D6.7 Researcher Declarations and Career Development

Deliverable Number	**D6.7**
Work Package	6
Version	1.0
Deliverable Lead Organisation	UNI
Dissemination Level	PU
Contractual Date of Delivery (release)	31/05/2017
Date of Delivery	04/07/2017
Status	**Final**

Editor

Hubert Jaeger, Uniscon GmbH

Contributors

All ESR

Reviewers

Supervisors of each ESR respectively, Simone Fischer Hübner (KAU), Eva Glavenius (KAU)

Abstract

This document is the collection of all PhD Research Proposals and Career Development Plans. All ESRs have submitted their PhD Research Proposals and Career Development Plans, which were devised with their supervisors and cosupervisors, discussed at the Network-wide Event in Vienna end of May and are approved by the Supervisory Board.

The purpose of the concrete PhD Research Proposals is to cope with the short time of three years to complete the PhD studies and the thesis. The purpose of the Career Development Plans is to orientate supervisors and co-supervisors as well as the network management to steer the ESR to best prepare them for their career after completion of PhD studies.

Table of Contents

1 Introduction

1.1 Scope and Objectives

This document is a collection of all reviewed PhD Research Project Plans (or Research Proposal - RP) and Career Development Plans (CDP) of the Early Stage Researchers (ESRs) of the EU H2020 Innovative Training Network Privacy&Us.

The purpose of the actual and detailed RPs is to cope with the brief period of time, namely three years, to complete the respective PhD studies and theses. Thus, a detailed planning is recommended. The RP therefore serves as a research roadmap and timeline in the development of ESR's individual research projects during the 3-year training programme. The RP should include a description of the background, an extensive review of the literature, a research statement including the research questions, the proposed approach, a discussion of the selected methods and a detailed work and time plan specifically highlighting the different stages of research and the research methodologies to be applied at each stage.

The purpose of the CDPs is to orientate supervisors, co-supervisors, and the Network Management, to be able to steer the ESRs, in order to best prepare them for their career upon completion of their PhD studies. The CDP should especially also enable the early detection of potential issues that may hamper the overall progress of the ESR's research project, and ultimately the Privacy&Us project.

In addition to title and organizational information, e.g. hosting organization, supervisor names, conduct of supervision, secondments, project description, training schedule, and other activities, the core elements of a personalised CDP include the individual long terms goals and secondly the short term goals (for the next 12 months) and the necessary steps to be taken towards the achievement of the defined long term goals.

1.2 Procedures and Next Steps

The process to write and review the RPs and the CDPs was conducted as follows:

Internal Guidelines for the Career Development Plans and Research Project Plans were released in month 6 of the project providing a common document on quality criteria for the production of CDPs and RPs of the fellows.

All ESRs initially created their RPs and CDPs under the guidance of their supervisors and submitted them to the project's subversion (svn) server by 15th May 2017, i.e. more than 2 weeks prior to the network-wide 2nd training event, held in Vienna, 30th May – 2nd June 2017. At this 2nd training event, each ESR gave a presentation explaining the RP to an examination committee consisting of their supervisors and secondment hosts and to all network members. First, the examination committee members and then the entire auditorium questioned and discussed the research settings, the worded research questions, and the proposed methods with which to answer them.

With the aforementioned feedback, the ESRs revised the submitted RPs and CDPs, again upon consultation with their supervisors and co-supervisors by mid June 2017.

Finally, the re-submitted RPs and CDPs were united, to create present compendium.

The CDP will be followed up in the second year and will also describe any potential deviations from the initial plans and the analysis of the potential risks and their impact should be described as a measure for detecting and addressing any potential risks.

1.3 Document Structure

The remainder of this document includes in Chapter 2 all Research Proposals and Individual Career Development Plans of the ESRs of the Network except for the Plans of ESR3, who has been on parental leave.

In an appendix at the end of the document, a description of the structure and content of the RPs and CDPs as well as a template for the CDP to be submitted in year 1 of the project are given.

Usable Transparency

Patrick Murmann (ESR01), Karlstad University (KAU)

Abstract. This document provides a summary of the research the author intends to conduct in the course of his three year scholarship as an early stage researcher (ESR) of Privacy&Us [Age15], a project funded by the European Union's Horizon 2020 research and innovation programme within the Marie Skłodowska-Curie Innovative Training Networks (ITN-ETN) framework. The document is based on recommendations provided in the *Guidelines for Career Development Plans* of this project [SRH16], and aims to describe the overall procedure and individual steps planned for the ESR's studies during the 36 months of the project. The planning is conducted with the goal of working towards the ESR's PhD thesis, which the ESR plans to defend at the end of his 48 month study period.[1] The intended outcome of these studies is to provide academia with a better understanding about the aspects involved in making privacy for users of information systems more transparent. At the end of his studies, the ESR hopes to contribute to science by presenting a set of design principles that demonstrably lead to the implementation of usable transparency enhancing tools.

[1] The study period of 48 months for doctoral students is a local regulation of Karlstad University. The ESR's study period is therefore extended by an 12 additional months after the end of Privacy&Us.

Terminology

Table 1 provides a list of terms and abbreviations used throughout this document.

Term	Description
DC	Data controller (GDPR, Chap. IV, Art. 24 et seq.)
DP	Data processor (GDPR, Chap. IV, Art. 24 et seq.)
DS	Data subject
ESR	Early stage researcher [Age15]
GDPR	General Data Protection Regulation [Eur16]
ISO	International Standards Organization
Personal data	Refers to personally identifiable information
PET	Privacy enhancing technology
Privacy	Refers to the term 'information privacy' or 'data privacy' as discussed by [vdHBPW16]
RQi	Research question number i
TET	Transparency enhancing technology/tool
Transparency	The principle as stipulated in GDPR, Chap. III, Art. 12 et seq.
Usability	Refers to the definition of usability in ISO 9241 [Int98]
User	Refers to the individual that uses a TET. That person may be the data subject whose data is being reviewed, or a legal representative or guardian
UI	User interface
ULD	Unabhängiges Landeszentrum für Datenschutz [Age15]
USE	USECON – The Usability Consultants GmbH [Age15]
WU	Wirtschaftsuniversität Wien [Age15]

Table 1: Terms and abbreviations used throughout this document.

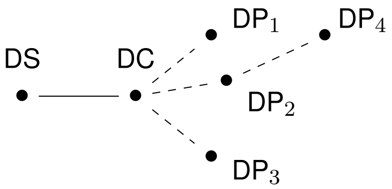


Figure 1: Relationship between a data subject (DS), a data controller (DC), and potentially several downstream data processors (DP). Dashed lines signify the retransmission of personal data to downstream processors.

