that this request is one-time only and the participant also has the option to abort the request. When the button "ophalen" (retrieve) is clicked the screen is transferred to the login screen of DUO. Here the participant is asked to log in with their DigiD. At the moment this only provides a demo version in which the participant needs to log in with a set account. The participant is asked to perceive and act as if this account is their own accessing their own data. After pressing "inloggen" (login) DUO will show a request screen in which the participant is once again informed about the request from Volksbank to share the participant's current student debt with the Schluss application. The amount of current student debt is also shown. After pressing "Delen met Schluss" (share with Schluss) the participant is transferred back to the Schluss page in which the student debt is now checked and labelled "in kluis" (inside vault). When the participant presses "indrukken voor akkoord" (press to confirm) the final page of Schluss is showed which states that the data request is completed and the Volksbank has received the participant's student debt. This confirmation is also shown on the screen of the mortgage broker.

Privacy experience

After the participant has used the application the mortgage meeting/story is rounded up and the third part of the user study starts. The experimenter will ask the mortgage broker to leave the room after which the semi-structured interview surrounding the privacy experience is started. This semi-structured interview tries to accomplish several results; A added value of the concept and its parts, with its sub-results of A1 User acceptance and A2 usability, clarity questions. It addresses questions such as *"What kinds of properties or functions should you add or adjust to the application?"* and *"Did you experience enough clarification within the application itself?".* B definition of privacy concerning personal data with its sub-results of B1 feeling of control on personal data, B2 feeling of insight/transparency of personal data, B3 feeling of protection of personal data. With all the sub-questions there is a baseline question asked within the privacy profile questionnaire. Questions, for instance, are: *"Do you have the feeling that parties you don't want to obtain your personal data can now less easily do so?"* and *"Do you got the feeling that you now have more insight into who receives and is in possession of your personal data?"* The third category concerns external effects. C1 influence on actions concerning data transfer and consent, C2 influence on trust concerning parties involved in data transfer, C3 influence on the transparency of data flow and understanding of the process. It addresses questions such as; *"Do you feel like you consciously considered the consequences of providing consent before you agreed to do so?" "Do you feel like you had enough knowledge to rationally make this decision?".* All premade questions, in order of appearance, can be found within Appendix A. The questions done during the actual interview can derive slightly from these in Appendix A due to the semi-structured nature of the interview. The transcribed interviews can be found in Appendix B.

Privacy profile

The last part of the user study consists of two small sets of questions. The first indicating the level of concern concerning online privacy and the second indicating the level of technical actions taken to ensure online privacy and thus also has a critical component of technical skills. To accomplish the first the Privacy Concern Index established by Westin was used (Westin, 1991). While this index is rather old and not developed for online privacy concern the Buchanan paper shows the validity of the often used Westin index in the digital age (Buchanan, 2007). Within the short questionnaire, the participants are asked to indicate whether fours statements are in line with their way of thinking. When answered yes none till one time the participant is ranked as privacy unconcerned. When answered yes two times the participant is ranked as privacy pragmatist and finally when selected three or four statements the participants are classified as privacy fundamentalists.

Buchanan (2007) also showed the importance of technical skill in describing the online privacy profile, which did not have a significant correlation with the Westin index. This 6 question scale is therefore also included. The six questions are answered on a 5-points Likert-scale ranging from never till always. Questions, for example, are; "how often do you delete cookies" in order to secure your online privacy the technical skill of knowing how to delete your cookies is required.**Fout! Bladwijzer niet gedefinieerd.** The complete questionnaire can be found within the appendix A. The scale was validated using Cronbach's alpha and had internal reliability of $\alpha = 0.66$ $M=3.58$ $SD=.54$ The mean score was taken to develop the variable Techscore.

Procedure

The participants are asked to sit down at the table in front of the mortgage broker and are given the information sheet and the informed consent. After reading both the documents the experimenter

asks whether everything is clear and if they have any remaining questions. After answering the questions asked the experimenter starts off with five interview questions concerning privacy to set a baseline. From this point forward the study is audio recorded. Next, the experiment introduces the first part of the user study, the thinking aloud experiment. The experimenter tells the participant that he or she is at a meeting to apply for a mortgage and introduces the mortgage broker. The experimenter tells the participant to pretend and imagine that it is a real meeting and they really want to get approval for their first mortgage and that he or she is asked to share their own data concerning the student debt using their own DigiD. The participant is told to listen to the instructions of the mortgage broker and while using the application to think out loud, saying what and why they are doing certain actions, tell when they do not know for certain what to do and when something is not clear. They are instructed to be elaborate as possible. The walk through the application will take no more than 5 minutes, depending on how long the participant will take to consider providing consent. The walkthrough will be observed by the experimenter who will log the time, count the hesitations, indicate how long consent giving takes and what kinds of struggles are countered. The second part of the user study will take up to 30 minutes. This part consists of a semi-structured interview done by the experimenter. The mortgage broker is asked to leave the room before the start of the interview. During the interview the experimenter takes notes. After the interview is completed the participant is asked to fill in a short questionnaire containing the privacy profile. The printed questionnaire is taken individually and collected by the experimenter. This short questionnaire does not take longer than one minute. The participant is debriefed and informed with the possible outcomes of the study.

DUO Blauwe Knop

Even though DUO is also part of the Schluss pilot, it also has its own Personal data management system, called de Blauwe Knop (Blue Button). Instead of using a pull-model such as Schluss the Blauwe Knop usage a push-model. This means that the user personally retrieves the information from DUO when needed instead of providing consent for another party to pull this data from DUO as in the case of Schluss. With the Blauwe Knop users remain totally in control over their data as it is downloaded onto their own personal computer in a PDF or XML format. The data can when needed to be digitally sent to parties of choice. This needs to be done manually by the user themselves. When the data is printed the authorization stamp of DUO expires. The PDM is set up for current and former students to provide easy access and overview of their student debt data.

Participants

DUO (Dienst Uitvoering Onderwijs) is the executive agency of education which is used by students and former students within the Netherlands to arrange their study loans. To fit this case the participants were selected on the criteria that they currently are students or were so in the past. Moreover, the participants needed to have a remained study debt at DUO. No other restrictions on the recruitment of the participants were made. All participants who reacted to the invitation were female, ranging between the ages of 19 and 21 (M=20 SD=.58). All the participants were current students and have an ongoing loan at DUO, hence a growing student debt.

