Privacy & Us

Initial formulations of the models and the modelling approaches

Deliverable Number	D3.1
Work Package	WP 3
Version	1
Deliverable Lead Organisation	TAU (Tel Aviv University)
Dissemination Level	Public
Contractual Date of Delivery (release)	2017/05/31
Date of Delivery	2017/05/31
Status	**Final**

Editor

Joachim Meyer (TAU)

Contributors

Agnieszka Kitkowska (ESR-2-KAU), Poornigha Santhana Kumar (ESR-4-USE/UoS), Juan Quintero (ESR-7-UNI/FAU), Yefim Shulman (ESR-8-TAU), Luiza Santiago Resende (ESR-9-TAU), Mark Warner (ESR-12-UCL)

Reviewers

Jetzabel Serna-Olvera (GUF)

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675730.

European Commission

1 Abstract

WP3 deals with the modelling of privacy-related behaviours. The WP deals with the development and empirical validation of predictive models of user behavior regarding privacy and privacy decisions. It aims to generate theoretical contributions, to develop and adapt modeling methods for privacy-related behavior and to provide model-based guidelines for system design.

The report consists of initial statements, written by the six ESRs who participate in this WP. The descriptions describe the aspects of their work that are related to the modelling of privacy-related behaviours. The ESRs were asked to present the basic topics of their research, the questions or behaviours they plan to model, and the general methods they want to apply in their modelling work. They also present some of the planned next steps in their work.

Table of Contents

2 Introduction

2.1 Purpose

The research on user aspects of privacy is a very wide field, grounded in large variety of academic disciplines, including computer science, psychology, economics, law, political science, and others. It also makes use of very different research methods, ranging from qualitative and descriptive to more rigorous quantitative methods.

Beyond the collection of empirical observations, and the conduct of conceptual analyses, the research should also lead to more general formulations of the connections between different factors and their effects on privacy-related behaviour and the outcomes from such behaviour. These formulations are essentially models of privacy-related behaviour. Models of privacy-related behaviours are important conceptual and analytical tools that can help us understand the relevant behaviours and go beyond the simple summary of empirical observations. In WP3 the participating ESRs report their efforts in developing such models and the validation of the models vis a vis empirical data.

The modelling approaches can be very broad and can differ widely, depending on the conceptual framework within which the ESR addresses the issue and the empirical data the model should ideally be able to predict.

2.2 The Modelling Reports from the ESRs

The first deliverable in WP3 reports the initial work the different ESRs who participate in this WP have done so far regarding the modelling of privacy-related behaviour in their Ph.D. research. The level at which ESRs have developed the models differs greatly between ESRs. This is due to the great variety in the research topics and approaches taken in the project.

Still all ESRs have made some important steps in the development of models for the description of privacy-related behaviours.

2.3 Glossary of Acronyms / Abbreviations

USE	USECON THE USABILITY CONSULTANTS GMBH
TAU	TEL AVIV UNIVERSITY
VDS	VASCO
KAU	KARLSTADS UNIVERSITET
WU	WIRTSCHAFTSUNIVERSITAT WIEN
GUF	JOHANN WOLFGANG GOETHE UNIVERSITAET FRANKFURT AM MAIN
ULD	UNABHAENGIGES LANDESZENTRUM FUER DATENSCHUTZ
UNI	UNISCON UNIVERSAL IDENTITY CONTROL GMBH
UC	UNIVERSITY COLLEGE LONDON

3 ESR-2 (KAU) Agnieszka Kitkowska - Measuring and manipulating privacy related attitudes and behaviours

3.1 Introduction

Over the last few decades, many researchers and policymakers from the field of information technology consolidated their studies around the issues of privacy. Much of their research concentrates on security issues data anonymization, minimization, improved encryption methods and others. Additionally, it focuses on legislative enforcement of privacy. Despite the researchers' efforts, the user's privacy decisions appear to be poor and uninformed. The previous studies demonstrated the existence of the discrepancy between privacy attitudes and behaviors, the so-called *'information privacy paradox'* (Norberg, Horne, & Horne, 2007). Regardless of broad research about this phenomenon, performed by interdisciplinary teams, the causes of the *privacy paradox* are still unclear, and the ways to diminish it remain undefined. Thus, online privacy research requires improved methods to enhance the understanding of the decision making processes, incorporating best practices from fields beyond computer science, such as human-computer interaction research and psychology, ensuring compliance with usability best practices, including human factors and ergonomics.

3.2 Relevant literature

Privacy is a complex and multidimensional concept. In general, it can be divided into three spheres: territorial (the physical area surrounding an individual), the privacy of a person (protection sphere preventing physical search and potential abuse), and lastly information privacy (Kokolakis, 2015). The latter focuses on personal data processing and is of interest to this research.

Information privacy can be considered as a value-based concept or a cognition-based concept. Westin defined privacy as '*voluntary and temporary withdraw of a person from general society'* (1967), giving ground for the cognitive approach to the matter. From this perspective, privacy is considered as a state and control, while a value-based approach identifies privacy as a general right or commodity (Xu, Luo, Carroll, & Beth Rosson, 2011). Due to the complexity of privacy, public understanding of its main concepts is often misinterpreted. As a result, the term privacy is used interchangeably with security, confidentiality, anonymity and more. These terms are related to privacy, but they are not synonymous.

3.2.1 Major trends in decision-making research

There are three major trends in decision-making research (Gonzalez & Meyer, 2016). The first is concerned with the classical economic tradition, such as the rational calculus of choice. This approach is often studied through the lens of the theories like utility maximization, reasoned action, costs and benefit calculus, or expectancy (Li, 2012). However, research demonstrated that the economic approach is insufficient for studies of online privacy decisions, mainly due to asymmetric or incomplete information, as well as psychological and cognitive constraints. The second approach is focused on naturalistic decision making (NDM)(Gonzalez & Meyer, 2016). The NDM concentrates on gaining an in-depth understanding of people's decisions in the meaningful and familiar real-world contexts (Canelas & Feigh, 2016). Its goal is to identify novel perspectives on people's choices by focusing not only on a single decision. The NDM includes issues of recognition and intuition. To the best of our knowledge, NDM has not been used in privacy research. So far, it was mostly applied in research of complex decision-making, performed by experts in dynamic settings (Klein, 2015). The last trend originates from psychology and focuses on simple heuristics, unconsciously or consciously used by people. This trend concentrates on psychological constraints accompanying rational calculations. Hence, it considers factors external to the rationale, such as emotions, contexts, and social norms, as well as limitations of human cognition (Gonzalez, Meyer, Klein, Yates, & Roth, 2013; Kahneman & Klein, 2009). This project aims to include the economic and the psychological approach to decision-making studies, and it desires to incorporate some elements of NDM, such as the role of intuition.

3.2.2 Privacy risks, economics and rationale

The economic approach to the investigation of the *privacy paradox* resulted in a large volume of research. Originating in rational decision making, behavioral economics have been fundamental for researchers, such as Acquisti and Grossklags (2005), Norberg (2007), Beresford et al. (2012) and many others. The majority of the studies using the economic approach focus on information disclosure, emphasizing transactional dimensions of online behaviors. This concept was applied in studies of the monetary value of information protection (Grossklags, Hall, & Acquisti, 2007), or even price-tagging of different types of information (Carrascal & Riederer, 2013). Similarly, privacy calculus studies aimed to explain that responsibility for privacy decisions lies in the calculation of expected benefits and losses of information disclosure, implying that users' decisions result from estimated privacy trade-offs. Privacy calculus models have been developed to improve understanding of privacy concerns and their potential implications on behavior (Tamara Dinev & Hart, 2006). The privacy calculus was fundamental in studies related to the risk-benefit analysis (Dinev & Hart, 2004; Hann, Hui, Lee, & Png, 2014). The studies using the economic approach frequently use utility maximization expectation theory (Li, Sarathy & Xu, 2011) and expectancy-value theory (Malhotra, Kim & Agarwal, 2004; Dinev & Hart, 2006). Research largely demonstrated that simple rational decision models and a cost-benefit calculus could not adequately account for privacy decisions. Thus it is necessary to consider additional psychological aspects of the decision process, the decision maker and the situation in order to be able to predict privacy decisions.

3.2.3 Psychological distortions, biases and affect heuristics

Judgments are frequently influenced by cognitive biases and heuristics (Grossklags et al., 2007). Some studies demonstrated how *optimism bias* impacts people's engagement in risky decisions (Baek, 2014; Cho, 2010). According to the *optimism bias,* people perceive themselves as less vulnerable than others, when confronted with risky decisions. This may result in under-protective behaviors. Additionally to the *optimism bias*, people seem to be overconfident about their knowledge and skills (Jensen, Potts, & Jensen, 2005). That results in disclosing more data and enhances risk exposure. Similarly, the *control paradox* discovered in previous research demonstrated how biases might influence privacy decisions. Hypothetically, providing users with greater control over data should result in improved privacy awareness and reduce security risks. However, results demonstrated in the past studies were contradictory, showing that greater *control* over data increases willingness to disclose personal information (Brandimarte, Acquisti, & Loewenstein, 2013).

Among other psychological factors impacting rational privacy decision making, Acquisti and Grossklags identified psychological distortion related to time: *hyperbolic discounting* (Alessandro Acquisti & Grossklags, 2003). People express tendencies to weight differently benefits placed at various points on the time scale. The effects of actions placed in the distant future seem to have lesser impact on the decision made today. Similarly, long-term risks and losses may be underestimated. That may enable people to remove or omit risks from the judgment processes. Next to the *hyperbolic discounting*, researchers considered *immediate gratification,* likewise influencing risk-taking by increasing the value of benefits in the near future over benefits in the later future.

Affect-heuristics add to the complexity of decision-making research. In short, according to affect-heuristics during the judgment process, people are looking for mental shortcuts. They tend to make decisions quickly, based on affect (Kehr, Wentzel, Kowatsch, & Fleisch, 2015).

One possible way to understand this is to assume the existence of two systems responsible for cognitive operations: System 1 (Sys 1) and System 2 (Sys 2). Sys 1 is automatic, effort-less, intuitive, perception based, while Sys 2 is analytic, effortful, and consciously controlled. The affect-heuristic is one of the outcomes of Sys 1 (Kahneman & Frederick, 2002). Psychological studies not only demonstrated the existence of both systems, but they also provided evidence that Sys 1 can dominate decision making (Denes-Raj & Epstein, 1994), even when people are aware of the irrationality of their decisions. Thus, it can be concluded that affect-heuristics are responsive to people's preferences, choices, both conscious and unconscious, and that they can be independent of cognition (Slovic, 2002).

3.2.4 Attitudes and behaviors: relationships and models

A significant amount of research considered the relations between attitudes and behavior. Various models of this relation were created, such as the Fishbein-Ajzen models, looking at the indirect impacts of attitudes on behavior; roles of different antecedents of behavior, such as previous experiences; or studies of causal influence of attitude and/or the affect heuristic on behavior (Bentler & Speckart, 1979). Models of behavior, such as the one proposed by Bentler & Speckart (1981) claimed for a causal relationships between attitude and behavior (Bentler & Speckart, 1981). However, over the last decades research demonstrated that this relationship is not as direct and obvious as originally claimed. Initially, attitudes were considered as a direct influencers on behavior, while modern psychology demonstrated that this is not always the case (Ajzen & Fishbein, 2000). The modern approaches to the decision-making process explain it as a matter of routinized choice, habit, or an antecedent of past behavior, resulting in *behavior → attitude* or even *behavior → behavior* relationships. Additionally, new studies revealed that people use mental shortcuts, in which they avoid full assessments of risks and benefits. These findings resulted in research focused on emotions, stress, and affect present during and prior to the decision making process (Betsch, Haberstroh, & Höhle, 2002).