1 Introduction

The preliminary working title of the ESR's PhD-thesis can be broken down into the terms 'usability' (the nominalised form of the adjective 'usable') and 'transparency.' In the context of this document, usability refers to the definition of ISO 9241 as the "extend to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use" [Int98]. Conversely, the term 'transparency' refers to transparency with regard to privacy in the context of information technology [vdHBPW16]. As such, transparency reflects the right of data subjects to receive meaningful insight about how and by whom their personal data are stored and processed, as well as what consequences arise for data subjects due to their personal data being disclosed. This right is not optional, nor can the lack of the implementation of respective functionality be written off to the complex interplay of multiple stakeholders [Art12]. Rather, transparency represents a legal right stipulated by the data protection law of the European Union in the General Data Protection Regulation (GDPR, Chap. III, Art. 12 et seq.) [Eur16].

Meaningful transparency for data subjects is particularly difficult to achieve if multiple stakeholders, such as a data controller as well as multiple downstream processors, are involved in processing their personal data (figure 1). Moreover, the vast amount of personal data collected by data controllers about data subjects may be either too large or too complex to be visualised in a way that is comprehensible by a layperson. In such cases, providing data subjects with meaningful insight about their personal data might turn out to be a challenge. [Art12] classifies respective shortcomings as a potential data protection risk in the context of cloud computing.

Transparency enhancing tools (TETs) enable data subjects to gain insight into which personal data they share with data controllers and downstream processors along the cloud chain. Whereas privacy enhancing technologies (PETs) have been researched since the beginning of the 1980s, the systematic research of TETs spans roughly a decade. More specifically, the rigorous analysis of the design of usable ex post-TETs is an area that has not sufficiently been dealt with in academia. In this context, the ESR plans to address the following research questions:

1. What kind of usable TETs exist in scientific literature?
   a) What are the characteristics of these TETs?
   b) How can TETs be classified according to these characteristics?

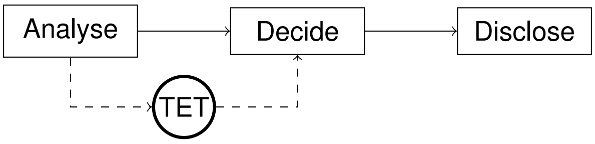


Figure 2: Sequential steps involved in an ex ante decision making process. Solid lines signify transitions between states. Dashed lines signify transitions supported by a TET.

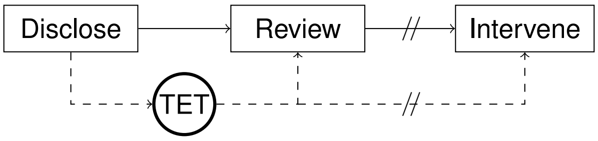


Figure 3: Sequential steps involved in an ex post review process. Intervention is not supported by all TETs.

c) What are the gaps of these TETs?

2. What are the expectations of users regarding TETs in terms of scope, granularity, and functionality?

3. Which principles are required to design TETs that are demonstrably usable by users?

2 Background

Transparency enhancing tools (TETs) come in two distinctive variants. *Ex ante* TETs display to users of data services by whom and how their personal data *will be processed before* they disclose any data to these parties (figure 2). The objective of ex ante TETs is to visualise the consequences of decisions made by data subjects in terms of their personal data being processed and stored by various stakeholders along the processing chain. Conversely, *ex post* TETs visualise which entities process personal data that *have been disclosed.* The objective of ex post TETs is to indicate how and by whom these data are currently being stored and processed (figure 3). Moreover, some ex post TETs enable users to exercise their legal right to rectify or erase their data from individual data processors [Eur95, Eur16], providing them with a means of intervening the processes that have been set in motion in the past.

The ESR's research addresses the challenges that arise as regards the user interfaces (UIs) of ex ante and ex post TETs, the latter currently being the focus. The challenges he expects to address in his research include, but are not limited to determining the proper granularity required to convey meaningful information to the user of a TET, as well as finding suitable techniques to allow for UIs that are usable [Int98].

As far as ex ante TETs are concerned, their ultimate purpose is to enable users to make informed decisions when disclosing personal data, while ex post TETs enable users to review and control such data once they have been disclosed. Designing UIs for both kinds of TETs depends on multiple factors, the most prominent being the target users' personal background,

Year	Authors	Title (abbreviated)
2007	Hsieh, Tang, Low, et al. [HTLH07]	Field deployment of IMBuddy...
2008	Abdullah, Conti, Beyah [ACB08]	A Visualization Framework...
2008	Kelley, Drielsma, et al. [KHDSC08]	User-controllable Learning...
2009	Kolter, Kernchen, Pernul [KKP09]	Collaborative Privacy...
2009	Sadeh, Hong, Cranor, et al. [SHC+09]	Understanding and capturing...
2009	Tsai, Kelley, Drielsma, et al. [TKD+09]	The impact of feedback...
2010	Kolter, Netter, Pernul [KNP10]	Visualizing Past Personal Data...
2010	Toch, Cranshaw, et al. [TCD+10]	Empirical models of privacy...
2011	Schlegel, Kapadia, Lee [SKL11]	Eying Your Exposure...
2012	Trabelsi, Sendor [TS12]	Sticky policies for data control...
2012	Kani-Zabihi, Helmhout [KZH12]	Increasing Service Users'...
2013	Balebako, Jung, Lu, et al. [BJL+13]	Little Brothers Watching You...
2013	Bilogrevic, Huguenin, et al. [BHA+13]	Adaptive Information-sharing...
2013	Louw, von Solms [LvS13]	Personally Identifiable...
2013	Biswas, Aad, Perrucci [BAP13]	Privacy Panel...
2013	Zavou, Pappas, Kemerlis [ZPK+13]	Cloudopsy: An autopsy...
2014	Mun, Kim, Shilton, et al. [MKS+14]	PDVLoc...
2015	Xu, Zhu [XZ15]	SemaDroid...
2015	Pistoia, Tripp, Centonze, et al. [PTCL15]	Labyrinth...
2016	Bier, Kühne, Beyerer [BKB16]	PrivacyInsight...
2016	Popescu, Hildebrandt, et al. [PHB+16]	Increasing Transparency...
2016	Fischer-Hübner, Angulo, et al. [FHAKP16]	Transparency, Privacy and Trust...
2016	Riederer, Echickson, et al. [REHC16]	FindYou...