Setting and apparatus

The user study took place at the participant's home to create a realistic environment which matches the actual usage environment. The Blauwe Knop will primarily be used from a private environment accessed from someone's own computer or mobile device. Within the user study, the participants

were asked to use their own laptop to cancel out any usability issues with the device itself and trust issues concerning downloading of the privacy-sensitive content.

Measurements

Thinking Aloud

The first part of the user study consists of a walk through the Blauwe Knop interface. During the actual use of the Blauwe Knop application, the participant is asked to think out loud and to be very elaborate and clear on what he/she is doing, what is unclear and why he/she is taking certain actions. Within this thinking aloud method the experimenter is not to interfere too much with the actual usage of the application. The experimenter is only allowed to stimulate the aloud thinking and the elaboration of reasoning (Lewis, 1982). The whole walkthrough is audio-recorded and the experimenter makes notes on the performed behaviour of the participant while using the application. The experimenter will especially pay attention to the time to complete the whole walkthrough, the number of errors and hesitations made, the kinds of errors or hesitations made, the time is taken to provide consent and whether actions are taken to open information boxes. The participant is first asked to log in with their personal DigiD, they can choose whether to use a verification through SMS-code or to use the DigiD app. When the SMS-code is chosen the participant is asked to fill in the six-digit code sent to their mobile phone in the login screen and click next. With the DigiD app, participants can log in with a pin code after which a matching code is shown which needs to be filled in on the computer screen. A QR-code appears on the computer screen which needs to be scanned with the smartphone. The application shows that you want to log in at DUO and after pressing log in the pin code can be entered to do so. The application gives notification of the successful login. Next, the participant is asked whether he or she is trying to login to DUO for themselves or to arrange things for a third party. After pressing “verder” the main screen “schuldoverzicht download” is shown. In this window, participants can view their personal information, download their student debts (Blauwe Knop) and click for more information on kinds of debts and privacy. After exploring the extra information the participant needs to click “download schuldoverzicht”. A new screen pops open in which participants can choose the kind of output, now only the option of pdf is possible but it does ask for a new consent with the button “download”. There is however some clarification provided when clicked on “wat moet ik kiezen” which states that the pdf only remains its authentication stamp of DUO when used online. Which expires after printing the pdf. Finally, a pop-up screen appears which thanks the participant for downloading, states the download is situated in the download folder and asked to provide feedback on the application. The participant has to open the file and scan whether this information is correct.

Mental model

After the participant has used the application the third part of the user study starts, the semi-structured interview surrounding the privacy experience and the mental model of the application is started. This semi-structured interview tries to accomplish several results; A added value of the concept and its parts this includes the understanding of the participant of the mental model and concept. Moreover, it includes the possibility of new application areas. It addresses questions such as *“Would you like to use the application for other services such as switching of a general practitioner, mobile provider or webshop?” “Do you understand what the Blauwe Knop has done?”* B concerns privacy consent management and external effects. A baseline concerning the feeling of control, insight and transparency and protection of personal data are asked prior to the walkthrough. *“Do you have the feeling that parties you don’t want to obtain your personal data can now less easily do so?”* and *“Do you feel like you consciously considered the consequences of*

providing consent before did so? The last category is usability; *"Did you experience enough clarification within the application itself?" "How did you experience the usage of the application"* All premade questions, in order of appearance can be found within Appendix A. The questions done during the actual interview can derive slightly from these in Appendix A due to the semi-structured nature of the interview. The transcribed interviews can be found in Appendix B.

Privacy profile

Finally, the same privacy profile is conducted as done with the Schluss application to classify the participants based on their level of privacy concern and technical ability to protect their information online.

Procedure

The participants are asked to sit down at the table and are given the information sheet and the informed consent. After reading both the documents the experimenter asks whether everything is clear and if they have any remaining questions. After answering the questions asked the experimenter starts off with five interview questions concerning privacy to set a baseline. From this point forward the study is audio recorded. Next, the experiment introduces the first part of the user study, the thinking aloud experiment. The participant is introduced to the storyline in which he/she wants to access their student debts in order to send it to a third party for new services or to get insight. The participant is instructed to use the application by clicking on the link on their personal laptop and walking through the user interface. While doing so to think out loud, saying what and why they are doing certain actions, tell when they do not know for certain what to do and when something is not clear. They are instructed to be elaborate as possible. The walk through the application will take no more than 5 minutes, depending on how long the participant will take to consider providing consent. The walkthrough ends after opening the downloaded file with the participant's student debt. The walkthrough will be observed by the experimenter who will log the time, count the hesitations, indicate how long consent giving takes and what kinds of struggles are countered. The second part of the user study will take up to 30 minutes. This part consists of a semi-structured interview done by the experimenter. During the interview the experimenter takes notes. After the interview is completed the participant is asked to fill in a short questionnaire containing the privacy profile. The printed questionnaire is taken individually and collected by the experimenter. This short questionnaire does not take longer than one minute. The participant is debriefed and informed with the possible outcomes of the study.

Analysis

No word by word transcription including verbal interpunction was done. In order to save time, the recorded interviews were transcribed by mostly using the own words of the participants, but only reporting relevant information and summarizing the answers to some extent. After transcription, the most relevant information per question was put in Excel sheets which provided a clear overview between the different answers per participant per question. Information regarding any recommendations for the PDM was marked red and answers containing information for answering the hypotheses were marked green. For each application, the answers of the four participants were compared and analyzed. The notes taken during the Thinking Aloud experiment were worked out and analyzed in combination with the time taken to complete the walkthrough, the time to provide consent and the privacy profile. The technology capability score from the Buchanan (2007) paper was conducted from taking the mean of all six questions. The scale was validated using Cronbach's alpha and had an internal reliability of α=.6635 M=3.58 SD=.54. Conclusions for design

recommendations were drawn on the basis of the interview and thinking aloud analysis, capturing both the explicit and implicit answers of the participants as their actual behaviour. The results were split up in usability and privacy concerning paragraphs (including trust, control, security, insight/understanding, privacy and privacy paradox). In the former, the design recommendations were given in order of appearance in the application flow. In the latter, these issues were discussed more indebt content-wise and showed how to improve these issues by referring to the Design recommendations stated above.