Despite all the efforts, the *privacy paradox* remained unsolved, and the research shows contradictory results. Some researchers challenged the dichotomy, and demonstrated that it is possible to resolve it. Lutz et al. (Lutz & Strathoff, 2013) reviewed privacy decisions through the societal lens, implementing Ferdinand Tönnies's duality: *Gemeinschaft* (emotional ties in communities) and *Gesellschaft* (societies holding rules that emerged from rational calculations). According to their social networks' study, online information disclosure is a result of the necessity of being a community member. The study shows that the emotional urge of *'belonging'* is stronger than the need for protection related to the security and privacy. Similarly, Wakefield (Wakefield, 2013) demonstrated that the affective side of human cognition has a decisive impact on online trust and privacy.

3.3 Research questions

This research aims to investigate the privacy decision-making process, and to determine causes for the *'privacy paradox*'. The goal of this project is to understand *why* people's attitudes differ from their behavior when confronted with privacy decisions. Further, by gaining insights into the decision-making process, this project's goal is to produce a visual interface influencing the privacy choices. This will be achieved by manipulating people's decisions by implementation the appropriate HCI techniques, identified in quantitative and qualitative studies, and compliant with usability heuristics and current legislation schemes such as the new European Union General Data Protection Regulation (GDPR). The main research questions planned for this research are as follow:

- What are the most important/strongest factors influencing privacy-related decision making?

This part of the project investigates users' perceptions of privacy concerns and risks, and their alignment with concepts proposed in previous research, such as Solove's *privacy harms* (Solove, 2006). Additionally, some of the cognitive biases and heuristics will be considered, such as *benefit immediacy* and *risk diffusion*.

- What is the role of contextual dependencies and affect heuristics in the privacy decision making process?

This section will involve the role of social norms, emotions and intuition in privacy decision making. The first approach originates from Nissenbaum's notion of *contextual integrity*. Nissenbaum defined context as social settings *characterized by canonical activities, roles and relationships, power structures, norms and internal values* (Nissenbaum, 2009). The contexts, such as social norms and rules, hypothetically could lead to the acceptance of situations violating privacy principles. The research aims to identify which of the contexts influence privacy decisions and whether it is possible to diminish their role in the decision making process.

- Can graphical privacy indicators become a *manipulation tool*, which enhance privacy risk awareness and lead to informed decisions?

The project will result in the user interface elements that manipulate privacy choices. The aim of this part of the research is to investigate whether the visual representations of privacy harms and risks can change users' behavior. The identification of UI elements will be achieved by incorporation the decision-making trends mentioned in Section 3.2.1 of this document.

Models of behavior are fundamental for this project, as they will contribute to the investigating the decision-making process. Because the desired outcome of this project is a novel user interface shaping privacy aware decision-making, models of behavior add to understanding people's choices. The incorporation of behavior models will enable us to understand the connection between attitudes and behaviors, as well as simplify the recognition of factors affecting these relations. Specifically, the privacy harms and risk perception will be modelled at the early stages of the project, followed by inclusion of affect heuristics, social and contextual dependencies and/or framing effects.

3.4 Modeling approach

This research, similarly to previous studies, does not aim to identify a single solution to the *privacy paradox*. However, it desires to support privacy-related decisions by impacting people's attitudes and/or behaviors. Therefore, models of behavior will be fundamental for the development of experiments involving users. The studies will incorporate the economic approach, with an emphasis on a cost-benefit calculus. Additionally, parameters such as emotion and intuition will be implemented into the models to investigate their role in attitude-behavior relationship. As this research focuses on adjusting privacy decisions, emotions will be considered not as an outcome but measured before and during the decision making process. This approach originates from previous studies by Loewenstein (e.g., Loewenstein, Hsee, Weber, & Welch, 2001) and Slovic et al. (Slovic, Finucane, Peters, & MacGregor, 2004).

The first part of the research will consist of conceptual models of user decisions regarding privacy harms, based on approaches proposed in previous research. The emphasis will be on emotions, intuition and contexts as factors that impact attitudes and behavior. Therefore, models mentioned in Section 3.2.1 will be considered. Additionally, it is desired to implement elements borrowed from Triandis's theory of interpersonal behavior that expand beyond traditional models such as Ajzen-Fishbein. As this research aims to explore the role of affect in decision making, Triandis's model will enable it by incorporation of variables such as positive and negative emotions, and subjective rules (Perugini & Bagozzi, 2001). It will also deepen the research by investigating a role of repetitiveness and habit on behavior, facilitating conditions and intentions (Cheung, Chang, & Lai, 2000).

- First models

The first study is based on the Solove's *privacy harms*. It aims to validate whether the recognized *privacy harms* correspond with the subjective groups identified by Solove, or whether people think differently? The desired mapping of the privacy harms is presented in Figure . However, a preliminary analysis of the collected data does not validate this mapping. Therefore, further analyses are required to identify how people think about *privacy harms*, whether they think of some of them more than others.

A second model is at a preliminary stage, since it requires the results of the first study. Based on the first study, Model B will investigate how the display of privacy harms affects people's choice (Figure 3.2:). This model incorporates additional parameters, such as emotions and intuition. The model aims to identify if the decisions differ accordingly to the positive, negative or intuitive (based on recognition) representations of privacy harms. In theory, the goal is to measure whether the emotions generated by different displays can change users' behavior as well as whether their weight on harms and benefit calculation is stronger than the weight of contextual factors.

- Empirical evaluation

Models will be evaluated by quantitative studies and statistical analysis. The models will also use mathematical methods to look for non-linear relations between variables in the models (Cavagnaro, Myung, & Pitt, 2010). This may enable a more accurate prediction of dynamic processes in judgment and decision making (Hotaling & Busemeyer, 2012). Numerous mathematical methods can possibly be used, such as psychophysical, axiomatic, algebraic and computational modelling.

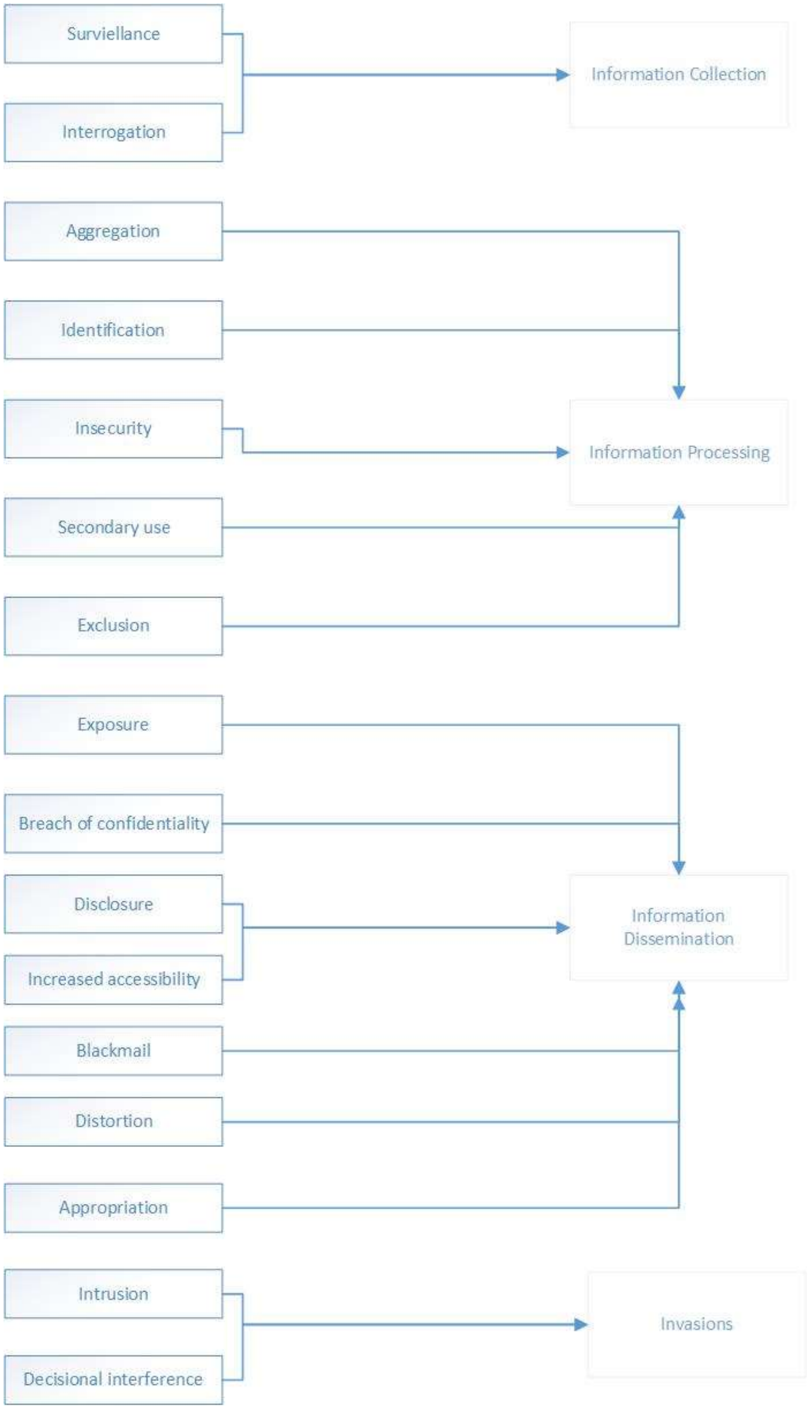


Figure 3.1: Model A: Privacy harms identified by Solove and the expected mapping (Solove, 2006).

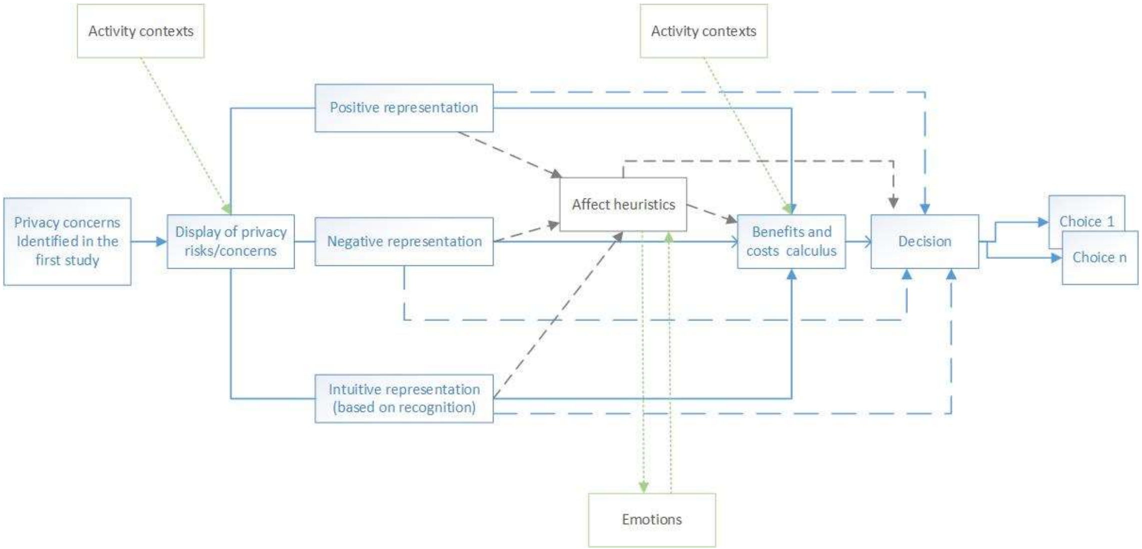

Activity contexts
Activity contexts
Positive representation
Privacy concerns Identified in the first study
Display of privacy risks/concerns
Negative representation
Affect heuristics
Benefits and costs calculus
Decision
Choice 1
Choice n
Intuitive representation (based on recognition)
Emotions

Figure 3.2: Model B: display of benefits and harms, and their influence on choice.