Table 2: Result set of the literature review.

previous knowledge, and preferences. Consequently, the design of suitable UIs will have to take into account the requirements of specific target groups of users. However, the design also depends on technical and legal aspects, and has to deal with conflicting interests of different stakeholders.

3 State of the art

The state of the art of usable TETs was elicited by a literature review that was conducted during the project months M09–M13. The systematic literature review abided by methodologies recommended by experts of the field [KB13, WW02]. It relied on clearly specified criteria to demarcate the scope of the review: It exclusively covered usable implementations of ex post-TETs published as scientific papers.

During a first stage of the information retrieval process, several databases were queried using search terms that were chosen, tested, and refined in continuous discussion with the ESR's supervisor, colleagues, and the subject librarian of Karlstad University.

The process yielded more than 800 unique papers, 12 of which passed the screening process according to the specified criteria. During the subsequent 'snowballing' phase, the references of the relevant articles were traced forwardly and backwardly, yielding another eleven papers that met the screening criteria out of more than 300 retrieved publications.

The information retrieval process was meant to be systematic but not exhaustive. It was not exhaustive in that it started out with a limited set of databases and search terms, and in that it traced the references only up to one generation of publications backwardly and forwardly. It was systematic in that it followed a rigorous methodology, and in that the screening of the retrieved publications was conducted according to strict well-defined criteria.

In order to address RQ1b, the final set of 23 publications (listed in table 2), all of which discuss usable implementations of ex post TETs, were analysed for recognisable patterns and common characteristics, such as the usage context, target group, processing entity, hosting platform, nature of predication, specificity of the personal being reviewed, representation, intervenability on part of the user, and whether user studies had been conducted to underpin the usability of the TETs. Addressing RQ1c, the resulting taxonomy then served as a basis for classifying the TETs discussed in all 23 articles. The findings of the classification are currently being formalised in form of a survey whose publication is pending. The survey also addresses similarities to and differences from related work that surveys existing implementations and literature, respectively [Hed09, JWV13].

At this stage, it has become obvious that the number of publications covering ex ante-TETs exceeds by far the number of ex post-TETs, motivating further research in the latter area. Most ex post-TETs were designed for highly specific usage contexts, and only few consider the concept of intervenability on part of data subjects. In general, the maturity of the TETs varied greatly, and the ones that leant towards large-scale infrastructures hosted by third parties [LvS13, PTCL15, TS12, ZPK$^+$13] were often not discussed in terms of actual usability.

Some reviewed TETs allow users to customise their privacy settings in terms of deciding which party has access to their data. In this respect, they are suitable for individualisation as regards the users' preferences [Int06]. However, TETs that make judgmental statements about the users' personal data do so without the user knowing the exact criteria of this judgement. Moreover, such TETs do not enable users to set their own preferences as regards individual thresholds for such statements. Some TETs lack a combination of multi-layered, multi-perspective forms of visualisation that provide general as well as detailed information about disclosed personal data. In such cases, the suitability for learning [Int06] does not seem to be satisfied. Considering such aspects might not only enable users with different levels of knowledge, but also different roles and backgrounds to more meaningfully review their disclosed personal data.

It is also apparent that out of 23 reviewed TETs only about half of the papers consequently address the aspect of usability of their respective implementation, including a requirement analysis based on the expectations of the intended target audience, a stringent user-centered design process, followed by a user study of the implemented prototype to scrutinise and validate the result of the design process. The ESR's studies are therefore directed towards bridging these gaps by systematically assessing the principles necessary to design an usable TET.

Based on the definitions of ISO for usability and the statutory guidelines for transparency stipulated in the GDPR, the ESR is currently working on compiling and codifying a list of usability and transparency characteristics. This list will serve as a normative basis used to scrutinise each of the reviewed TETs, yielding objective statements as to whether the respective criterion is met. Such comparison will allow for an evaluation that is not only reproducible, but also based on well-known design and legal principles, respectively.

4 Proposed approach

In order to bridge the gaps determined during the classification of existing TETs, the ESR plans to design an ex post-TET that is demonstrably usable by the intended target audience. The ESR hopes to achieve demonstrable usability not only by working towards the expectations of that audience, but also by successfully evaluating the usability of the implemented TET via user studies. The ESR plans on implementing a series of TETs, each iteration picking up from the insight gained from the design and evaluation of its predecessor.

The target audience of the TET is defined by laypersons without domain knowledge in the disciplines of data security or information privacy. The elicitation of the design requirements will specifically focus on the expectations and experience of this interest group. Satisfying the needs of experts, such as professional auditors of personal data, will be optional and not the primary focus of the design.

The purpose of the implemented TET will be to enable its users to review and rectify the personal data they have disclosed to data service providers. To that end, users will be able to categorise and query the personal data that have been collected on them according to their own preferences, making customisation and individualisation of the UI of the TET an important design goal. The TET will thus contribute to making transparent what kind of personal data are stored and processed by whom, and providing data subjects with a means of control and intervention as regards the management of their disclosed personal data.

5 Research methodology

The purpose of the literature review was to provide the ESR with a better understanding of the status quo of available TETs, and to enable him to clearly demarcate his future work from existing related work. The subsequent survey served the purpose of analysing the characteristics and gaps of these TETs, and to present them in form of a structured classification scheme that allows for mapping characteristics to publications, and vice versa.

These findings will allow for designing a series of TET-prototypes that fill the indicated gaps and that thus demarcate themselves from existing solutions. Analysing the expectations and demands of the intended target audience, the usage context of a TET prototype will be specified during an analysis phase. Respective findings will lend themselves to the specification of the necessary requirements needed to satisfy the analysed design goals. Based on the specification of the elicited requirements, a series of prototypes will be designed and implemented. The subsequent evaluation of these prototypes will validate the actual usability of the implemented TETs by the representatives of the target audience.

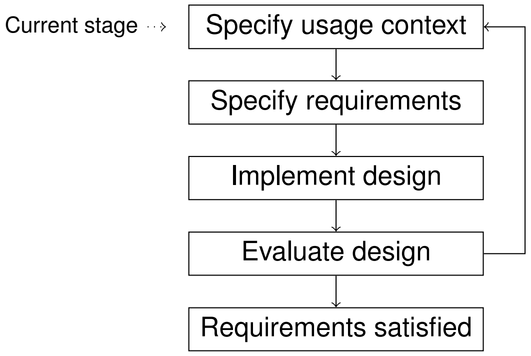


Figure 4: Course of activities in the context of human-centered design according to ISO 9241-210:2010 [Int10].