Results

Privacy profile

For all the different pilots taken together with the Westin score was highly significantly correlated with the mean technical capability score, $R=0.80$ $p<0.05$

Schluss

Among the 4 participants, the three categories were evenly distributed there were two people ranked as privacy unconcerned (one filling in one answer and the other selecting none). One as privacy pragmatist and one as fundamentalist. These classifications were obviously mirrored within the in-dept interview through the experienced privacy, the trust level and the number and kinds of recommendations made to improve the application. See the subsections within the privacy experience interview for more elaborate results. The fundamentalist also took the most time providing consent for both Schluss and the Volksbank. The unconcerned had the lowest technical capability score.

Tech score: M=3.58 SD=.54

DUO Blauwe Knop

Among the 4 participants, all categories were represented. Two people were ranked as unconcerned one as pragmatist and one as fundamentalist. The fundamentalist stood out as she took remarkedly more time to provide consent (both for pressing the first and the second download button) than the other participants while still having the lowest overall time to complete the application. Moreover, the fundamentalist had the highest technical capability score. The Westin classification was less reflected in the privacy experience interview than it was for the Schluss application. Ass the participants were less divided in their answers than they were at Schluss.

Tech score: M=3.25 SD=.42

Thinking aloud

Schluss

Most participants went very quickly through the application and spend around two minutes completing the data request. One participant's completion time was around four minutes due to a very extensive wait for the vault to be created and due to a more thorough reading of the information on the screen. No participants made any obvious hesitations. However, there were some common mistakes. Everyone mistook the checkbox in round 5 to be clickable and were confused when this did not seem to be the case. Moreover, 3 out of the four participants did not see the notification that the accept button needed to be pressed for 3 seconds. One participant wanted to change the time of consent, while not optional. Finally, three participants mistook the arrow on the final screen for a button, behind which more information would be placed. Two of the

participants read the information sheets at the beginning and none of the participants clicked on the terms, 3 of which did not even see the option to do so. All the participants considered the time to create a vault took too long.

DUO Blauwe Knop

Just like the Schluss application, all participants were very quick to complete the walkthrough and did so in around two minutes. They spend very little time reading the information provided and quickly pressed the buttons to go through the application and to download their student debt and personal data. Only one participant bothered to read one of the three drop-down menus with exploratory data. Therefore all participants were unaware of critical information for the usage and downloading of the PDF. The results showed were all incorrect according to the participants. They all currently have a loan and thus a debt at DUO. However, the file stated, “there are no longtime debts known”. This could be due to the fact that all participants are still in college and thus are not obligated to start paying off their debt. However, these debts do not fall under one of the criteria mentioned for leaving it out of the debt on the downloaded form. The error confused all the participants and made the use of the application less relevant. All participants were confused about the options button with only one option. With two participants the wrong site popped up after logging in. One mentioned “session expired” and the other went to the normal site of DUO. It was not clear how to go back to the original site. None of the participants clicked the feedback button. One participant became confused as she used her previously installed option to only open the document, while the screen stated that the downloaded file was placed within the download folder.

Privacy experience

Schluss

<u>Usability</u>

Overall the participants experienced the Schluss application as easy and pleasant to use due to the easy user flow, the pictures and the friendly colours. The walkthrough was very clear and the information screens at the beginning and during the wait of the vault creation made the concept of Schluss more clear. However half of the participants did not bother to read these information sheets. And even when read there were still a lot of hesitations and uncertainties about the role of Schluss. Mostly concerning the storage of data within Schluss.

Design 1: implement an explicit notification that Schluss does not store the data prior to retrieving data. Include how users can be certain about the trueness of this statement

Moreover, multiple participants would like more background information on Schluss and its aims. This can be provided in a more elaborate text which is optional to go through a menu. Due to this optionality users are not forced to read the more elaborate information when not interested but users who have the possibility and freedom to do so.

Design 2: implement a menu in which the user can find more background knowledge in plain text on Schluss and its goals and aims

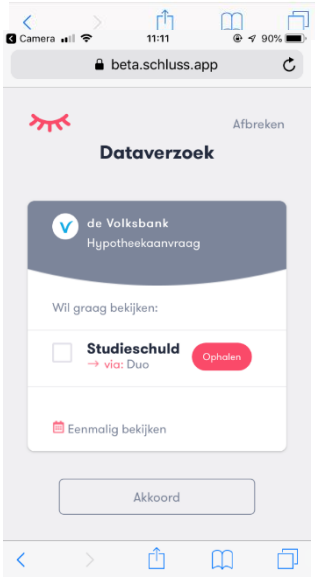
Going further in the application, only one of the participants saw the option to see the terms. Most of them also mentioned that they were not looking for it but did consider it too unobvious. It is important for users to have the freedom to choose whether or not to read the terms and conditions. But in order to have this choice, it needs to be noticeable for all users.

Design 3: slightly more emphasis on the terms button

Multiple participants were confused about whether or not the vault was personally linked. The pin code was often mistaken as a vault code and thus considered as an account code. Participants questioned whether others could log in on their vault when chosen the same code number. In this way, the 5-digit pin code was not considered to be safe. Participants would like to have a personal account preferably secured with their DigiD. DigiD has a very valued reputation among the participant as it represents trust, security and safety. Moreover, it is associated with serious actions considering important data. Implementing to raise the trust level and also to raise more awareness of carefully thinking about providing consent.

Design 4: create login account through DigiD instead of pin code to access the Schluss application/vault

The creation of the vault took in all cases quite some time. One participant looked for ways to aboard the creation of the vault as it took nearly one and a half minute. The participant assigned the long waiting time to the limited network reception of her mobile phone. The information screens were however considered as a pleasant distraction during the waiting time.



Design 5: Reduce time to create a vault

As mentioned in the thinking out loud section, all participants made the mistake to click on the checkbox in the first screen concerning the data request after logging in. participants mentioned that this confused them as they did not understand why the checkbox was in place when it was not clickable. Only after trying the checkbox multiple times the participants continued to search for a new button to click. The button “ophalen” was then correctly clicked. Participants suggested to remove the checkbox if it did not have a purpose, or make it clickable so that the participant has to check the

student debt after which the “ophalen” button should be clicked. The latter should then not be placed behind the data request but below the list of multiple requests as the big “Akkoord” button and leaving that one out on this particular screen.