As the research is at an early stage, and the precise studies/experiments are not entirely defined, the exact statistical methods for validation have not been determined. However, it is probable that Bayesian statistics comprising of Structural Equation Modeling (SEM) will be applied, as the experiments will focus on cognitive process and latent parameters, such as emotions and intuition. The Baysian method allows to capture a prior distribution of assumptions and to model their posterior distributions. This enables computation of predictive distributions of latent parameters. Additionally, Bayes factors may be transformed to weights of models enabling their composite estimations (Kass & Raftery, 1995). The application of SEM enables analysis of causal qualitative relationships in data and transforms them into quantitatively applicable causal claims (Pearl, 2012).

The described approach is not final and may require adjustments. In addition, it does not rule out qualitative studies focused on mental models and their role in privacy decisions. As has been demonstrated in recent research, understanding of privacy behaviors benefits from an investigation of mental models (Coopamootoo & Groß, 2014).

3.5 Next steps

The next stage of the research regarding models of behavior aims to analyze the results of the *privacy harms* study. We will use statistical methods to measure the strength of privacy harms.

Additionally, the study implemented scales developed in the past research, measuring information disclosure and privacy protection behaviors (Joinson, Paine, Buchanan, & Reips, 2008). It also incorporated Westin's index questionnaire items. The scales implemented in the study may enable validation of newly developed harms questionnaire. Furthermore, the incorporation of already existing questionnaire items aims to identify whether people's attitude toward information disclosure and online protection changed over time. We hope that the incorporation of additional scales will enable in-depth understanding of privacy displays and contribute to the development of Model B.

Once the results of the *privacy harms* study are validated, we hope to build the novel user interface elements required for Model B. The further steps will be as follow:

- Mapping privacy harms with users' privacy rights defined in the EU GDPR.
- User requirements gathering incorporating user-centered design guidelines, emphasizing usability and accessibility best practices.
- Development of user interface and series of experiments with users, such as usability tests and eye tracking to validate the model.

4 ESR-4 (USE/UoS) Poornigha Santhana Kumar - Designing for Privacy & Security at Point of Sale Commercial Transactions

4.1 Introduction

Any user would prefer to feel secured and privacy assured at a Point of Sale (PoS), and we aim to deliver this experience to the users. Considering personality and modelling the relationship between personality and acceptance of NFC will help in improving the user experience gained by the users at PoS.

We focus on Near Field Communication (NFC) payments, as it is an emergent technology, and as forecasted by some authors (Lee, 2001) (Staib), NFC payments are commonly used in retail shops now-a-days. We also choose to work on retail shop checkouts, as they involve a wide range of customers (in age, gender and profession) and accept all types of payment (cash, credit/debit card, NFC in cards and mobile phones).

The technical aspect of NFC has been well explored in the literature, with various studies trying to improve the protocol and security of NFC. There are also several studies on using NFC's in various fields like in tourism, museums and in navigation. (Blöckner, 2009) and (Choo, 2012) explore the possibilities of using NFC technology in museums to interact with exhibits and indoor navigations respectively. (Pesonen, 2012) reviews the possibilities of using NFC technologies in tourism.

Given the large literature on NFC's technical aspects and advantages, the usability and user experience related to NFC remains unexplored. Regarding NFC payments, literatures focus only on developing models or framework for businesses (Pousttchi, 2009) (Chae, 2015). There exists nearly no research using models or frameworks to build a NFC application regarding user experience.

Some researchers use TAM (Technology Acceptance Model) to measure the acceptance of NFC payments and mobile payments in general. The psychological dimensions like trust (Lu, 2011) (Boes, 2015) , social influence], perceived risk and cost (Tan, 2014) are considered in various studies. The acceptance of NFC payments has also been studied based on locations. (Ondrus, 2007) and (Shin, 2014) study the state of NFC payments in Switzerland and Korea respectively. The above studies conclude by projecting the acceptance NFC's in those locations. Even though several studies have explored the acceptance of NFC's payments based on various dimensions, the user personality aspect of the TAM is still unknown.

4.2 Research Questions

To enhance the experience gained by user while using NFC and to improve the usability of NFC payments, we plan to answer the following research questions

- RQ1: How does a specific design of the transaction affect the experience of felt security and privacy by the user?

We will be using the famous Human-Centered design (HCD) (ISO 9241-210) process as we will be designing for user experience. As a first step, based on HDC we will be developing various transaction design prototypes. Then, we will be evaluating the developed prototypes with potential users on the experience felt by them while using each design. The evaluation results will reveal the transaction design, which will provide user with security and privacy enhanced experience.

Figure 4.1 shows the model we will be using to build the prototypes. We are currently in the first phase: Understanding and specifying the context of use. In-depth literature studies were conducted to understand the existing usability-related issues in NFC payments. As a next step in this phase, we will be using questionnaires to understand the existing context and users' mental models.

- RQ2: How does mobile NFC and card NFC differ in terms of usability and user experience gained?

Since Mobile NFC and card NFC differ greatly on factors like feedback delivered, information revealing and security, we would like to investigate the difference between them and their effect on the user.

- RQ3: What is the role of personality on perceived experience of felt security and privacy of the user?

In the third research question we would like to explore the role of personality on the experience gained. As personality plays an important role in various aspects of our life (Barlett, 2012) (Judge, 2002), we believe that considering personality would deliver good insights for the community.

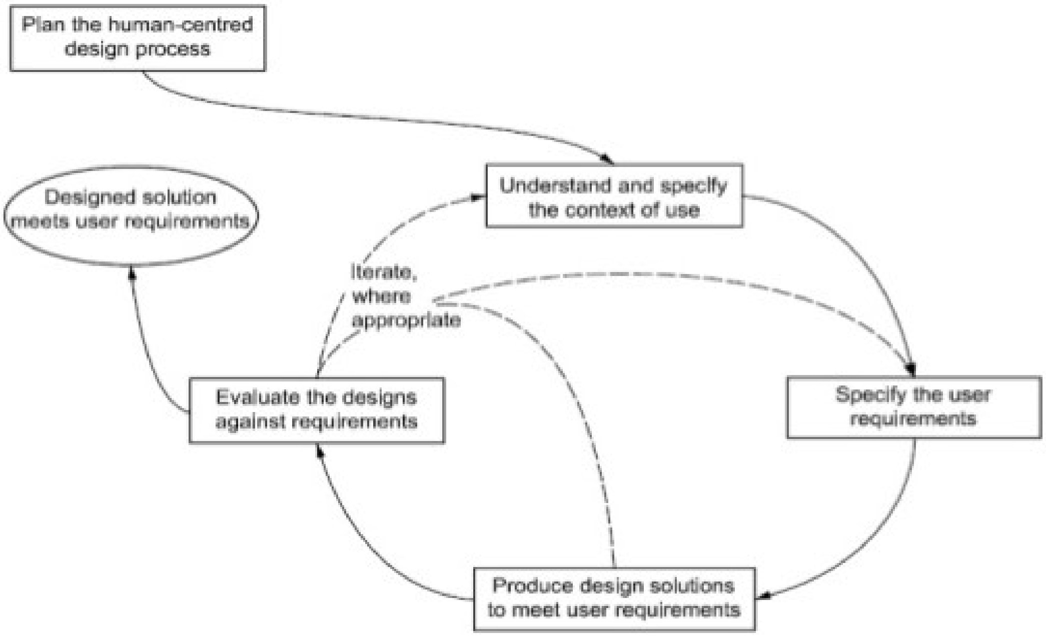

Plan the human-centred design process
Understand and specify the context of use
Designed solution meets user requirements
Iterate, where appropriate
Evaluate the designs against requirements
Specify the user requirements
Produce design solutions to meet user requirements

Figure 4.1: User Centered Design process (ISO 9241-210)

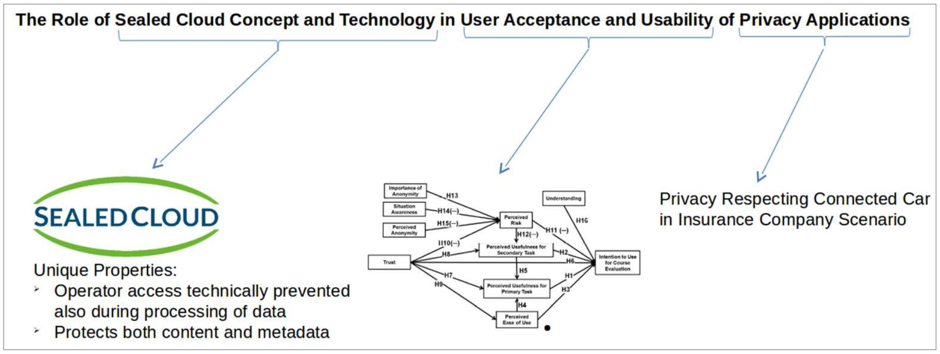
4.3 Planned model

We aim to model the relationship between user personalities and technology acceptance of NFC. As mentioned earlier, the existing TAM studies do not consider the personality of the user. Devaraj, Easley and Crant (Devaraj, 2008) explores the relationship between TAM and five-factor model (FFM) and found strong and moderate relations between the two models. Since it is evident that personality plays a role in technology acceptance we would like to model the effect of personality on NFC payment acceptance.

5 ESR-7 (UNI/FAU) Juan Quintero - Model of User Acceptance of the Sealed Cloud Technology in the Connected Car in the Insurance Company Scenario

5.1 Introduction

The project concept, which has been detailed in Figure 5.1, focuses on the impact Sealed Cloud technology (Jäger et al., 2014) has on user acceptance in a privacy preserving application. To develop this concept, a Sealed Cloud implementation will be used in the context of a chosen privacy application scenario. Using this Sealed Cloud implementation, within the chosen context, a User Acceptance Model will be developed.


The Role of Sealed Cloud Concept and Technology in User Acceptance and Usability of Privacy Applications

Unique Properties:
- Operator access technically prevented also during processing of data
- Protects both content and metadata

Privacy Respecting Connected Car in Insurance Company Scenario

Figure 5.1: Explanation of ESR7 project title

To choose the privacy application scenario, a review of existing privacy preserving Uniscon GmbH projects was conducted. The main goal of this review was to choose a scenario where privacy enhancing technology was relevant to resolve privacy compliant operations. The scenario chosen was a privacy respecting connected car, the data of which would be used by the insurance industry. Figure 5.2 depicts a connected car system model, where networked cars drive through the streets using their sensors and cameras, collecting personally identifiable information (PII) and non-PII data, such as: the car's position and speed (PII), road state and weather conditions (non-PII), energy consumption (PII), as well as other data. In the process of normal operations, these connected cars will be collecting and storing large quantities of private information, which may result in end-user privacy concerns.

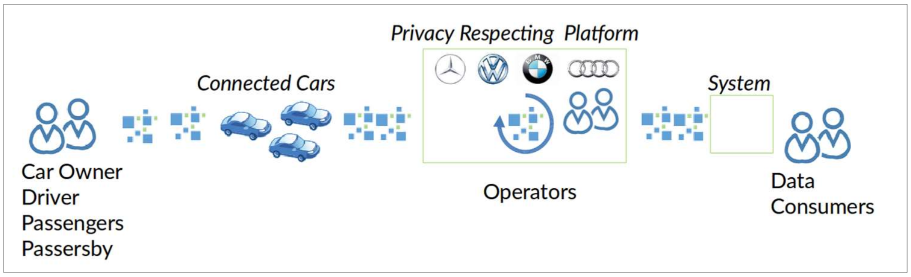
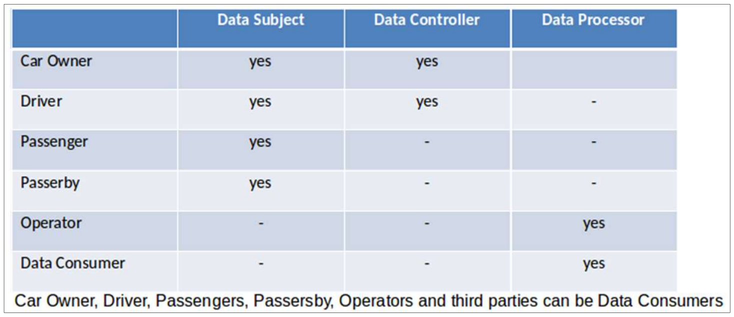


Figure 5.2: Connected Car system model

In the insurance company scenario, the Data processors (insurance companies) could analyse the data of Data subjects to find out behaviour patterns (driving style, speed, etc.) and reward them with offers or discounts. A mapping between the actors involved in the connected car model and the GDPR regulation (Regulation, E. U., 2016) is proposed in Table 5.1.