The development life cycle (figure 4) is based on the recommendations for *Human-centered design processes for interactive system* by ISO 9241-210:2010 [Int10]. The design cycle will be reiterated until the designed prototype meets the requirements specified a priori. At that point, the concluding evaluation will have proved the validity of the analysed goals and yield design principles that lead to the design of a usable TET. The elicitation of these principles based on human-centered design will form the major background for the ESR's thesis throughout his studies.

The ESR is currently evaluating the area of e-health as a possible usage context for the design and subsequent evaluation of a prototypical implementation. In order to specify the requirements for the design, the ESR conducted interviews with representatives of the intended target audience to elicit their expectations of a usable TET. The interview questions specifically built upon the gaps detected during the classification of existing TETs (RQ1c). The ESR hopes to use the expectations of the interviewees to infer requirements for the design of the prototype, thereby addressing RQ2. The prototype will be evaluated as to whether it is usable by the target audience. It may undergo several iterations of refined usage contexts and system requirements before it is finally considered to be usable in the context it was specified for. The requirements and specifications that lead to the design of a usable TET will thereupon serve as the principles that answer RQ3.

6 Work plan

The ESR's work plan relies on personal time management on two levels: Firstly, the macrostructure of the ESR's work is tightly linked to the schedule of the Privacy&Us-project. This schedule is based on the three-year plan of the project, covering the project months M09–M44. It relates to taking part in the secondments at partner institutions, the training events in Karlstad, Vienna, and Tel Aviv, as well as the participation in deliverables for work packages 4 and 5, respectively. It also relates to cooperation with other ESRs and members of the project whose work depend on or provide input for the author's own studies.

Secondly, the microstructure of the plan relates to planning, designing, implementing, and evaluating the actual tasks required to conduct the ESR's studies. During the course of the project, these tasks aim at working towards the above macrostructure, and ultimately towards the ESR's PhD thesis. On this fine-grained level, the work is primarily focused on the local competences of the respective locality, such as facilities specifically available at and provided by the project partners during the secondments. It also refers to acquiring new knowledge and practical skills provided via courses that are being offered by the ESR's home institution, project partners, or during the training events.

For both and macrostructure and microstructure, the ESR relies on the profound academic experience and domain knowledge of his supervisors whom he expects to provide him with the guidance necessary to successfully master the planning and conducting of his studies. He expects his supervisors to provide him with advise regarding how to prioritise individual facets of his work on a high level. He also relies on the advise of his supervisors when it comes to selecting journals and conferences appropriate for specific aspects of his work. The ESR hopes to maintain a continuous stream of mutual exchange by providing his supervisors with regular minutes and updates about his work.

Since the ESR's work is tightly linked to the elicitation and evaluation of design prototypes, which, in turn, depend on input provided by multiple third parties, he expects his work be greatly affected by various unpredictable factors. Such factors might include irregularities in terms of appointment management, contradictory statements in terms of preferences or ethnographic customs, and varying previous knowledge of individuals. Likewise, the ESR expects that at least two iterations of the design cycle (section 5) will be necessary to reach a state of proven usability of the design prototype during the evaluation phase.

Table 3 lists the ESR's project and research plan covering the project months M09–M44, which cover the time period August 2016 to July 2019.

Acknowledgement

The project leading to these studies has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675730 [Age15].

Month	Activity
M09	Elicit methodology, databases, search terms for the imminent literature review.
M10–M13	Conduct literature review on ex post-TETs.
M14	Write technical report about the procedure and results of the literature review.
M15–M16	Write a survey elaborating on the characteristics detected in the reviewed TETs.
M17–M18	[USE] Conduct interviews about user perception on data privacy and user expectations regarding TETs. Contribute to deliverable 4.1.
M19	Transcribe and codify the conducted interviews.
M20	Analyse and structure the findings gained via the interviews and publish them at the IFIP-Summer School.
M21	Elicit concrete requirements for the design of a usable TET in the context of e-health.
M22	Design the initial prototype of a useable TET.
M23	Prepare a user study on the comprehensibility and usability of the first iteration of the designed TET.
M24	Conduct the initial user study/usability test.
M25	Publish the results of the user studies.
M26	Contribute to deliverable 5.2.
M27–M29	[WU] Assess the projects pursued by the researchers of WU and relate them to the ESR's own work.
M30–M31	[WU] Work towards a joint publication of KAU and WU in the area of TETs, privacy perception, and transparency.
M32	Joint publication with researchers of WU.
M33	Integrate the results gained from the cooperation with WU in the design of the 2nd prototype.
M34	Conduct a user study on the usability of the 2nd iteration.
M35	Prepare for PhD-licentiate.
M36	Prepare for and conduct the PhD-licentiate at KAU.
M37	Focus on the study of the legal requirements of the designed prototype.
M38–M39	[ULD] Discuss and study the conformity of TETs in general, and the designed TET in particular with the experts at ULD.
M40	If necessary, integrate the results gained from the cooperation with ULD in the design of the 3rd prototype.
M41	If necessary, conduct a concluding user study on the final TET.
M42	Aggregate the design principles of the overall design process that lead to the creation of a usable TET.
M43	Publish the principles of usable TETs.
M44	Clean-up work and documentation for the Privacy&Us-project.

Table 3: Project plan for the project months M09–M44 / August 2017–July 2019. 'USE,' 'WU,' and 'ULD' denote time spent on secondments abroad.

List of Figures

List of Tables

References

[ACB08] K. Abdullah, G. Conti, and R. Beyah. A Visualization Framework for Self-Monitoring of Web-Based Information Disclosure. In *2008 IEEE International Conference on Communications*, pages 1700–1707, May 2008.

[Age15] Research Executive Agency. Grant Agreement – 675730 – Privacy.Us, July 2015.

[Art12] Article 29 Data Protection Working Party. Opinion 05/2012 on Cloud Computing. Technical Report 01037/12/EN, WP 196, Article 29 Data Protection Working Party, July 2012.

[BAP13] D. Biswas, I. Aad, and G. P. Perrucci. Privacy Panel: Usable and Quantifiable Mobile Privacy. In *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*, pages 218–223, Sept 2013.

[BHA$^+$13] Igor Bilogrevic, Kévin Huguenin, Berker Agir, Murtuza Jadliwala, and Jean-Pierre Hubaux. Adaptive Information-sharing for Privacy-aware Mobile Social Networks. In *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '13, pages 657–666, New York, NY, USA, 2013. ACM.