Design 6: Make checkbox clickable in order to make participant conscious of what to data to share. Replace the “Ophalen” button with the “Akkoord” button.

All participant wanted to be able to change the “eenmalig bekijken” in order to provide a clear understanding of how long the parties involved are allowed to view the data. Moreover, participants also wanted the option to withdraw their consent. Removing any uncertainties of potential storage of data by both Schluss and the Volksbank and providing more control and insight into their personal data.

Design 7: Make “eenmalig bekijken” adjustable and an explicit button

Not all participants were conscious that they shared their student debt with Schluss. In order to improve this, there should be more emphasis on the first consent button, the one providing consent to retrieve it from DUO and share it with Schluss. Participants mentioned that this was more troublesome than the later screen in which they shared it with the Volksbank as that was the main goal of the use of the application. They needed to provide the student debt with the Volksbank anyway in order to be able to apply for a mortgage. Participants thus mentioned that the final screen was not the one where they needed to consciously think whether or not to share their personal data but that this in fact needed to be done one screen earlier. In order to accomplish this conscious deliberation and decision making a checkbox should be installed in the DUO screen stating an explicit warning that users are about to share their student debt with Schluss. After checking this box users must then click on a share button.

Design 8: Create more emphasis on consciously sharing data with Schluss. Create checkbox which explicitly mentions that student debt will be shared (and stored) with Schluss. Share button can only be clicked after checking the box.

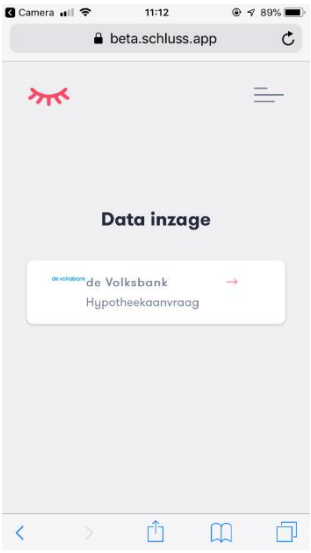
Most participants had a clear understanding of what data they had shared while using the application however one participant mentioned that student debt is not just one number. Is multi-layered, containing different numbers within the old and new system matched with different interest percentages and different instalments. Some of which also can be transferred into a gift after graduation. The application was not clear on what the number shared represented.

Design 9: Provide more elaborate information on what part of the student debts is shared, splitting out debts in different systems and those which still can be transformed into a gift. Create an option to choose which parts to share and recommend which once are needed for certain applications.

All but one of the participant did not see the “hold 3 seconds to consent” notification.[3] Some participants found this requirement strange while others mentioned it to be well thought of as they now did not click the “Akkoord” button by mistake. However, due to the fact that most participants did not see that the button must be pressed for 3 seconds after they did find out, they were more busy with getting the action right then consciously thinking about what the action actually entailed and the consequences of providing consent. This can be solved by putting the explanations of the 3 seconds action above the button. Or to replace the button with a more conventual manner of providing consent; creating a checkbox with an explicit warning.

Design 10: Move the explanation of the 3 seconds action above the button. Or replace the 3 seconds safety with a consent box and explicit warning.

Within the final data insight screen, all but one participants tried to click on the arrow behind the data transfer of the Volksbank. The arrow indicated that there was something behind this box and that it served as a button. Participants mentioned that they were expected to find a more detailed overview and explanatory information of the data transfer when clicking the arrow. They were confused and disappointed when the arrow turned out to be unclickable and were unable to see more details of the data transfer.



Design 11: Make the arrow on the data insight screen clickable which results in more detailed information about the data transfer.

Participants were positive about the overview provided by the last screen. They understood that more data transfers would be placed here when made. It provides a clear insight into what is shared with whom. However, all participants stated that they wanted the ability to withdraw their consent. This can be implemented on this overview page. Moreover, one participant suggested that this page should be shown at the beginning of the application, before showing the new data request. This would provide more ease and time to get familiar with the application instead of jumping right into the data request. This time is essential for the user to become conscious of what the application does and requires them to do. The decision of consent will thus be taken more seriously and will be given more conscious deliberation. Within this start screen, previous consents of data transfers can be shown and adjusted. Moreover, new data request will be pop up as notifications. By clicking on the new data request the original first screen will be shown, displaying the details of the new request.

Design 12: Implement consent withdraw button in “data inzage”

Design 13: implement “data inzage” as start screen after logging into the vault. Showing previous data transfers and the ability to adjust them and provide notification for the new data request.

[3] As the 3-second button was an recent update in the design and was also quickly taken out, I was unable to get a screenshot in which it was present.

Trust

Many participants are still quite sceptic about Schluss and the company behind it. Their trust in both the application and the company will be better when Schluss is more common in use among friends and relatives but also by different companies besides the Volksbank. Brand awareness places a huge role in the habituation of trust. This can be improved by commercials in any kind and valued reviews online. Participants want to be able to google Schluss and find elaborate information on the firm, what it does and what its goals and aims are. Participants mention that if Schluss was a governmental tool, like DigiD that they would trust it more. Private organisations are thus considered less trustworthy due to personal gain and profit. When the government will implement Schluss and therefore shows its trusts in the application, for instance by linking DigiD to the vault, participants are far more likely to trust Schluss.

Control

Participants had very different opinions on the control Schluss provided them and correlated with the assigned privacy classification. The two privacy unconcerned mentioned that they had more control due to the Schluss application. They mentioned that due to this enhanced control it was easier to get insight into the flow of data and to be sure no unwanted parties were involved. Moreover, only specific information was transferred. This provided a feeling of more safety. However, the other two participants ranked as privacy pragmatist and privacy fundamentalist experienced less control due to the application. They both considered Schluss as a third person on which they had no certainty hence no control. Moreover, the Internet is seen as a black box on which the user has no control and no insight into the data flow and its receivers. However, all participants agreed that the user has no control or freedom in what to share. This path is restricted due to the fact that it is already laid out by Schluss. All participant wanted more options to choose from both in what to share and for how long, see Design 7, 9, 12 and 13.