Table 5.1: Mapping of Insurance company scenario to Terminology and Definitions of GDPR



	Data Subject	Data Controller	Data Processor
Car Owner	yes	yes	
Driver	yes	yes	-
Passenger	yes	-	-
Passerby	yes	-	-
Operator	-	-	yes
Data Consumer	-	-	yes

Car Owner, Driver, Passengers, Passersby, Operators and third parties can be Data Consumers

To develop a user acceptance model, it is necessary conduct a literature review to find the user acceptance factors and models closest to our scenario.

This report is organised as follows: section 5.2 describes the project research questions, which provide the focus for the research. In section 5.3 two models of user acceptance relating to privacy applications were reviewed. Informed by the literature review and the reviewed models, a first model approach is presented with proposed user acceptance factors. Finally, section 5.4 presents the methods proposed to develop and validate the final user acceptance model.

5.2 Research Questions

The problem described in section 5.1 is how Data controllers and Data processors can explain to Data subjects the purposes for processing, profiling, and pseudonymisation his data. The goal for these explanations is to encourage the Data subjects to give their informed consent and improve his acceptance.

As research questions related to the user acceptance model are:

- What is the Sealed Cloud Technology impact on the user acceptance in the connected car in the insurance company scenario?
- What are the user acceptance factors in the connected car in the insurance company scenario?
- How does cloud technology using mainly organizational measures to secure confidentiality and integrity compare to Sealed Cloud Technology with regard to user acceptance?

5.3 Modeling Approach

Benenson and Girard (2015) define a theoretical development of a user acceptance model for anonymous credentials, proposing a model that integrates the Technology Acceptance Model (TAM) with secondary goals. This model is shown in Figure 5.3.

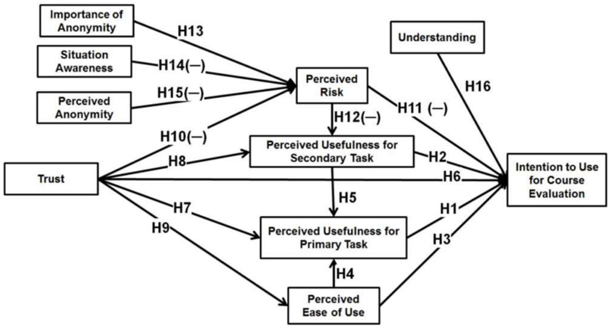


Figure 5.3: Research model for user acceptance of Privacy-ABCs for course evaluation (Benenson & Girard, 2015, p. 13)

Spiekermann (2008) proposes another user acceptance model for Ubiquitous Computing without TAM extension for many reasons explained in (Spiekermann, 2008, p. 127). Figure 5.4 describes an UC-AM (UC Acceptance Model).

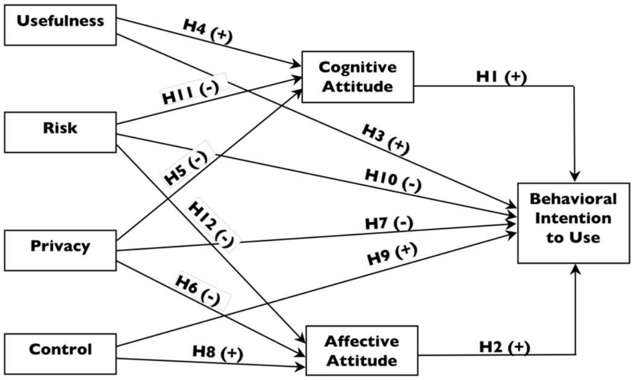


Figure 5.4: UC Service Acceptance Model-Hypotheses and (expected directions) (Spiekermann, 2008, p. 138)

Taking into account the models and user acceptance factors explained in (Benenson & Girard, 2015. p. 13; Spiekermann, 2008, p. 138) it has proposed a user acceptance model according to the connected car scenario described in this research. Figure 5.5 shows this.

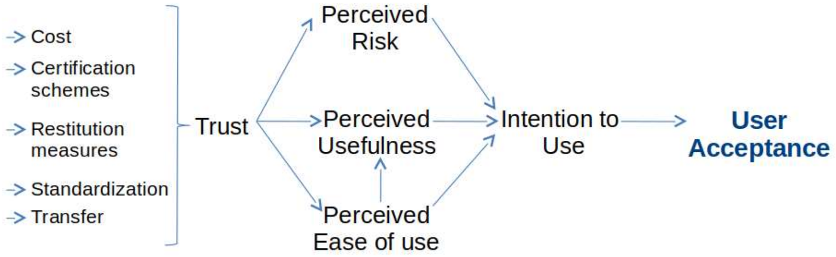


Figure 5.5: User Acceptance Model in the connected car in the insurance company scenario

The factors proposed in this model are defined as:

- **Perceived Ease of Use:** “the degree to which a person believes that using a particular system would be free of effort” (Davis, 1989. p. 320).
- **Perceived Risk:** “subjective belief of suffering a loss in pursuit of a desired outcome” (Pavlou, 2003, p. 77).
- **Perceived Usefulness:** “the degree to which a person believes that using a particular system would enhance his or her job performance” (Davis, 1989. p. 320).
- **Intention to Use:** based on (Warshaw & Davis, 1985, p. 214) is defined in (Benenson & Girard, 2015, p. 6) as: “degree to which a person has formulated conscious plans” to use or not to use a specific technology”.
- **Trust:** Benenson and Girard (2015, p. 6) define as a belief that this technology “has the attributes necessary to perform as expected in a given situation in which negative consequences are possible” (Mcknight et al., 2011, p. 7).
- **Transfer:** the trust in the company itself is transferred to trust in its cloud without any evidence of the security in this cloud (Marshall et al., 2012. p.551).
- **Cost:** the cost implies trust. Paying for a service of security, the user assumes that more provisions are received without knowing if these provisions exist (Marshall et al., 2012. p.551).
- **Restitution measures:** the user’s trust increases when the provider makes restitution to the user for all problems that happens (Lacohée et al., 2006. p.2).
- **Standardization and certification schemes:** It allowed to describe in more technical detail the features of the technology (Prismacloud, 2015. p.5).

5.4 Next Steps

Figure 5.6 depicts the proposed method to get the final model of User Acceptance. First, it defines, at a high level, a scenario description. Then, based on a literature review, more details of this scenario are added. These iterations allow that a completed scenario description is reached, and many user acceptance factors are identified to formulate a user acceptance model. Users using surveys will validate the model. With the feedback of the validations is possible to iterate between user acceptance factors identification, user acceptance model formulation, and user acceptance model validation. Two iterations are proposed to get a final user acceptance model.

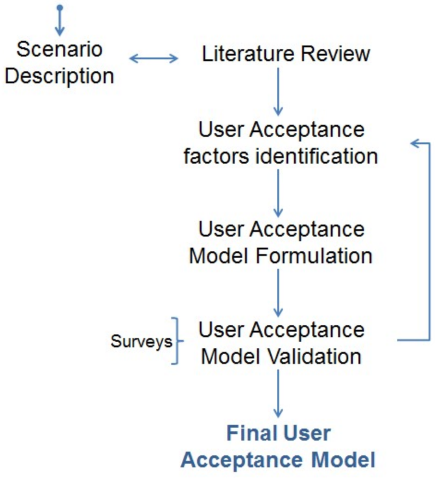

Scenario Description
Literature Review
User Acceptance factors identification
User Acceptance Model Formulation
Surveys
User Acceptance Model Validation
Final User Acceptance Model

Figure 5.6: Method to get a user acceptance model

The next step is, based on the literature review, a first iteration between user acceptance factor identification, user acceptance model formulation, and user acceptance model validation.

6 ESR-8 (TAU) Yefim Shulman - Modelling Responses to Privacy-related Indications

6.1 Introduction

The increasing proliferation of Information Technology, in the modern day, nudges users to deal with Information Systems on a regular basis. These interactions, if done invoking conscious decision-making, either can be associated with gaining tangible benefits (e.g., fulfilment of work duties on salaried job, acquiring goods and getting services online, etc.), or they can come out of necessity (to communicate with relatives and friends, to exchange information, to access entertainment, etc.). Other interactions with technology can occur without awareness of the users, that is, be just a by-product of various activities, decisions and informed interactions.

All these interactions may lead to the disclosure of personal information, and, as a consequence, give rise to privacy-related concerns. The level of awareness about possible outcomes for users' privacy and the level of comprehension and internalisation of these possible effects can influence users' decisions to engage into this or that activity.

Decisions in question are consent-type decisions, which are made under consideration (or lack thereof, what complicates the problem even more) whether and to which extent to disclose one's personal information. Even when appearing like a choices made among alternative options, said choices can be partitioned into a set of consequent yes-or-no decisions, when the options can be isolated, i.e. are to certain extent independent.

In order to get a better understanding and to be able to predict decisions involving privacy concerns, a model should be developed. The proposed model can be a product of combining approaches and tools from Economics, Information Science and psychological research in human cognition, decision-making and behaviour.

6.2 Research Questions

Present research aims to build a predictive model of users' decision-making when faced with privacy-related implications. In order to achieve this goal, we ought to address the following research questions:

- Privacy decision-making.

Here we need to understand users' privacy concerns, how users perceive privacy threats, evaluate losses and gains when making decisions on self-disclosure. Additionally, we should examine how people, in reality, response to indications provided by information system that are associated with changes in perceived privacy "status quo"

- Processing alerts in humans.

We have to have a notion of how cognition processes work in humans when alerted, including looking into possible kinds of alerts, when people notice them, how people process the information provided, what factors can alter the way people notice and process alerts, etc.

- Modelling approach.

We will investigate what frameworks can be used for modelling human decision-making, and what psychological precursors, factors and biases form decision-making process in humans.

Researchers have been investigating human decision-making from an economic standpoint, using a variety of models, based on classical economics, expected utility theory and its generalized extensions, and behavioural economics.

Acquisti et al. (2016) discuss how privacy has been being regarded as an economic good and provide an explanation on how individuals' informed decisions about their privacy are being hindered, because of asymmetry of the information available to people at the moment of making privacy-related decisions. Cumulative Prospect Theory can be applied for the purposes of modelling human decision in privacy-related interactions as a model of decision making under risk. Barberis (2013) provides multiple examples of how it has been used to model decisions in the areas starting from finance and insurance spanning to understanding betting markets, pricing, consumption-saving decisions, etc., and even describes some macroeconomic and prescriptive economics applications.

The existing theoretical body of research behind privacy decision-making draws from various subject areas. Li (2012) designs a decision-making matrix, based on an elaborate overview of approaches and theories used in privacy research, and on the concept of a "dual-calculus model", which is defined by the author as a combination of privacy- and risk-calculi for decision making in privacy-related issues.

Egelman and Peer (2015) study privacy decision making from psychological standpoint. They argue that individual differences are better predictors of decision process results than the widely studied personality traits approach, testing their hypothesis against the Five Factor Model.

Mahmood and Desmedt (2013) carry out a – self-described – first attempt to develop mathematical models of privacy, which results in devising a game theory model and a graph theory model. The authors conceive their models as a "privacy vulnerability scanners", but they also argue that, by using the proposed models, it might be plausible to increase rationality and reduce psychological deviations of individuals in privacy decision making.

Multiple empirical studies concerning privacy decision making (e.g., in Malhotra et al., 2004; Hann et al., 2007; Xu et al., 2011, and many others) were conducted utilizing behavioural economics and generalized expected utility methods, employing privacy calculus. Applying machine learning problems solutions, they produced results providing insights for understanding the "privacy paradox" and individuals' attitudes towards privacy-related decisions.