[BJL$^+$13] Rebecca Balebako, Jaeyeon Jung, Wei Lu, Lorrie Faith Cranor, and Carolyn Nguyen. "Little Brothers Watching You": Raising Awareness of Data Leaks on Smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, pages 12:1–12:11, New York, NY, USA, 2013. ACM.

[BKB16] C. Bier, K. Kühne, and J. Beyerer. PrivacyInsight: The Next Generation Privacy Dashboard. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9857 LNCS:135–152, 2016.

[Eur95] The European Parliament and the Council of the European Union. *Directive 95/46/EC of the European Parliament and of the Council*, October 1995.

[Eur16] The European Parliament and the Council of the European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council, Art 12 (8)*, April 2016.

[FHAKP16] Simone Fischer-Hübner, Julio Angulo, Farzaneh Karegar, and Tobias Pulls. Transparency, Privacy and Trust – Technology for Tracking and Controlling My Data Disclosures: Does This Work? In *IFIP International Conference on Trust Management*, pages 3–14. Springer, 2016.

[Hed09] Hans Hedbom. *A Survey on Transparency Tools for Enhancing Privacy*, pages 67–82. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[HTLH07] G. Hsieh, K. P. Tang, W. Y. Low, and J. I. Hong. Field deployment of IMBuddy: A study of privacy control and feedback mechanisms for contextual IM. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 4717 LNCS:91–108, 2007.

[Int98] International Organization for Standardization. Guidance on usability. Technical Report ISO 9241-11:1998(E), ISO, March 1998.

[Int06] International Organization for Standardization. Ergonomics of human-system interaction—Part 110: Dialogue principles. Technical Report ISO 9241-110:2006(E), ISO, April 2006.

[Int10] International Organization for Standardization. Ergonomics of human-system interaction—Part 210: Human-centered design for interactive systems. Technical Report ISO 9241-210:2010(E), ISO, March 2010.

[JWV13] M. Janic, J. P. Wijbenga, and T. Veugen. Transparency Enhancing Tools (TETs): An Overview. In *2013 Third Workshop on Socio-Technical Aspects in Security and Trust*, pages 18–25, June 2013.

[KB13] Barbara Kitchenham and Pearl Brereton. A systematic review of systematic review process research in software engineering. *Information and software technology*, 55(12):2049–2075, 2013.

[KHDSC08] Patrick Gage Kelley, Paul Hankes Drielsma, Norman Sadeh, and Lorrie Faith Cranor. User-controllable Learning of Security and Privacy Policies. In *Proceedings of the 1st ACM Workshop on Workshop on AISec*, AISec '08, pages 11–18, New York, NY, USA, 2008. ACM.

[KKP09] J. Kolter, T. Kernchen, and G. Pernul. Collaborative Privacy - A Community-Based Privacy Infrastructure. *Emerging Challenges for Security, Privacy and Trust*, 297:226–236, 2009.

[KNP10] J. Kolter, M. Netter, and G. Pernul. Visualizing Past Personal Data Disclosures. In *Availability, Reliability, and Security, 2010. ARES '10 International Conference on*, pages 131–139, Feb 2010.

[KZH12] Elahe Kani-Zabihi and Martin Helmhout. *Increasing Service Users' Privacy Awareness by Introducing On-Line Interactive Privacy Features*, pages 131–148. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.

[LvS13] Candice Louw and Sebastiaan von Solms. Personally Identifiable Information Leakage Through Online Social Networks. In *Proceedings of the South African Institute for Computer Scientists and Information Technologists Conference*, SAICSIT '13, pages 68–71, New York, NY, USA, 2013. ACM.

[MKS$^+$14] M. Y. Mun, D. H. Kim, K. Shilton, D. Estrin, M. Hansen, and R. Govindan. PDVLoc: A personal data vault for controlled location data sharing. *ACM Transactions on Sensor Networks*, 10(4), 2014.

[PHB$^+$16] A. Popescu, M. Hildebrandt, J. Breuer, L. Claeys, S. Papadopoulos, G. Petkos, T. Michalareas, D. Lund, R. Heyman, S. van der Graaf, E. Gadeski, H. Le Borgne, K. deVries, T. Kastrinogiannis, A. Kousaridas, and A. Padyab. *Increasing Transparency and Privacy for Online Social Network Users – USEMP Value Model, Scoring Framework and Legal*, pages 38–59. Springer International Publishing, Cham, 2016.

[PTCL15] M. Pistoia, O. Tripp, P. Centonze, and J. W. Ligman. Labyrinth: Visually Configurable Data-Leakage Detection in Mobile Applications. In *2015 16th IEEE International Conference on Mobile Data Management*, volume 1, pages 279–286, June 2015.

[REHC16] Christopher Riederer, Daniel Echickson, Stephanie Huang, and Augustin Chaintreau. FindYou: A Personal Location Privacy Auditing Tool. In *Proceedings of the 25th International Conference Companion on World Wide Web*, WWW '16 Companion, pages 243–246, Republic and Canton of Geneva, Switzerland, 2016. International World Wide Web Conferences Steering Committee.

[SHC$^+$09] N. Sadeh, J. Hong, L. Cranor, I. Fette, P. Kelley, M. Prabaker, and J. Rao. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing*, 13(6):401–412, 2009. cited By 121.

[SKL11] Roman Schlegel, Apu Kapadia, and Adam J. Lee. Eyeing Your Exposure: Quantifying and Controlling Information Sharing for Improved Privacy. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, SOUPS '11, pages 14:1–14:14, New York, NY, USA, 2011. ACM.

[SRH16] Jetzabel Sema, Kai Rannenberg, and Majid Hatamian. Guidelines for Career Development Plans. Technical Report Version 1.0, MS7, Privacy&Us project, October 2016.

[TCD$^+$10] E. Toch, J. Cranshaw, P. H. Drielsma, J. Y. Tsai, P. G. Kelley, J. Springfield, L. Cranor, J. Hong, and N. Sadeh. Empirical models of privacy in location sharing. *Proc. of ACM UbiComp*, 2010.

[TKD$^+$09] J. Y. Tsai, P. Kelley, P. Drielsma, L. F. Cranor, J. Hong, and N. Sadeh. Who's viewed you? The impact of feedback in a mobile location-sharing application. pages 2003–2012, 2009.

[TS12] S. Trabelsi and J. Sendor. Sticky policies for data control in the cloud. In *Privacy, Security and Trust (PST), 2012 Tenth Annual International Conference on*, pages 75–80, July 2012.

[vdHBPW16] Jeroen van den Hoven, Martijn Blaauw, Wolter Pieters, and Martijn Warnier. Privacy and information technology. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Spring 2016 edition, 2016.