Security

Only one participant thought that the data was better protected through the use of the Schluss application. Two stated not to think that it was any different also not less. One participant stated that the data transfer felt less secure due to the pin code, see design 4.

Insight/understanding

All participants noted that they had a clear insight in which parties received their information. However, in both the cases of Schluss and Volksbank, they remained uncertain which direct person received the data and is now able to access it.

Privacy

The two privacy unconcerned stated to experience more privacy when using Schluss due to the fact that they were the ones transferring the data. More importantly, the data was limited to the actual data which they wanted to transfer and fewer people were able to get to this data without them knowing. The privacy unconcerned thus defined privacy mostly as control, both control on what is shared and who receives the data.

The pragmatist and fundamentalist experienced less privacy due to the uncertainty of the Internet and the actions behind Schluss. This uncertainty is also reflected as less control on their personal data and both participants thus defined privacy as control. To improve this lack of control or

uncertainty more information on Schluss can be provided, see Design 1, 2 and 8. These findings support hypothesis 1.

Privacy paradox

All participants chose ease and usability above privacy. The two privacy unconcerned stated that they did not feel that they are important enough for other parties to violate their privacy and do something with their data. They perceived their data as no use to others and did not see any potential threats. The pragmatist firstly mentioned privacy as she did not feel any bother to go through more lengths to be informed properly and thus to secure her privacy. She did mention that she attributes more value to her medical data then student debt due to possible consequences of that information becoming public. The fundamentalist chose privacy above ease and usability however showed in her later answers that she seeks comfort in ease more than she actually values her privacy.

All but one privacy unconcerned mentioned that they indeed went very fast through the application without explicitly thinking about the consequences of consent. They stated that this was indeed due to the ease and usability of the user interface and -flow of the application.

> *"The button was so big, so present that I just pressed it because it screamed to be clicked."*

> *"Ehm… Yes. Yes, you are right… I did indeed click without thinking, how terrible… I feel ashamed."*

The privacy unconcerned mentioned that from the beginning of the application for a mortgage she knew she had to provide consent so that it does not matter in which way she did so, even though it was indeed easy. With this and the uncertainty concerning Schluss in mind, there must be more focus on sharing the data with Schluss, see Design 8. The 3 seconds button was a good effort for users to more consciously press the consent button but due to the unconventional design element, it backfired. To improve this Design 10 can be implemented.

There was a high correlation between the technical ability score of the participants and the time of consent given to Schluss to retrieve the data from DUO. Stating that when people are more likely to protect their privacy online through technical skills they are more likely to take a longer time to consent.

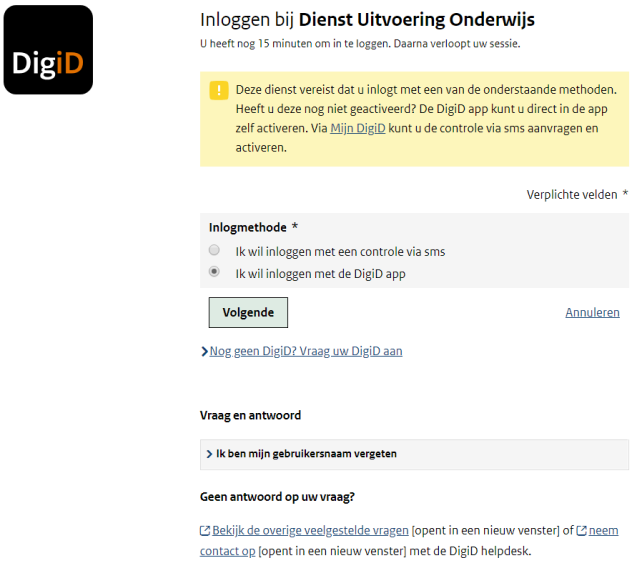
The privacy unconcerned both stated that they feel that when systems like Schluss become more common in use and are used for different data transfers, people will become more aware of providing consent. This opinion was mostly based on the fact that users gain more control and a better overview of the data flow and the parties involved due to the application. With as main condition that the overview page (Design 12 and 13) will be implemented at the beginning of the application. Both the unconcerned however do mention that this opinion counts for themselves. They do feel like other people, for example, people with lower education, are more vulnerable to the ease of providing consent without actively thinking about the decision and being aware of the consequences. In this way, they do state that this can form a big problem which needs to be foreseen. Both the pragmatist and fundamentalist think that using the platform of Schluss on a large scale can cause tremendous problems due to the thoughtless thinking of people which is reinforced by the ease and usability of the interface. As mentioned Design 12 and 13 can be implemented to foresee this problem to some extent. Moreover, Design 1, 4, 6, 7, 8, 9 and 10 will also contribute on making the user more aware of the severity of the situation, make them act to think about their

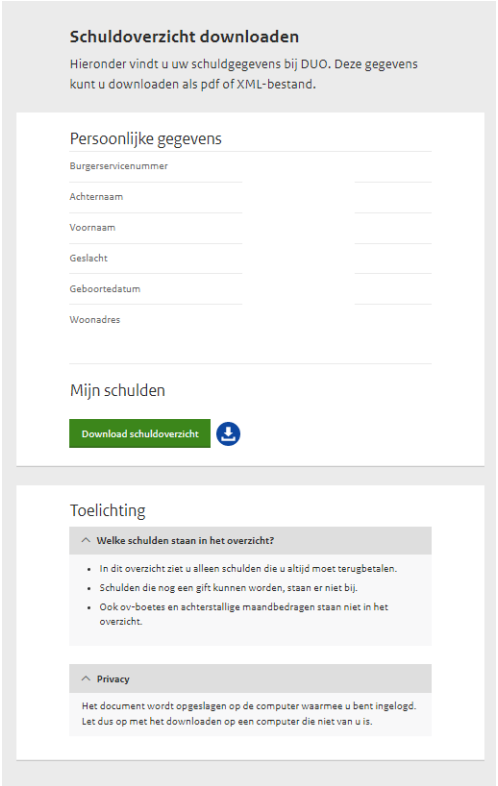
actions and thus lower the usability and ease of flow to enhance awareness and privacy experience. The results presented above support hypothesis 2.