In a set of studies of privacy-related issues in Social Networking Services, Krasnova et al. (2009 and 2010) apply the privacy calculus and produce structural models to investigate Internet users' privacy concerns and motivations regarding personal information disclosure. In Krasnova et al. (2012), authors account for users' cognitive patterns and uncover cultural implications of privacy attitudes and behaviour.

Keith et al. (2013) apply the privacy calculus to show that the relationship between decisions on personal information disclosure and an intension to disclose such information is weak, while still statistically significant. Eling et al. (2013) take an inductive approach to build a decision making model, linking trust in a service provider and intrusiveness of requested information to highlight the decisional calculus proposed in their paper.

In Dinev and Hart (2004) the authors first attempt to measure privacy concerns and to estimate dependencies between factors and privacy constructs ("concerns of information finding" and "concerns of information abuse"). Later, in Dinev and Hart (2006), the researchers provide more ground for the use of an extended privacy calculus, showing that – at least for the example of E-Commerce – Internet trust and personal interest can outweigh privacy concern constructs. After employing common statistical methods of dimensionality reduction and supervised learning in the first work, Structural Equation Modelling in the second, and joined by other researchers, this bigger collective of authors develops a theoretical framework for understanding Internet privacy attitudes (Dinev et al., 2013), with empirical Structural Model attesting to the validity of proposed constructs.

Thus, the examples discussed above demonstrate the applicability of approaches derived from economics to model privacy decision making. It is obvious, however, that most of the existing models used to study privacy issues are limited in the way that they do not account for certain aspects of memory and cognition related to decision making. Such usually unaddressed aspects include: momentary awareness of privacy issues, current level of fatigue and (or) mental workload, attention span and sense-making of privacy indications, and other mental effects (e.g., information over-load, cognitive laziness, etc.).

6.3 Modelling Approach

Decisions made in terms of privacy can be generalized as the decision of people giving their consent explicitly or implicitly,

- for sharing their personal information (e.g., in social networks),
- for allowing access to their personal information (e.g., for third-parties, automated agents, etc.),
- and for engaging in interactions (e.g., getting access to social networks activities, purchasing products, etc.)

The current research shall focus on the privacy-related decisions of explicit nature (i.e., in legal terms, as a non-implied-in-fact transactions).

For the purposes of the current research factors affecting privacy-related decision-making should be considered: the nature of the information, the ownership of which is delegated to another entity; their own perceived knowledge about said entity; and the circumstances under which the information is requested; users' individual characteristics.

Hereby, the research aims to develop a model of the users' decision-making, which shall be considered as performance of actions in response to privacy-related indications. In this way, privacy shall be represented as a function of

- the parameters of the information requested to be disclosed or perceived to be disclosed,
- the identity or assumed identity of who will have access to the information,
- the context in which the information is provided,
- the users' individual characteristics,
- and the features of the indications from the system that are to point to the possible privacy implications of a user's action.

The model should be based and later validated on a combination of existing research on user privacy decision-making preferences, dedicated web surveys on users' privacy decisions, and laboratory experiments, assessing the effects of different variables on user decisions.

The model will be built upon the combination of methods from Economics and Cognitive Science, which can be used to predict users' decisions based on the perceived costs and benefits and available information at a given moment.

In order to include various effects of internal and external factors influencing decision making, a broader model of cognition should be constructed – one that simulates dynamic cognitive processes as functions in a system, consisting of input and data acquisition, memory, attention, decision making, and output generation. For the purposes of the current research the ACT-R cognitive architecture is chosen to construct such a model.

Aforementioned features help to build a model that could benefit from accounting for a whole set of context under which the necessity of making decisions can take place, including but not limited to simulating momentary awareness, as well as attention and judgment processes in the individuals. Additionally, incorporating the Cumulative Prospect Theory methods and (or) other privacy calculus to model human irrational decision making with ACT-R architecture seems as plausible as it may prove fruitful.

6.4 Next Steps

The study includes a series of surveys and laboratory experiments involving several hundred participants. Surveys will deal with attitudes towards privacy and privacy breaches. The experiments will test responses to different indications about possible privacy risks that are implemented in interfaces.

In accordance with assumed modelling approach further actions should be undertaken.

6.4.1 Defining the scope

The domain of privacy is extremely broad. The term itself corresponds to several definitions looking at privacy from different perspectives. It can be defined in different dimensions (as an economic good, as a human right –Regan's shared perceptions, public values, collective components; territorial privacy and online privacy, privacy as a value; etc.) and includes a whole set of complex interrelated interdisciplinary concepts: right to be alone, control over information, Westin's states of privacy, information privacy, privacy by subject areas (medical, financial, etc.), and etc.

Thus, the whole privacy domain should be narrowed down in accordance with the research goals and in order to make the modelling process practically plausible. Having limited the scope of privacy field with which the research is dealing, the framework of modelling methods is to be clearer defined as well as the modelling scope itself is to be more precisely identified.

6.4.2 Surveys: information on privacy-related decisions

Exploratory surveys should be conducted in order to gain initial understanding of users' preferences and attitudes towards privacy and privacy breaches. The surveys' structure and content should be developed depending on the scope of privacy domain defined previously. The results of the surveys are expected to provide insights for later phases of the research, e.g. design of the model.

6.4.3 Preliminary design

The initial model should be devised based in the findings retrieved from the exploratory survey and in relation with the pre-defined scope of the research field and the chosen methodological framework. The initial model is to be improved during the later phases of the research and, thusly, transformed into experimental model used for iterative test-validation process.

6.4.4 Experimental platform

The experimental platform should be constructed (or existing platform should be chosen and obtained from other sources), and adjusted for the purposes of the research. The actual experimental model is to be implemented with the use the platform. The tests to be run on said platform should serve to the improvement of the model's performance and to the validation of the modelling approach and results.

7 ESR-9 (TAU) Luiza Santiago Rezende - Reframing Informed Consent in Information Privacy Law through Behavioral Economics and the Paternalism-Libertarianism Spectrum

7.1 General Research Questions

Informed consent, or notice and choice in the American terminology, in the context of information privacy law, is the requirement to obtain the data subject's consent before collecting his or her personal data. The strictness and detailing of the consent requirement vary among legislations, however, both in the European Union and in the United States, which differ significantly in their structure and content regarding privacy protection (Whitman, 2004), and will be the focus of the present thesis, informed consent is central

Despite the centrality of the concept, in the last two decades, authors from different fields have shown growing skepticism regarding the real advantages of the informed consent requirement in the context of information privacy, uncovering several shortcomings, which will be classified as issues involving cognitive limitations, information asymmetry, or time constraints. Other authors have proposed solutions to these shortcomings, which are identified and organized in terms of their paternalistic or libertarian character.

Given the above background, the research questions are: a) based on the characterization of the shortcomings of informed consent in information privacy law as issues of cognitive limitation, information asymmetry or time constraint, what tools or strategies can be used to help mitigate or overcome these shortcomings? b) Should these strategies or tools have a paternalistic or libertarian background?

The central goals of the thesis are in: a) unveiling the multiple shortcomings of informed consent in privacy and characterizing them in terms of their behavioral elements, what will enable further comparison with shortcomings from other fields; b) identifying different solutions to the shortcomings of informed consent in privacy, analyzing them in terms of their paternalistic or libertarian character; c) through a theoretical and normative analysis and after performing comparisons with analogous cases in different industries, discussing what are the most suitable solutions to informed consent in privacy and what background - paternalistic or libertarian - they should have.

7.2 Characterization of the Modeling Approach

In the first stage of the research, the shortcomings of informed consent in privacy in terms of their related behavioral characteristic (cognitive limitation, information asymmetry and time constraint) will be modeled. Then, in a second stage, bridges with other fields which presented similar behavioral issues will be built, seeking to understand: a) what was the policy response to each of those issues; and b) what kind of insights can be extracted and applied in the field of information privacy.

Behavioral economics is a suitable framework because of the tools it offers to understand biases, human limitations and other influencing factors during decision making. To consent or not is a complex decision, influenced by multiple psychological and behavioral elements. Behavioral economics will help unravel these elements, providing a deeper and interdisciplinary view of shortcomings and available solutions to informed consent in information privacy.

As a definition, Thaler and Mullainathan (2000, p.1) state that "behavioral economics is the combination of psychology and economics that investigates what happens in markets in which some of the agents display human limitations and complications." In some sense it is essentially critical to the assumptions of classic economy, which are:

a) agents have well-defined preferences and unbiased beliefs and expectations; b) they make optimal choices based on these beliefs and preferences. This in turn implies that agents have infinite cognitive abilities (or, put another way, are as smart as the smartest economist) and infinite willpower since they choose what is best, not what is momentarily tempting; and c) although they may act altruistically, especially toward close friends and family, their primary motivation is self-interest (Thaler, 2016, p. 1579).

The assumptions above define the *Homo economicus*, or the *Econ*. Behavioral economics replaces Econs with *Homo sapiens* (Thaler, 2016, p. 1579), focusing on what is the real human behavior, as it can be viewed empirically, and not a rational prediction of what human behavior could be.

As will be advocated in the thesis, behavioral economics is a useful tool to design regulatory models, and different authors have suggested ways to perform this task. Acquisti et al. (2015), for example, account for data subjects' vulnerabilities in the privacy realm and propose that policy decisions take that into consideration. Aligned with the premises of behavioral economics, which see the individuals as likely to commit errors and be influenced by emotional states, they affirm that policies that focus only on "empowering the individual" are likely to be ineffective, and propose that policies require from data subjects minimal informed and rational decision-making, thus having a protective base independent of human action. In the same line, Thaler and Sunstein (2009) propose policy strategies aligned with the premises of behavioral economics. They support libertarian paternalism, in which *nudges* are allowed in order to help people take decisions that would benefit them more. An interesting question regarding libertarian paternalism, and which will be discussed in the context of the paternalism-libertarianism spectrum, is to what extent the choice architect is sufficient to decide what is the best option for a group of individuals. Lastly, Sunstein (2011), in a different work, provides a framework of how behavioral economics can positively influence regulation, giving examples from different industries and directly migrating concepts from behavioral economics to law.

Behavioral economics also helps us understand situations where there is manipulation involved, as companies may benefit from existing biases in the data subject's behavior in order to promote their interests. Ryan Calo (2014, p. 999) has explored this concept, explaining that the digitalization of commerce increases the capacity of companies to exploit the limits of a consumer's ability to pursue his or her self-interest, triggering irrationality or vulnerability and leading to harm; he also adds that behavioral economics offers a useful framework to deal with this challenge (Calo, p.999). In a similar sense, Conti and Sobiesk (2010, p.278) state that "malicious interface techniques are commonplace both on and off the desktop, and are in direct contradiction to usable interface design best practices as well as several laws and statutes." They also offer a taxonomy for those techniques, proposing further studies of each category: "coercion, distraction, exploiting errors, forced work, obfuscating desired content, restricting or masking functionality, and deception or misrepresentation, among others." (p. 278) As Calo and Conti & Sobiest make it clear, data subjects, who are already impacted by information asymmetry in relation to companies, are made even more vulnerable by these manipulative techniques; some of the shortcomings presented in the previous section are related to this issue and possible solutions to them will be explored.

The next step after modeling the behavioral characteristics of the shortcomings of informed consent is to compare them to cases from other industries where similar behavioral issues were involved, assessing in each case what was the policy decision adopted and how these insights can be useful in the information privacy context.

7.3 Initial description of the modeling approach that will be taken (what kind of model will be developed, what will, and what will not be modeled, etc.)

Authors from different fields have been pinpointing informed consent's shortcomings. They are grouped and named below according to their behavioral characteristics and list them in Table 7.1.