[WW02] Jane Webster and Richard T. Watson. Analyzing the past to prepare for the future: Writing a literature review, 2002.

[XZ15] Zhi Xu and Sencun Zhu. SemaDroid: A Privacy-Aware Sensor Management Framework for Smartphones. In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, CODASPY '15, pages 61–72, New York, NY, USA, 2015. ACM.

[ZPK$^+$13] A. Zavou, V. Pappas, V. P. Kemerlis, M. Polychronakis, G. Portokalidis, and A. D. Keromytis. Cloudopsy: An autopsy of data flows in the cloud. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8030 LNCS:366–375, 2013.

Patrick Murmann (ESR01), Karlstad University (KAU)

1 Career Development Plan Year 1

Target audience and use of this document: The Career Development Plan is intended to be a document to guide the ESR and the supervisors as and where applicable the direct superior at the hiring institution with the procurement of the Marie Curie programme. It contains a series of personal information of the ESR and should be treated as confidential. Where necessary the document may be made available to the project leader, the management board or a designated group of persons for the purposes of mediation or dispute resolution. Where necessary and specifically asked for the document may be made available to the European Commission or the reviewers appointed by the EC for purposes of the evaluation of the project and other purposes specified in the programme's funding regulations.

I. Personal and Organizational Information

ESR´s Personal Information			
Name:	**Patrick Murmann**	**ID number**:	731116-1355
Office Address:	Universitetsgatan 2, 651 88 Karlstad	**Phone**:	+46 54 700-1363
Mobile:	+46 703 986340	**E-Mail:**	patrick.murmann@kau.se

ESR´s Host Organization Information			
Name:	**Karlstad University**	**Phone**:	+46 54 700-1000
Address:	Universitetsgatan 2, 651 88 Karlstad		
***If enrolled organization is different from host organization, please specify:**			
Name:	—	**Phone:**	—
Office Address:	—		

II. Supervision

Supervision			
Supervisor´s Name:	**Simone Fischer-Hübner**	**Title**:	Prof. Dr.
Place of Employment:	Karlstad University	**Phone**:	+46 54 700-1723
Responsibility Distr.:		**E-Mail:**	simone.fischer-huebner@kau.se
Co-Supervision			
Co-Supervisor´s Name:	**Melanie Volkamer**	**Title**:	Prof. Dr.
Place of Employment:	Karlstad University / TU Darmstadt	**Phone**:	+46 54 700-1469
Responsibility Distr.:		**E-Mail:**	melanie.volkamer@kau.se
Conduct of Supervision (per activity describe form of supervision and estimated supervision hours)**:**			

Simone Fischer-Hübner: proportion of employment allotted: 7%
Melanie Volkamer: proportion of employment allotted: 3%

- Regular meetings with the student and the assistant supervisor.
- Assisting in managing the relationship with the external (tertiary) supervisor.
- Cooperative brainstorming and structuring of information as regards the student’s work.
- Review of the student’s submitted material in order to get it published.
- Assisting the student in choosing and planning his courses over the entire period of his PhD-studies.
- Providing personal advisory, e. g. by educating the student via individual training that is mandatory at the department (study course “Introduction to research studies in computer science”).
- Advising the student on conducting his literature review.
- Advising the student on getting his results published.
- Advising the student on starting a consecutive evaluation study.
- Advising the student on preparing user studies as regards the evaluation of usability and interface design of prototypes.
- Joint brainstorming meetings.
- Introduction to PhD studies at the Computer Science department.
- Assisting the student in maintaining his individual study plan (required at KAU), career development plan, and the research proposal.
- Cooperative publication of articles.
- Cooperative authoring of deliverables.

III. Secondment

ESR´s Secondment			
Supervisor’s Name:	**Michael Bechinie**	**Position**:	Head of Experience Design
Organization´s Name:	**Usecon**	**Phone**:	+43 1 7435451-402
Address:	Objekt 2, Modecenterstraße 17, 1110 Vienna	**E-mail:**	bechinie@usecon.com

IV. Research Project

ESR´s Project			
Title:	**Usable Transparency**	**Ref. No:**	ESR 1

Overview and background

Transparency is an important privacy principle. It is related to the right of individuals to be informed about how and by whom their personal data have been processed and about the logic involved, for instance, in automatic data processing, regarding algorithms, decision criteria, and sources of data. Transparency is especially difficult to provide in the context of Big Data and Cloud Computing, in which data processors may not be known at the time of data collection, the personal data may be aggregated with additional information, or the amount of data may be too vast for users to visualize and comprehend.

Transparency tools are either ex ante or ex post. The former tell users how, by whom and the methods by which data are processed before any personal data are collected. The latter tools provide means to track how, by whom and with which methods personal data are processed, after the data are collected.

Source: Grant Agreement, No. 675730 – Privacy.Us

V. Long-Term Career Objectives

Long-Term Career Objectives (over five years)

The research will address the challenges regarding user interface design of both ex ante and ex post transparency tools. The ESR plans to address the following research questions:

- What kinds of usable TETs exist, what are their characteristics, and how can the former be classified according to the latter?
- What are the expectations of average users regarding TETs in terms of scope, granularity, and functionality?
- Which principles and HCI-techniques are required to design TETs that are actually usable by average users?

Goals: Acquire in-depth knowledge about the mental models of users of PETs. Acquire in-depth knowledge about the visualisation techniques used in existing PETs. Design mock-ups and wireframes of TETs. Implement prototypes of TETs. Test and evaluate the implemented prototypes.

VI. Short-Term Career Objectives

A. Project Research Results

Project Research Results

Presented according to Privacy & Us project Plan.

Milestones	Expected Results
M13	Finish literature review.
M15	Finish technical report on methodology of the review.
M18	Finish interviews at Usecon.
	Finish literature survey.
	Finish deliverable 4.1.
M19	Finish evaluation of results gathered at Usecon.
M20	Finish paper on results for publication.

Deliverables

- **D4.1: User Interface Requirements (WP 4), due date: 2017-05-31**

Anticipated Publications

- **Survey on 'Ex post-TETs'**
- **User perception and expectation on TETs**

Anticipated Conference/Workshop Attendance & Courses/Seminar Presentations

- *Privacy&Us-Training Events (2016, 2017)*
- *IFIP Summer School 2017*

B. Training

Research and Technical Training

Courses at KAU:

- **Computer science colloquium (started, ongoing course)**
- **Introduction to research studies in computer science (passed)**
- **Review course (informally started as part of ‘individual training’)**

Secondment Plan

Usecon The Usability Consultants GmbH
Objekt 2, Modecenterstr. 17, 1110 Vienna, Austria
April 3rd – May 31st 2017.