DUO Blauwe Knop

Usability

Overall the participant went very quickly through the walkthrough. When asked they all responded that the flow of the application was very easy and clear. They knew where to click next. All participants mentioned experiencing a safe and secure feeling due to the two-way verification of DigiD with SMS or DigiD application. They were all familiar with DigiD, logging in through SMS and the option to log in for themselves or as a representative. When going to the main screen all participants mentioned that they had seen the explanatory information headings. However, only one participant bothered to open the debts drop-down menu, which was also not completely read. The privacy drop-down menu was never clicked on. Participants mentioned that it did not seem important nor relevant or connected to the downloading of the student debts due to the placing of the information at the bottom of the page and the separate box it was in. Moreover, they mentioned that they did not need extra guidance for an easy download and did not need to read the privacy section as they trusted DigiD and DUO. After being asked to read the drop-down menus in the interviews all participants stated that they were unaware of the privacy statement that the document was stored on the laptop they were using and thus must be careful when using a computer which is not their own. Participants agreed that this privacy statement must be made more explicitly, in such a way that every user becomes aware of this fact. Moreover, it must be placed near the download button to create the association between the warning and the download button. Moreover, due to this close placement users are inclined to read the warning as they are drawn to the download button and therefore also notice the warning just above it. An explicit red exclamation mark before the warning can help to message the urgency of reading. The awareness of the consequences of downloading personal information is essential in reducing the privacy paradox and unconscious consent giving. By stating this warning the time taken to provide consent will expand,





creating more time to make an informed and deliberate decision. The chance of clicking consent just because there is a big button will significantly reduce.

Design 14: Make the messages of "toelichting" more explicit by stating the privacy statement as a warning explicitly above the download button. Create a warning sign (exclamation mark "!") in front of the statement

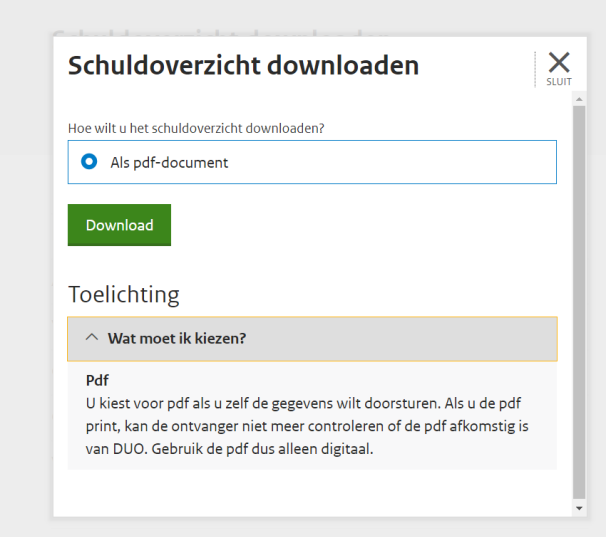
Participants perceived the explanation of debts less important than the privacy statement. However, did state that the explanation of different kinds of debts should be included above the download button to give users more the change of informing themselves. Due to the fact that it is now placed under the download button users already click download before scrolling down to inform themselves. Participants also wanted to know in more detail what they were going to download. They wanted to know the amount shown on the downloaded sheet before downloading. This insight provides the user with more control and awareness in their decision making concerning the download. This can be realized by implementing a screen before the current download screen. Showing the current debt and the debt which will be shown on the downloaded file. Within this screen, the explanation of "welke schulden staan in het overzicht" can also be shown as plain text without a drop-down menu. After reading which information about one's debt will be shown within the download the user can proceed to the download screen. Creating this overview page will besides more control and awareness also implement another action to be taken before turning to the download screen. In this manner, users are less rushed into downloading but are provided more time and space to inform themselves to make a deliberate action.

Design 15: create a new first page in which the current debt is shown and state the debt which will be visible in the download. Include the information of "welke schulden staan in het overzicht".

One participant mentioned that she found it strange that there were two download buttons next to each other. The sign for the Blauwe Knop is not recognised by any participants as such. However, they do recognize the download icon. The Blauwe Knop needs to become more familiar to the public in order to create the desired association and to erase the confusion of two similar buttons next to each other. Another way to resolve this confusion is to make the Blauwe Knop the only download button available.

Design 16: Enhance familiarity of Blauwe Knop or make it the only one available to click.

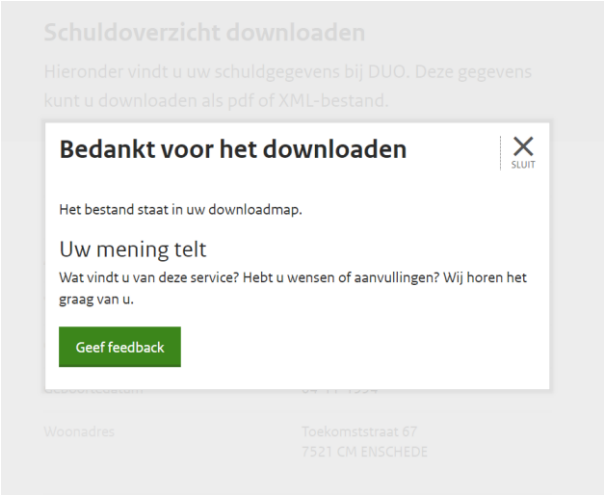
Participants were confused by the provided option on possible ways to download the student debt when there was only one option possible. Therefore many participants also mentioned that they did not see the point of opening the drop-down menu and reading the information on the digital authorization stamp of DUO which expires when printed out. When the participants were asked to read the explanatory text during the interview multiple noted that they did not expect this to be under the heading of "wat moet ik kiezen?". The heading did not capture any urgency to read it while the information is critical for everyone downloading the PDF. Moreover, none of the



participants read this same warning stated at the bottom of the downloaded file. Therefore none of the participants was aware of the fact that they were unable to physically distribute the downloaded file. This should be made more explicit, which can be done through a warning beside the PDF option with a red exclamation mark. Implementing this warning again will expand the reaction time of the user creating more room for informed and conscious action.

Design 17: Implement more download options besides PDF-document or erase the options button.