Table 7.1: Shortcoming of informed consent in privacy

Shortcomings of Informed Consent in Privacy		
Name of the Shortcoming	Characteristics	Type
a) Complexity	The length and legalistic language of the privacy notices make it hard for the average data subjects to understand it and therefore to provide an informed decision regarding the collection of their personal data. Without a proper understanding of what is being notified, it is improbable that the consent that is given will be informed;	Cognitive Limitation
b) Present Bias	Behavioral economists have shown that human beings tend to constantly undervalue the possible long term disadvantages and overvalue the short-term benefits of a certain action or activity; In the context of informed consent it means that people will accept data collections with long term risks in exchange for short term benefits, such as access to a website, because they are biased and are unable to realize the real gravity of long term risks. Therefore, the existence of biases also highlights the doubt about whether the consent offered is informed or not (i.e., if the data subject really considered the risks informed or not)	Cognitive Limitation
c) Manipulation	Studies show that companies manipulate the format, language and content of privacy notices in order to obtain the consumer choice that is more advantageous to their business goals. This casts doubts on whether the data subjects are willingly consenting to a certain data collection, or if they are being manipulated to do that. Therefore, even in the presence of stricter rules, if there is no close control of what is happening on the ground, companies may circumvent informed consent requirements	Cognitive Limitation
d) Ubiquity	A study showed that if a person decided to read all the privacy policies he or she encounters in a year, he or she would take seventy-six work days to do it. This is an illustration of how long and complex they are and, besides improbable, undesirable and maybe impossible, how economically inefficient it would be to promote all this reading.	Time Constraint
e) Multiple Sources of Collection	In new information systems such as smart cities, there are multiple sources of collection with diverse purposes, thus presenting a challenge on how to design privacy notices that can reflect all the different types of data uses without overwhelming the data subject	Time Constraint
f) Continual Collection	Some wearables are constantly collecting data, therefore there is the challenge of knowing how many times should consent be required and also the challenge of not overwhelming the data subject with thousands of consent requests a day	Time Constraint
g) Lack of Awareness	Information privacy and its existing risks and concerns are subjects not yet broadly diffused and understood by the general public. Besides that, important figures in the industry and new technologic trends seem to influence the public into undervaluing privacy, therefore reducing people's incentive to read privacy notices and inform themselves about data collection and processing. If people do not want to be informed and do not read privacy notices, their consent cannot be deemed informed	Information Asymmetry
h) Unfeasibility	In the context of big data techniques, companies engage in a massive data collection, in the first place, and only afterwards they may know more precisely how they will use the data, therefore the notice in advance will be	Information Asymmetry

	inevitably incomplete, preventing the consent to be deemed informed (as the data subject was not informed of future uses of his or her data);	
i) Lack of Control	Some authors argue that merely consenting in advance is not enough to configure plain informed consent. It would be necessary to allow data subjects to have greater control over their data, allowing them to see, edit and delete, whenever they want, all the data that was collected	Information Asymmetry
j) Lack of Interface	In the case of surveillance systems, such as CCTVs, some biometrics and some wearables, there is not an interface between the data subject and the data collector, therefore posing a challenge on how to inform the data subject about the collection of the data, in order to obtain informed consent;	Information Asymmetry

The modeling approach will compare those identified behavioral issues with cases from other industries that presented similar characteristics, focusing on the policy decision that was adopted in each case and how they can generate new insights to the information privacy context.

7.4 Next steps in the model development and evaluation

The next steps of the modeling approach will be: a) further analyze the behavioral characteristics of the shortcomings of informed consent; b) build analogies with other fields that presented similar behavioral characteristics and c) verify what policy solutions were adopted in each case, focusing on their paternalistic or libertarian background.

On the analysis of the policy solutions, a spectrum that goes from paternalism to libertarianism was developed, and the aim is to evaluate them according to these parameters. The last step will be to use these policy assessments from other fields to analyze alternatives to informed consent in the information privacy context.

Table 7.2: Paternalism-Libertarianism Spectrum

Paternalism-Libertarianism Spectrum							
Name of category	Interventionist Paternalism (Legal and Technological)		Objective Paternalism	Libertarian Paternalism	Paternalistic Libertarianism	Technological Libertarianism	Market Libertarianism
Charac-teristic	Legal: laws determine what must be done; there is no choice available to the user	Technological: developers build rigid systems that have a political/legal choice embedded on it; there is no choice left to the user	A rule, after issued, is followed up by continuous tests or inquiries in order to validate its efficacy. If it's not achieving the desired results, the rule has to change	Interventions are made by choice architects, helping users to choose the options that are more beneficial to them. User can opt out	Design, cognitive facilitators or any other tools are used to improve the quality of the user's choice. However, the choice of the improvements is not made by the user	Users have the help of technological agents or tool to make better choices	Users have total freedom to trade and profit from their assets. Constitutional or public law limits might apply
In the context of informed consent	More substantive laws should be issued, determining what data can be collected and processed, how and when	Rules determine higher privacy standards to protect data subjects	A new rule on informed consent is issued and is constantly being tested to see if the desired result is achieved	The default option is the most privacy protecting one.	Privacy notices are improved through design and other resources to help its comprehension	Privacy agents help users decide the best privacy choice for them	Data subjects can freely trade their personal data and even profit from it

8 ESR-12 (UCL) Mark Warner - Exploring narratives as functions for developing conviction in privacy decision-making

8.1 Introduction

This research is concerned with understanding and modelling the privacy disclosure decision-making behaviour of MSM when diagnosed with HIV. The behavioural model being proposed extends existing privacy theory to include narrative construction and identity, proposed as a function for building conviction around disclosure decisions for managing identity in conditions of uncertainty.

8.2 Research Question

This research is an exploration of the privacy dynamics involved in the management of online identities through self-disclosure and self-presentation. The research will focus on a specific demographic, men who have sex with men (MSM) who have recently been diagnosed with HIV. MSM are disproportionately affected by HIV in the UK, accounting for almost half of those currently diagnosed (Terrence Higgins Trust, n.d.). The anachronistic discourse around HIV as a highly infectious and life threatening condition is a cause of stigma (Henry et al., 2015), an attribute Goffman (1963) describes as a deeply discrediting aspect of a person's identity. This increases the privacy concerns of those affected by the condition (Derlega, Green, Serovich, & Elwood, 2002; Fesko, 2001; Winchester et al., 2013; Zhang & Li, 2017), creating a heightened state of uncertainty when developing online disclosure decisions. Under these conditions, how do MSM when diagnosed with HIV manage their online identities through self-presentation and self-disclosure, while protecting their privacy?

8.3 Modelling Approach

The privacy model developed by Adams and Sasse (2001) presented in Figure 8.1 provides a view of the decision-making processes around information disclosure, using a cost-benefit analysis model to weigh the perceived costs of disclosing against the perceived benefits. The model introduces trust in the data recipients and judgement of the sensitivity of the information, two subjective and emotionally influenced factors. These factors, together with the uncertainty over both the short and long-term costs to privacy are explored here with the use of conviction narrative theory (CNT) (Chong & Tuckett, 2015; Tuckett & Nikolic, 2016).

This social-psychological theory is proposed as an extension to the existing model (Figure 8.1). Whilst many of the decision-making theories take a dual model approach, with Kahneman (2011) popularising this with System 1 and System 2. CNT instead suggests a circular interaction exists between the cognitive analytical (System 2) and emotional (System 1) processes, activated within a person's social context. CNT is a judgement and decision-making theory, developed by Chong and Tuckett (2015) to model behavioural decision-making under conditions of uncertainty. These conditions are created when actions are taken that are affected by a future that is today unknowable. In the world of technology this is especially pertinent, with technological evolutions creating changes to the complex socio-technical systems within which we interact.

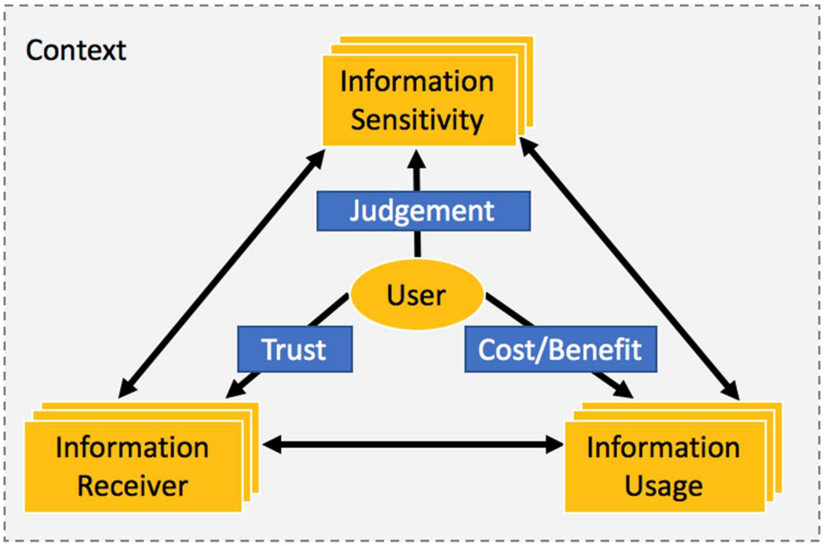


Figure 8.1: Privacy model factors and issues. Adapted from "Privacy in multimedia communications: Protecting users, not just data." By A. Adams and M. Sasse, 2001, In People and Computers XV—Interaction without Frontiers

The model being proposed in this current research is presented in Figure 8.2, introduces the Adams and Sasse (2001) privacy model as a component for developing narratives used by individuals' in forming decision conviction affecting identity. CNT proposes that in conditions of uncertainty, when the probability of a successful action cannot be known through the application of a probability calculus, narratives are developed to help build conviction towards decisions. Online technologies are often subject to information system asymmetry, with users being unaware of how their data will be handled by the information receiver. As the pace of technological change is so fast moving, long-term costs are often unforeseen or unknown at the point the information is disclosed (Acquisti & Grossklags, 2005). Whilst existing privacy models (Adams & Sasse, 2001; Dinev & Hart, 2006) identify factors affecting disclosure, they do not explain how users are able to build conviction for decision-making, and how the outcome of these decisions can support future decisions. When a MSM is diagnosed with HIV, disclosure and the risk disclosure has on identity creates an environment of considerable uncertainty.

Because of these concerns, where a choice exists, seropositive MSM are unlikely to disclose their serostatus unless there is a perceived benefit in doing so. The first phase of this model proposes the creation of a set of initial, high level goal based narratives. These may include narratives for "protecting long-term privacy", as well as "gaining help and support" for the person's newly diagnosed condition. Using this model, high-level narratives are used to seek out opportunities that support a persons' goals. As an example, MSM diagnosed with HIV may seek knowledge, help and support around their condition and identify support websites where they can interact with people with share experiences. They may identify websites that allow them to browse without giving over their name or any personal details.