Interdisciplinary Training

- **Philosophy and history of science (passed, certified)**
- **Information retrieval (passed, certified)**
- **Self management (Privacy.Us-course, certificate pending)**
- **PETs (remote course offered by UCL, started)**

Professional Training

- **Supervision and individual training received from the supervisors (ongoing)**
- **Computer science colloquium (ongoing)**

Other Training Activities

C. *Networking Activities*

- **Secondment in Vienna (April 2017 – May 2017).**
- **Privacy&Us-Training Events (August 2016 in Karlstad; June 2017 in Vienna).**
- **Cooperation with fellow ESRs.**
- **Cooperation with fellow students at WU.**

D. Research Management

Personal and remote supervision by the supervisors hosted at KAU/TU-Darmstadt.

E. Other activities

Other Activities (professional relevant)
Activities conducted between M09–M16: The state of the art of usable transparency in the context of privacy was elicited by a literature review that was conducted during the first 5 months of the project. The systematic literature review abided by methodologies recommended by experts of the field. It relied on clearly specified criteria to demarcate the scope of the review: It covered usable implementations of ex post-TETs. During a first stage of the information retrieval process, several databases were queried using search terms that were chosen, tested, and refined in continuous discussion with the ESR's supervisor, colleagues, and the subject librarians of Karlstad University. The process yielded more than 800 unique papers, 12 of which passed the screening process according to the specified criteria. During the subsequent 'snowballing' phase, the references of the relevant articles were traced forwardly and backwardly, yielding another 11 that met the screening criteria out of more than 300 retrieved publications. The final set of 23 publications, all of which discussed usable implementations of ex post TETs, were analysed for recognisable patterns and common characteristics. The resulting taxonomy then served as a basis for classifying all 23 articles. The findings of the classification were documented in form of a survey that addressed similarities and differences to related work. The purpose of the literature review was to provide the ESR with a better understanding of the status quo of TETs that are available today, and to enable the him to clearly demarcate any future work from related work. The subsequent survey served the purpose of analyzing the characteristics and gaps of these TETs, and to present them in form of a structured classification that allows for mapping characteristics to publications, and vice verse.

VII. Signatures

Date & Signature of fellow

Date & Signature of supervisor

2 Acknowledgement

Privacy&Us received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie Action (MSCA), grant agreement No 675730.

Agnieszka Kitkowska (ESR02), Karlstad University (KAU)

Research Proposal ESR 2: Measuring and manipulating privacy related attitudes and behaviours

This document presents the research plan for the PhD project "Measuring and manipulating privacy related attitudes and behaviours". In brief, the project aims to investigate the disparity between privacy attitudes and behaviours, recognized in the research as the privacy paradox. The project aims to develop an instrument measuring people's attitudes and behaviours about the data disclosure. The developed instrument will enable an in-depth understanding of people's privacy perceptions and it will help to identify what are the most influential factors affecting privacy decisions. The project will result in privacy indicators that educate users about the privacy, providing people with choice and enabling greater control over their data. Additionally, these indicators will inform users about their privacy rights, as defined in the EU General Data Protection Regulation. This document provides an overview of the literature and state of the art of online privacy research. Further, the document describes proposed approach and methods planned for the project. The research proposal concludes with a work plan demonstrating the project's execution over the next three years.

1.1 Introduction

This research aims to investigate decision-making process, and to analyse *privacy paradox* identified in previous research (1). The goal of this project is to understand why people's attitudes differ from their behaviour when confronted with privacy decisions. Some researchers argue that the *privacy paradox* is an effect of the complexity of the privacy decision-making, and that it is caused by the lack of technologies enabling informed choices (2). Regardless of its origin, the *privacy paradox* seem to affect people, and therefore in this research we will consider it as an existing problem. This research will aim to understand how people perceive privacy, and whether privacy indicators could improve people’s decisions. By gaining insights into the decision-making process, this project will produce privacy indicators that influence attitudes and/or behaviours, by balancing strength of the factors affecting privacy choices, such as emotions, routine/habit, and time. The *privacy paradox* is an extensively studied phenomenon; however, the previous research's results have been inconsistent, sometimes even contradictory, leaving the space for further studies.

This project aims to contribute to the current state of the art the following:

- Cross-cultural research considering diversity of users with different cultural, ethical and demographic background.
- Instrument measuring people’s privacy perceptions.
- Privacy indicators providing people with choice and informative feedback regarding decision outcomes; enabling greater control over data.
- Set of guidelines for design and display of privacy indicators enhancing risk aware and informed privacy decision making.

1.2 Background

The access to internet and increased availability of online services, such as social networks, eHealth applications, storage facilities and more, created rich ecosystem of interconnected applications. The growing number of internet users equipped with internet connected devices results in an extensive amount of information flow between cloud-based providers and third party applications. Therefore, people are often unaware of the service providers' privacy policies. This causes uncertainty and carelessness among people who no longer have control over their personal information. Additionally, the growing amount of online services and applications adds to the complexity of the interconnected structure of mobile, web and wearable applications, making difficult to understand potential risks and harms that may result from the use of applications. People are no longer able to say where their information is stored or who can access it, which results in entire or partial lack of control over personal data. Despite of the lack of control and knowledge about the interconnected systems, people adopt the newest applications and use them on a daily basis.

The European Union report shows that the modern digital environment increases peoples' concerns about data protection (3). It found that only 15% of respondents feel they have the control over personal data, and 67% of participants are concerned about the lack of control over their online information (3). The same source shows that the majority of people consider online information disclosure as an inevitable part of the modern life;

however, they are left with no choice but to trade personal information for use of online services. According to the report, almost 60% of participants think that providing personal information is a *big issue*. Similar views are reported in USA, where 93% of Americans think it is important to know who can get the information about them, and 90% find it important to control what information about them is being collected (4).

The raising privacy concerns became a subject of interest among policy makers. In Europe, digital privacy is protected by law, such as the EU Directive 95/46/EC (5), Directive 2009/136/EC (6). Additionally, the upcoming GDPR has been established and will come into force for all EU members in May 2018, imposing new rules and requirements for the personal information processing (7). The GDPR introduces extended jurisdiction, applicable beyond Europe, as long as the data subjects reside in EU. Additionally, it imposes financial sanctions for lack of compliance. Furthermore, the GDPR enhances end-users' rights, such as breach notifications, right to access, right to erasure, data portability; it requires application of the Data Protection by Design and by Default into the development process, and well defined and easily accessible consent. However, the legislative efforts to protect privacy are insufficient because of the lack of an appropriate communication of privacy issues to the end-users, who may not understand or be aware of their privacy rights.