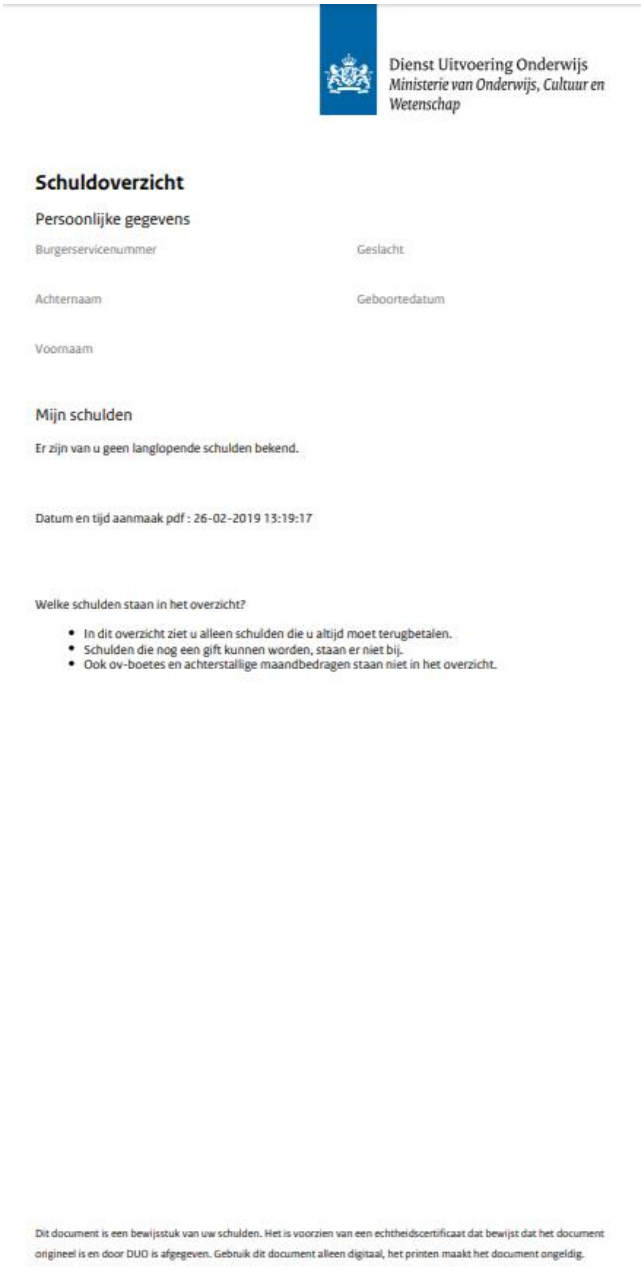
Design 18: replace the drop-down menu of "wat moet ik kiezen" with a short red warning about the inability to analogically send the document underneath the PDF option. Start the warning with a red exclamation mark.



On the final screen, none of the participants saw the line "het bestand staat nu in uw download map". All focus was captured by the big feedback button. Participants did not understand the connection between the download and the option to provide feedback. All participants, even though they did not read the instruction, were quick to find the document in their download map as this was a conventual manner of opening downloaded files. With some participants, the file also opened automatically and one participant chose the option to only open the file without downloading it. The automatic message of "het bestand staat nu in uw download map" created in this situation some confusion.

Design 19: Make feedback option and end of downloading process less connected. Create a separate pop-up for the feedback or create more distance between the two elements.

When opening the downloaded document all participants were surprised to notice that there were no long time debts known; “Er zijn van u geen langlopende schulden bekend”. While all participants currently had a loan which they entirely have to refund. Moreover, none of them received any debts which still could be transferred into a gift after graduation. Their loans thus did not fall under the restrictions for leaving out the debt on the downloaded file. This created quite some confusion, as participants did not know what to believe and where to find their actual debts. The error might be due to the fact that all the participants are still studying and thus have not started paying their debts. Moreover, their debt is still growing every month. However, this inclines that there is already a known debt which also needs to be accessible for the users while still being a student. While students might use the Blauwe Knop less, there are still cases in which students are buying houses on the salary of their partner or else. There is, therefore, no obvious reason why the Blauwe Knop application should not work for these participants.



Dienst Uitvoering Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap

Schuldoverzicht

Persoonlijke gegevens

Burgerservicenummer | Geslacht

Achternaam | Geboortedatum

Voornaam

Mijn schulden

Er zijn van u geen langlopende schulden bekend.

Datum en tijd aanmaak pdf : 26-02-2019 13:19:17

Welke schulden staan in het overzicht?

- In dit overzicht ziet u alleen schulden die u altijd moet terugbetalen.
- Schulden die nog een gift kunnen worden, staan er niet bij.
- Ook ov-boetes en achterstallige maandbedragen staan niet in het overzicht.

Dit document is een bewijsstuk van uw schulden. Het is voorzien van een echtheidscertificaat dat bewijst dat het document origineel is en door DUO is afgegeven. Gebruik dit document alleen digitaal, het printen maakt het document ongeldig.

Design 20: Create the possibility for current students to access their current student debt.

Besides fixing this error, the downloaded file must also provide feedback when possible errors occur. This feedback must handle some of the confusion and provide an explanation on where to find the desired information and solve any misunderstandings. The explanatory bullet points already do this to some extent but were experienced by the participants as incomplete and thus unclear as they were lacking background information for an uninformed user. The bullet point would be more clear when using examples of different student debts. For instance, comparing the old and new system and pointing out which parts of the debt are included in the downloaded sheet, preferably in a graphical manner such as a pie-chart. To keep the downloaded sheet more focussed on the essence this explanatory information can be referred to on the sheet by a hyperlink connected to the explanatory page created by Design 15. Within this page, the examples can be given. In this manner, the information is presented before any confusion can arise. However, does provide the possibility to go back to the information when issues remain unclear or when not read properly the first time. When the latter is the case, users will still have some recollection of seeing the graphic representation of the different kinds of debt. Helping them so relocate to the provided information.

Design 21: Create "voor meer informatie en voorbeelden van de hierbij getoonde en niet vertoonde schulden zie; http://..." this hyperlink will connect to the information page created by Design 15 and will include graphic examples of different kinds of debts which are and are not included in the downloaded sheet (pie-chart).