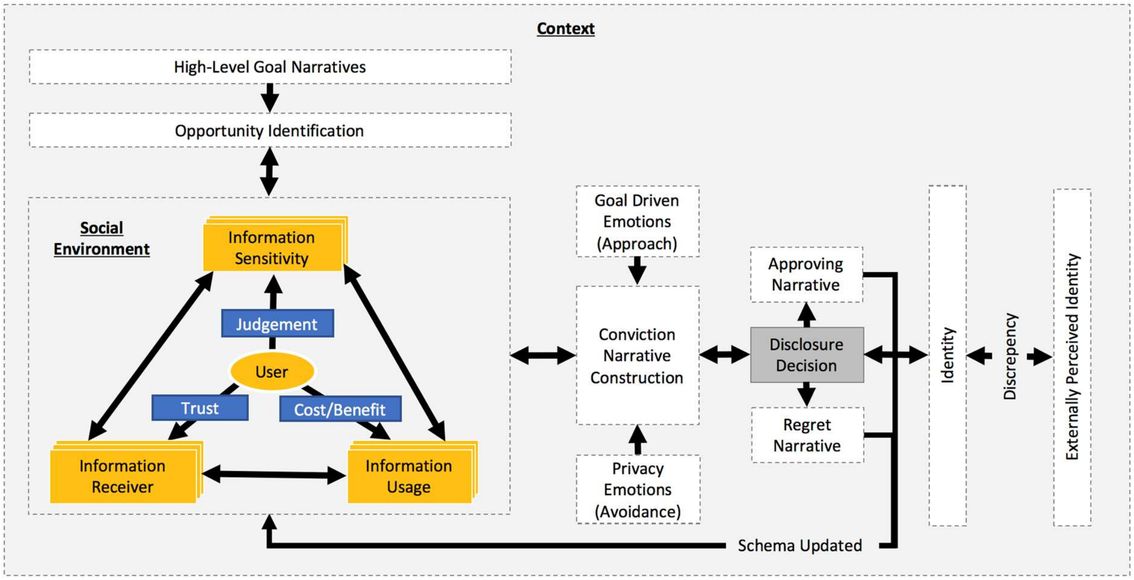


Figure 8.2: Proposed privacy narrative model developed for this research

Once an opportunity has been identified to meet a high-level goal, a set of rules are proposed that enable individuals to start evaluating possible future disclosure actions. The Adams and Sasse (2001) privacy model (Figure 8.1) proposes three decision functions that a user will evaluate before taking action: a judgement on the sensitivity of the information being disclosed, an evaluation of the trust in the information receiver and an analysis of the cost and benefit. In this current research, it is proposed that individuals use a set of adaptive heuristics (Gigerenzer & Todd, 1999; Kahneman, 2011) that fit previous schemas of behaviour from memory to evaluate these decision-factors (Klein, 2008). Schemas and heuristics are used to assess these elements of the model against the goals pursued by the individual.

To help the individual evaluate the complex technical environment within which they are disclosing, narratives are constructed, allowing them to visualize and compare different future scenarios resulting from the various identified actions. These narratives are developed as a result of a human capacity to visualise, describe and communicate the future using an ability to use memory to mentally travel both into the past and the future (Chong & Tuckett, 2015; Suddendorf & Corballis, 1997; Tulving, 1993). This simulation of the future using narratives allows individuals to "test" their actions, developing and simulating different narratives for different scenarios, creating subjective "knowledge" on their outcomes which create either approach or avoidance emotions. When evaluating the action of disclosure, individuals may discover new information, which cause them to develop avoidance or approach emotions. Depending on the state of the individual, this new information may impact on the narrative they have developed, CNT proposes two states: integrated (I^S) and divided (D^S)(Chong & Tuckett, 2015).

People in a D^S are not open to information which conflicts with their existing narrative, only allowing for positive narrative reinforcement, whilst in an I^S people continue to re-evaluate their narrative, allowing for conflicting approach and avoidance feelings to develop. If new information is received, the I^S will accept and process this information and re-evaluate the narrative, changing actions and the narrative completely if the new information creates feelings of unpleasantness. When conflicting information is received in the D^S, the individual will receive and store the information, but will not process or reflected upon it, perhaps until the persons' state changes.

In the social environment, when making decisions in uncertain conditions, Tuckett and Nikolic (2016) suggest that narratives are used to more easily communicate information and emotions in order to gain co-operation. This function may result in receiving narratives from others that create feelings of approach or avoidance, and depending on the state in which the person is in, may result in a stronger feeling of accuracy or in re-assessment of the disclosure. In the context of online interactions, people may seek guidance online, reading the narratives of others who have been through similar experiences to develop support for their own actions.

Once a disclosure decision has been made, the results from the actions will create a lived experience, impacting on a person’s identity within a specific context. In this current research, we draw on Goffman's (1959) dramaturgical approach to identity, suggesting that this information is used to present a version of the person’s self to their external audience, evaluating how this information has affected the impression they have “given-off”. The discrepancy between how the person believes they are, and how their external audience perceived them is likely to impact on the creation of the experience narrative. If the perception of others is negative, a regret narrative is created; if the discrepancy between the two identity states is low, and the impression “given-off” is a positive one, an approving narrative is created. These experience narratives are fed back into the social environment of the individual acting as a form of social learning, as well as being stored in the persons’ memory as schemas of behaviour, used in future decisions-making (Klein, 2008).

8.4 Next Steps

The initial modelling approach taken in this research will be based on exploratory, qualitative interviews carried out with MSM who have been recently diagnosed with HIV in the UK. This initial phase of the research will allow for discovery, and to determine the “fit” of the proposed model, and existing privacy models within the context of the research area. This research will be further developed to understand and model how people manage tensions that may develop between long term privacy narratives, and short term user goals.

Whilst the acceptance of technologies that enables disclosure of information is an important aspect of the user engagement lifecycle. Technology acceptance is outside the scope of this research, but may be discussed as a consideration to our findings.

9 Conclusions

The different sections in the document present the thoughts and progress the ESRs made in the development of their individual research projects. They also describe the initial steps they took to develop models of privacy-related decisions in the context of their PhD research.

When reading the different sections, it is clear that the ESRs are at different points in their work and at different levels of development of their work. This is natural, given that the research projects are each on its own trajectory and will continue to develop in parallel with some developing certain aspects of the work earlier than others.

One observation that arises from reading the contribution is the overlap and the existence of possible connections between the different projects, at least at the level of the methods they will use. Hence we will encourage ESRs to discuss their modelling approaches with others. Perhaps this can allow them to create syntheses of models or to benefit from insights and knowledge others have gained.

10 References

Acquisti, A., & Grossklags, J. (2003). Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. 2nd Annual Workshop on "Economics and Information Security, 3, 1–27.

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making challenges in privacy decision making. IEEE Security & Privacy, 3(1), 26–33.

Acquisti, A., Brandimarte, L., Loewenstein, G. (2015). Privacy and human behavior in the age of information, Science, 347 (6221) 509.

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. Journal of Economic Literature, 54(2), 442-492.

Adams, A., & Sasse, M. (2001). Privacy in multimedia communications: Protecting users, not just data. People and Computers XV—Interaction without Frontiers. Retrieved from http://link.springer.com/chapter/10.1007/978-1-4471-0353-0_4

Ajzen, I., & Fishbein, M. (2000). Attitudes and the attitude-behavior relation: Reasoned and automatic processes. European Review of Social Psychology, 11(1), 1–33. http://doi.org/10.1080/14792779943000116

Baek, Y. M. (2014). Solving the privacy paradox: A counter-argument experimental approach. Computers in Human Behavior, 38, 33–42. http://doi.org/10.1016/j.chb.2014.05.006

Barberis, N. C. (2013). Thirty years of prospect theory in economics. The Journal of Economic Perspectives, 27(1), 173-195.

Barlett, C. P. (2012). Direct and indirect relations between the Big 5 personality traits and aggressive and violent behavior. Personality and Individual Differences 52.8, (pp. 870-875).

Benenson, Z., Girard, A., & Krontiris, I. (2015). User acceptance factors for anonymous credentials: an empirical investigation. Workshop on the Economics of Information Security (WEIS).

Bentler, P. M., & Speckart, G. (1979). Models of attitude-behavior relations. Psychological Review, 86(5), 452–464. http://doi.org/10.1037//0033-295X.86.5.452

Bentler, P. M., & Speckart, G. (1981). Attitudes "cause" behaviors: a structural equation analysis. Journal of Personality and Social Psychology, 40(2), 226–238. http://doi.org/http://shelob.ocis.temple.edu:3395/10.1037/0022-3514.40.2.226

Beresford, A. R., Kübler, D., & Preibusch, S. (2012). Unwillingness to pay for privacy: A field experiment. Economics Letters, 117, 25–27. http://doi.org/10.1016/j.econlet.2012.04.077

Betsch, T., Haberstroh, S., & Höhle, C. (2002). Explaining Routinized Decision Making. A Review of Theories and Models. Theory & Psychology, 12(4), 453–488. http://doi.org/0803973233

Blöckner, M. (2009). Please touch the exhibits!: using NFC-based interaction for exploring a museum. Proceedings of the 11th International Conference on Human-Computer Interaction with Mobile Devices and Services. ACM.

Boes, K. L. (2015). The Acceptance of NFC Smart Posters in Tourism. Information and Communication Technologies in Tourism Springer International Publishing, (pp. 435-447).

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced Confidences: Privacy and the Control Paradox. Social Psychological and Personality Science, 4(3), 340–347. http://doi.org/10.1177/1948550612455931

Calo R. (2014). Digital market manipulation. George Washington Law Review, 82, 995.

Canelas, M., & Feigh, K. (2016). Toward Simple Representative Mathematical Models of Naturalistic Decision Making Through Fast-and-Frugal Heuristic. Journal of Cognitive Engineering and Decision Making, 10(3), 255–267.

Carrascal, J., & Riederer, C. (2013). Your browsing behavior for a big mac: Economics of personal information online. Proceedings of the …, 11. Retrieved from http://arxiv.org/abs/1112.6098%5Cnhttp://dl.acm.org/citation.cfm?id=2488406

Cavagnaro, D. R., Myung, J. I., & Pitt, M. a. (2010). Mathematical Modeling. In The Oxford Handbook of Quantitative Methods in Psychology, Vol. 1 (pp. 437–452).

Chae, J. S. (2015). Business Models for NFC based mobile payments. Journal of Business Models 3.1.

Cheung, W., Chang, M. K., & Lai, V. S. (2000). Prediction of Internet and World Wide Web usage at work: A test of an extended Triandis model. Decision Support Systems, 30(1), 83–100. http://doi.org/10.1016/S0167-9236(00)00125-1

Cho, H. (2010). Determinants of behavioral responses to online privacy: The effects of concern, risk beliefs, self-efficacy, and communication sources on self-protection strategies. Journal of Information Privacy & Security, 6(1), 3–27. http://doi.org/10.1080/15536548.2010.10855879

Chong, K., & Tuckett, D. (2015). Constructing conviction through action and narrative: how money managers manage uncertainty and the consequence for financial market functioning. Socio-Economic Review. Retrieved from http://ser.oxfordjournals.org/content/13/2/309.short

Choo, J. H. (2012). I 2 navi: An indoor interactive NFC navigation system for android smartphones. Proceedings of the World Academy of Science, Engineering and Technology 72, (pp. 735-739).

Conti, G. & Edward S. (2010). Malicious Interface Design: Exploiting the User, International World Wide Web Conference Committee, 278.

Coopamootoo, K. P. L., & Groß, T. (2014). Mental Models : An Approach to Identify Privacy Concern and Behavior. Symposium on Usable Privacy and Security.

Crane, S., Lacohée, H., & Zaba, S. (2006). Trustguide—trust in ICT. BT Technology Journal, 24(4), 69-80.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS quarterly, 319-340.

Denes-Raj, V., & Epstein, S. (1994). Conflict Between Intuitive and Rational Processing: When People Behave Against Their Better Judgment. Journal of Personality and Social Psychology, 66(5), 819–829. http://doi.org/10.1037/0022-3514.66.5.819

Derlega, V., Green, K., Serovich, J., & Elwood, W. (2002). Perceived HIV-related Stigma and HIV Disclosure to Relationship Partners after Finding Out about the Seropositive Diagnosis. Journal of Health Psychology, 7(4), 415–432.

Devaraj, S. R. (2008). Research note—how does personality matter? Relating the five-factor model to technology acceptance and use. Information Systems Research 19.1, (pp. 93-105).

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents - measurement validity and a regression model. Behaviour & Information Technology, 23(6), 413–422. http://doi.org/10.1080/0144929041000171 5723

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents-measurement validity and a regression model. Behaviour & Information Technology, 23(6), 413-422.

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. Information Systems Research, 17(1), 61–80. http://doi.org/10.1287/isre.1060.0080

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. European Journal of Information Systems, 22(3), 295-316.

Egelman, S., & Peer, E. (2015). Predicting privacy and security attitudes. ACM SIGCAS Computers and Society, 45(1), 22-28.