Trust

There was a good feeling of trust in the application. Most of this was due to the familiarity and associations made with DigiD and DUO. Participants trusted DigiD and DUO to a large extent as they are govern based and associated with "serious business". The double login through SMS-verification also contributes to the trust experienced. Moreover, participants mentioned that the more actions needed to be taken to complete the application the more trust they experienced. These increased steps felt as a guidance of the application to secure their privacy and awareness. Of course, the number of steps taken has its maximum at which the usability is compromised. However, Design 15 and 21 can help to increase the level of trust and comfort among users without harming usability.

Control

Most of the participants experienced more control over their personal data due to the set-up of the application. They apricated the fact that they were able to access their personal data and to manage who they send it to when needed. And most importantly, that this was all done on their demand and by themselves. The storage on their own laptop also provided a sense of control as they felt like they now "owned" the data. However, one participant mentioned that she experienced less control due to the need for the document to be transferred digitally. Yes, she would have control to whom she sends the document but did not experience any control on the possible interference of unwanted parties through the Internet while it goes through multiple channels. The level of control will also be enhanced due to the implementation of Design 14, 15, 18 and 21 which will provide more insight and understanding in the downloaded data and its consequences and thus more informed control on one's decision making.

Security

The point made in the section of control concerning the digital transfer was also represented as a feeling of lack of security (due to lack of control). Two participants, both privacy unconcerned made this point that they did not feel secure when sending the document digitally. Moreover, the storage on one's own laptop, while providing a better feeling of control, did negatively contribute to the feeling of security for half of the participants. They experienced their own laptop as unsafe and easily hackable. The other half of the participants did not feel like anyone would bother to hack their laptop and did not experience their laptop as unsafe. On the other hand, DigiD was mentioned to be very secure.

Insight/understanding

Participants experienced more insight into their personal data (even though this was incorrect) and the data flow due to the fact that they experienced more control over who received the data. Many participants were unaware of the height of their student debt before using this application. However as already stated in the previous two paragraphs there remained a lack of insight due to the digital nature of any possible transfers of the data. Moreover, participants mentioned that while they knew who they send the data, they had no insight nor control over who they forwarded it to. To enhance the insight of users on their data and the understanding of the data itself, the consequences of providing consent and the data flow, Design 14, 15, 18, 20 and 21 can be implemented. Due to the

enhanced insight and understanding, users will become more aware of what they are doing and the consequences of their actions. The extra time created by the implementation of the design recommendations 14, 15, 18 and 21 will provide more peace during the user flow. Providing the extra time and space needed for the user to consciously make an informed decision, instead of acting automatically triggered by the usability features of the design interface. Design 20 will contribute to expanding the population able to get more insight into their data by providing access to the Blauwe Knop application.

Privacy

The definition of privacy among the participants was very divided across the control and access camps. Two participants (privacy unconcerned and fundamentalist) experienced more privacy due to the enhanced control while another unconcerned experienced less privacy as she felt that her personal data was not more secured due to the digital transfer. And the pragmatist experienced more privacy due to the different actions taken before being able to download, this included the two verification of DigiD. In the latter case, less control was experienced as better secured hence better privacy. These results are not unanimous on the definition of privacy and thus cannot support hypothesis 1 completely.

Privacy paradox

One of the privacy unconcerned strait out mentioned that the preferred ease above privacy. The other participants struggled in making a decision. While two participants (pragmatist and fundamentalist) after some time also chose ease for most purposes they did prefer privacy with "important issues" such as banking. The participant left, classified as privacy unconcerned, stuck with privacy however during the interview implicitly chose ease over and over again. The main cause being no foreseeable threats at this moment in time. The latter participant, for example, did express that she saw no threat in someone obtaining her student debt, while she would pick privacy when more important information was shared. She gave the example of her BSN as being important information, one she would think more carefully before sending or downloading. It is important to note that this participant at the start of the interview explicitly mentioned that she had seen her BSN and was aware of downloading it. While at the end of the interview when asked whether she had downloaded the personal data with conscious deliberation she mentioned she did not in this case but would do so when more important information such as her BSN was shared or downloaded. Something which was in complete conflict with her actions as she actually also downloaded her BSN on the student debt sheet. This privacy paradox was also found within the answers of the other participants. While thinking back at their actions during the walkthrough they all admit to quickly and unconsciously pushed download due to the fact that it was easy to do and that they were drawn to the big button. Moreover, they all mentioned not to be thinking about the consequences of downloading and were not consciously aware of the fact that the downloaded file was now stored on their laptop.

The situation of Schluss, with a third person handling the data flow, was also sketched for the participants to provide a comparable situation. All of the participants preferred the set-up of the Blauwe Knop more than that of Schluss. The main reason being the relatively little more effort needed for the Blauwe Knop. While the set-up of Schluss provided a lot of unease in the form of distrust, less control and uncertainty. In this dilemma, all participants thus chose for privacy over ease.

Finally, all participants stated that when access and transfer of information would become this easy due to its digital user-friendly interface that providing consent would become an automated action as it is done so frequently. Managing one's consents on data flows all together would only enhance this automated unconscious behaviour. Another problem stated is the inability to use when no consent provided. This is something which is already happening with smartphone applications. In order to use Google Maps, you have to consent with sharing your location for instance.

These outcomes show that the Blauwe Knop is at high risk of reinforcing the privacy paradox due to the mediating nature of the user-friendly interface. Which supports hypothesis 2. Easy improvements in this area can be made by implementing the Design recommendations 14, 15, 18 and 21. As mentioned in the insight and control section, these improvements create a more calm user flow in which the user is nudged to consciously think about what he or she is doing and to be informed about the possible consequences. Instead of becoming a zombie following the intended user flow without being conscious of the actions taken. In this manner, there will be a higher constancy between the intention or attitude about privacy and the actual behaviour. While the Blauwe Knop is also at risk for this consent paradox the current set-up does provide some comfort in minimalizing this unconscious sharing compared with other PDM platforms. For starters the information is only shared with the user themselves, managing the risks of providing easy consent. Moreover, it provides a clearer insight due to the controlled data flow. Secondly, the login with DigiD makes the user more aware of the seriousness of the desired action. Creating more time to consciously think about providing consent or not. The trusted environment, however, creates more comfort, automatism and less concern to actively think about one's actions resulting in an amplification of the paradox.