Eling, N., Krasnova, H., Widjaja, T., & Buxmann, P. (2013). Will you accept an app? Empirical investigation of the decisional calculus behind the adoption of applications on Facebook. Thirty Fourth International Conference on Information Systems, Milan.

Fesko, S. L. (2001). Disclosure of HIV status in the workplace:

Gigerenzer, G., & Todd, P. M. (1999). Fast and frugal heuristics: the adaptive toolbox. Simple Heuristics That Make Us Smart. https://doi.org/10.1177/1354067X0171006

Goffman, E. (1959). The Presentation of Self in Everyday Life. Teacher, 21(5), 259. https://doi.org/10.2307/2089106

Goffman, E. (1963). Stigma. Notes on the management of spoiled identity. A Spectrum Book. https://doi.org/10.2307/2091442

Gonzalez, C., & Meyer, J. (2016). Integrating Trends in Decision-Making Research. Journal of Cognitive Engineering and Decision Making, 10(2), 120–122. http://doi.org/10.1177/1555343416655256

Gonzalez, C., Meyer, J., Klein, G., Yates, J. F., & Roth, A. E. (2013). Trends in Decision Making Research: How Can they Change Cognitive Engineering and Decision Making in Human Factors? Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 57(1), 163–166. http://doi.org/10.1177/1541931213571037

Grossklags, J., Hall, S., & Acquisti, A. (2007). When 25 Cents is too much : An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information. Information Security, 7–8. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.137.696&amp;rep=rep1&amp;type=pdf

Hann, I., Hui, K., Lee, S. T., & Png, I. P. (2007). Overcoming Online Information Privacy Concerns: An Information Processing Theory Approach. Journal of Management Information Systems, 24(2), 13-42.

Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., & Png, I. P. L. (2014). Overcoming Online Information Privacy Concerns: An Information Processing Theory Approach. Journal of Management Information Systems, 24(2), 13–42.

Henry, E., Bernier, A., Lazar, F., Matamba, G., Loukid, M., Bonifaz, C., … Préau, M. (2015). Was it a Mistake to Tell Others That You are Infected with HIV????: Factors Associated with Regret Following HIV Disclosure Among People Living with HIV in Five Countries (Mali, Morocco, Democratic Republic of the Congo, Ecuador and Romania). Results from. AIDS and Behavior, 19(2), 311–321. https://doi.org/10.1007/s10461-014-0976-8

Hotaling, J. M., & Busemeyer, J. R. (2012). DFT-D: a cognitive-dynamical model of dynamic decision making. Synthese, 67–80. http://doi.org/10.1007/s11229-012-0157-0

International Organization for Standardization (2009). Ergonomics of human system interaction - Part 210: Human-centered design for interactive systems (formerly known as 13407). ISO FDIS 9241-210:2009

Ion, I., Sachdeva, N., Kumaraguru, P., & Čapkun, S. (2011, July). Home is safer than the cloud!: privacy concerns for consumer cloud storage. In Proceedings of the Seventh Symposium on Usable Privacy and Security (p. 13). ACM.

Jäger, H. A., Monitzer, A., Rieken, R., Ernst, E., & Nguyen, K. D. (2014). Sealed cloud-a novel approach to safeguard against insider attacks. In Trusted Cloud Computing (pp. 15-34). Springer International Publishing.

Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of Internet users: Self-reports versus observed behavior. International Journal of Human Computer Studies, 63(1–2), 203–227. http://doi.org/10.1016/j.ijhcs.2005.04.019

Joinson, A. N., Paine, C., Buchanan, T., & Reips, U. D. (2008). Measuring self-disclosure online: Blurring and non-response to sensitive items in web-based surveys. Computers in Human Behavior, 24(5), 2158–2171. http://doi.org/10.1016/j.chb.2007.10.005

Judge, T. A. (2002). Relationship of personality to performance motivation: a meta-analytic review. Journal of applied psychology 87.4, (p. 797).

Kahneman, D. (2011). Thinking, fast and slow. Allen Lane.

Kahneman, D., & Frederick, S. (2002). Representativeness revisited: Attribute substitution in intuitive judgmen. Heuristics of Intuitive Judgment: Extensions and Applications, (January 2002), 1–30. http://doi.org/10.1038/2251090a0

Kahneman, D., & Klein, G. (2009). Conditions for Intuitive Expertise: A Failure to Disagree. American Psychologist, 64(6), 515–526. http://doi.org/10.1037/a0016755

Kehr, F., Wentzel, D., Kowatsch, T., & Fleisch, E. (2015). Rethinking Privacy Decisions: Pre-Existing Attitudes, Pre-Existing Emotional States, and a Situational Privacy Calculus. In ECIS 2015 Completed Research Papers. Retrieved from http://aisel.aisnet.org/ecis2015_cr

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. International Journal of Human-Computer Studies, 71(12), 1163-1173.

Klein, G. (2008). Naturalistic decision making. Human Factors, 50(3), 456–460. https://doi.org/10.1518/001872008X288385

Klein, G. (2015). A naturalistic decision making perspective on studying intuitive decision making. Journal of Applied Research in Memory and Cognition, 4(3), 164–168. http://doi.org/10.1016/j.jarmac.2015.07.001

Kokolakis, S. (2015). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security. http://doi.org/10.1016/j.cose.2015.07.002

Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. Identity in the Information Society, 2(1), 39-63.

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: why we disclose. Journal of Information Technology, 25(2), 109-125.

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: The role of culture. Business & Information Systems Engineering, 4(3), 127-135.

Lacohée, H., Crane, S., & Phippen, A. (2006). Trustguide: final report. Trustguide. October, 1, 25.

Lee, Z.-Y. H.-C.-J. (2001). An analysis and comparison of different types of electronic payment systems. Management of Engineering and Technology. PICMET'01. Portland International Conference on. IEEE.

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. Decision Support Systems, 51(3), 434–445. http://doi.org/10.1016/j.dss.2011.01.017

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. Decision Support Systems, 51(3), 434-445.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. Decision Support Systems, 54(1), 471–481. http://doi.org/10.1016/j.dss.2012.06.010

Loewenstein, G., Hsee, C. K., Weber, E. U., & Welch, N. (2001). Risk as Feelings. Psychological Bulletin, 127(2), 267–286.

Lu, Y. (2011). Dynamics between the trust transfer process and intention to use mobile payment services: A cross-environment perspective. Information & Management 48.8 , (pp. 393-403).

Lutz, C., & Strathoff, P. (2013). Privacy concerns and online behavior – Not so paradoxical after all? Multinationale Unternehmen Und Institutionen Im Wandel – Herausforderungen Für Wirtschaft, Recht Und Gesellschaft, 81–99. http://doi.org/10.2139/ssrn.2425132

Mahmood, S., & Desmedt, Y. (2013). Two new economic models for privacy. ACM SIGMETRICS Performance Evaluation Review, 40(4), 84-89.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information Systems Research, 15(4), 336–355. http://doi.org/10.1287/isre.1040.0032

Marshall, C., & Tang, J. C. (2012, June). That syncing feeling: early user experiences with the cloud. In Proceedings of the Designing Interactive Systems Conference (pp. 544-553). ACM.

Mcknight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. ACM Transactions on Management Information Systems (TMIS), 2(2), 12.

Mullainathan, S. & Thaler, R. (2000). Behavioral Economics, NBER Working Paper No. w7948.

Nissenbaum, H. (2009). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox : Personal Information Disclosure Intentions vers us Behaviors. The Journal of Consumer Affairs, 41(1), 100–126. http://doi.org/10.1111/j.1083-6101.2009.01494.x

Ondrus, J. a. (2007). An assessment of NFC for future mobile payment systems. Management of Mobile Business, 2007. ICMB 2007. International Conference on the. IEEE.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trustand risk with the technology acceptance model. International journal of electronic commerce, 7(3), 101-134.

Perugini, M., & Bagozzi, R. P. (2001). The role of desires and anticipated emotions in goal-directed behaviours: Broadening and deepening the theory of planned behaviour. British Journal of Social Psychology, 40(1), 79–98. http://doi.org/10.1348/014466601164704

Pesonen, J. a. (2012). Near field communication technology in tourism. Tourism Management Perspectives 4 , (pp. 11-18).

Pousttchi, K. M. (2009). Proposing a comprehensive framework for analysis and engineering of mobile payment business models. Information Systems and E-Business Management 7.3 , (pp. 363-393).

Prismacloud Consortium. (2015). Legal, Social, and HCI Requirements. Deliverable D2.1.

Regulation, E. U. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union (OJ), 59, 1-88.

Shin, S. a.-j. (2014). The effects of technology readiness and technology acceptance on NFC mobile payment services in Korea. Journal of Applied Business Research 30.6.

Slovic, F. (2002). The Affect Heuristic. Heuristics and Biases; The Psychology of Intuitive Judgement, 397–420. http://doi.org/10.1016/j.ejor.2005.04.006

Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2004). Risk as analysis and risk as feelings. Risk Analysis, 24(2). Retrieved from papers2://publication/uuid/F4B3EA59-C2F7-4F62-9223-701C27F152C2

Solove, D. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, (477), 477–560.

Spiekermann, S. (2008). User control in ubiquitous computing: design alternatives and user acceptance. Aachen, Germany: Shaker.

Staib, P. J. (n.d.). System and method of facilitating contactless payment transactions across different payment systems using a common mobile device acting as a stored value device. U.S. Patent Application No. 10/940,939.

Suddendorf, T., & Corballis, M. (1997). Mental time travel and the evolution of the human mind. Genetic, Social, and General Psychology. Retrieved from http://cogprints.org/725

Sunstein, C. (2011). Empirically informed regulation. University of Chicago Law Review, 78, 1349 (2011).

Tan, G. W.-H. (2014). NFC mobile credit card: the next frontier of mobile payment? Telematics and Informatics 31.2, (pp. 292-307).

Terrence Higgins Trust. (n.d.). How common is HIV? | Terrence Higgins Trust. Retrieved March 5, 2017, from http://www.tht.org.uk/sexual-health/About-HIV/How-common-is-HIV_qm_

Thaler, R. & Sunstein, C. (2009). Nudge: Improving Decisions about Health, Wealth, and Happiness.

Thaler, R. (2016). Behavioral economics: Past, present, and future. American Economic Review, 106, 1577.

Tuckett, D., & Nikolic, M. (2016). The Role of Conviction and Narrative in Decision Making under Radical Uncertainty. Researchgate.net, (August). Retrieved from https://www.researchgate.net/profile/David_Tuckett2/publication/271215450_Constructing_conviction_through_action_and_narrative_How_money_managers_manage_uncertainty_and_the_consequence_for_financial_market_functioning/links/57ce985d08ae582e0693419e.pdf

Tulving, E. (1993). What is episodic memory? Current Directions in Psychological Science. Retrieved from http://www.jstor.org/stable/20182204

Wakefield, R. (2013). The influence of user affect in online information disclosure. Journal of Strategic Information Systems, 22(2), 157–174. http://doi.org/10.1016/j.jsis.2013.01.003

Warshaw, P. R., & Davis, F. D. (1985). Disentangling behavioral intention and behavioral expectation. Journal of experimental social psychology, 21(3), 213-228.

Whitman, J. (2004). The two western cultures of privacy: Dignity versus liberty. Yale Law Journal, 113, 1151.

Winchester, M. S., McGrath, J. W., Kaawa-Mafigiri, D., Namutiibwa, F., Ssendegye, G., Nalwoga, A., … Rwabukwali, C. B. (2013). Early HIV disclosure and nondisclosure among men and women on antiretroviral treatment in Uganda. AIDS Care, 25(10), 1253–1258. https://doi.org/10.1080/09540121.2013.764386

Xu, H., Luo, X., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. Decision Support Systems, 51(1), 42-52.

Zhang, Y., & Li, X. (2017). Uses of information and communication technologies in HIV self-management: A systematic review of global literature. International Journal of Information Management, 37(2), 75–83. https://doi.org/10.1016/j.ijinfomgt.2016.11.003

11 Index of figures

12 Index of tables