Despite of the ongoing research within the field of online privacy, its complex and multidimensional structure requires further work to increase people's privacy awareness. This research aims to produce privacy indicators that could influence people’s decisions, enhance risk awareness, and most importantly, provide people with choice and in a result with a greater control. By the privacy indicators, we mean notifications about the online services’ privacy practices, such as consent and privacy policies. Previous studies showed that current privacy indicators are ineffective, often due to their language ambiguity (8), excessive amounts of text (9), contextual dependencies (10) (11), or inaccurate visual representations (12), (13), (14). This research aims to gain further understanding why the display of privacy indicators fail to inform the users about their rights and risks related to the data disclosure. We aim to demonstrate that to improve the communication and display of privacy information, it is necessary to gain an in-depth understanding of the privacy decision-making process by asking both users, and experts about their privacy perceptions, and examining whether these align with legislative privacy principles. We believe that this knowledge will enable creation of improved and individualized privacy indicators, strongly relying on visual representations of privacy issues and displayed at the specific time/frequency during the human-computer interaction.

1.3 State of the Art

The concept of privacy was broadly discussed by philosophers, however, there is no single and comprehensible definition of the term (15). Privacy can be viewed as *territorial* (the physical area surrounding individual), a *privacy of a person* (protection sphere preventing physical search and potential abuse), and *information privacy* (16). The latter, focused on personal data processing, is of interest to this research. Information privacy can be perceived as a value based concept or cognitive based concept. Westin defined privacy as *voluntary and temporary withdraw of a person from general society* and *the ability to determine for ourselves when, how, and to what extent information about us is communicated to others* (1967) (15). This cognitive perspective considers privacy as a state and control, while value based approach identifies privacy as a general right or commodity (17). Due to the multidimensional nature of privacy, people frequently misunderstand it and interchange it with terms such as security, confidentiality, anonymity and more.

Over the last few decades, privacy became central for researchers and policymakers dealing with information technology. While much of the research is dedicated to various methods enhancing privacy, such as data anonymization, minimization, improved encryption methods, privacy legislation and more, the end-user's privacy decisions seem to be poor and uninformed suggesting that the research needs improvement. Such improvement could be achieved by implementation of an appropriate approaches, gaining better understanding of the decision-making, incorporating methods obtained from the human-computer interaction (HCI), psychology and human ergonomics.

1.3.1 Decision-making research - economic approach

The economic approach to the investigation of the *privacy paradox* originated from rational studies of decision-making. The economics have been fundamental for researchers such as (18), (19), (20) and many others. The majority of studies using the economic approach focus on information disclosure, emphasizing its transactional nature. This concept was applied in studies about the monetary value of information protection (21), or even price tagging of different types of information (22). 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 behaviour (23). The privacy calculus was fundamental in studies related to the risk-benefit analysis (24), (25). The studies using economic approach frequently apply utility maximization expectation theory (26) and expectancy-value theory (27), (23). However, research demonstrated that economic based decision models and the cost-benefit calculus on their own could not adequately represent privacy decision-making process. It is necessary to consider other aspects, such as psychological factors in order to improve understanding of privacy decisions.

1.3.2 Psychological distortions, biases and affect heuristics

From the psychological point of view, the decision-making process is more complicated. Cognitive biases and heuristics frequently influence rational decisions (18). For example, studies demonstrated how the *optimism bias* affects risky decisions (28), (29). Users tend to perceive themselves as less vulnerable than other users, when confronted with risky choices. This frequently results in under-protected privacy behaviours. Additionally to the *optimism bias*, people seem to be overconfident about their knowledge and skills (30). This results in disclosing more data and increased risk exposure. Similarly, the *control paradox* affects people's decisions. Previous research indicated that, unexpectedly, people given greater control over their personal information were willing to disclose more than people provided with less control (10).

Additionally, research demonstrated that studies of decision-making process must consider *time* as one of the crucial factors influencing people's choices. For example, phenomenon called *hyperbolic discounting*; people tend to choose the smaller-sooner rewards over the bigger-later rewards (31). This phenomenon was applied to the privacy studies, which demonstrated its strong impact on decision-making process (32).

Similarly, affect-heuristics add to the complexity of decision-making research. In short, according to affect-heuristics, during the judgment process people look for mental shortcuts. They tend to make decisions quickly, based on affect (33). Some studies showed that the affect-heuristics influence peoples' judgments of risks and benefits, creating an inverse relationship between the two (34). This may confirm Zajonc's theory claiming that peoples' choices rely on emotions and *likes* (i.e. people buy a product because they like it) (35). Similarly, research of Epstein and Mower demonstrated that affect is fundamental for behaviour motivation, and Damasio's study showed a crucial role of feelings, resulting from peoples' mental images somatically marked with positive or negative emotions (36).

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) (37). 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 (38). Psychological studies not only demonstrated the existence of both systems but also provided evidence that Sys 1 can dominate decision-making (39), 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 (36).

1.3.3 Attitudes and behaviours: relationships and models

Various models of the relation between attitudes and behaviours were created, such as the Fishbein-Ajzen models, looking at the indirect impacts of attitudes on behaviour (40); roles of different antecedents of behaviour like previous experiences; or models considering the causal influence of attitude (affect) on behaviour (41). The past models of behaviour, such as the one proposed by Bentler and Speckart claimed a causal relationship between attitude and behaviour (42). Initially, the attitudes were considered as direct influencer on behaviour, while modern psychology recognized that this relationship is less direct (40). The modern approaches to the decision-making explain it as a matter of routinized choice. Additionally, modern research applied factors, such as emotions and stress into the models of decision-making (43). This resulted in a more complex representation of decision-making. For example, Triandis's model incorporates multiple factors influencing behaviour, such as habit, facilitating conditions and intentions (44).

1.3.4 There is no privacy paradox

As already mentioned, some studies demonstrated contradictory results about the *privacy paradox*, showing that the disparity is easy to explain (45) or it does not exists (2). For example Lutz and Strathoff reviewed privacy decisions through the societal lens, implementing Ferdinand Tönnies's duality: *Gemeinschaft* (emotional ties in communities) and *Gesellschaft* (societies holding rules originating from rational calculations) (45). According to their 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 security and privacy protection. Similarly, Wakefield (46) demonstrated that the affective side of human cognition has decisive impact on online trust and privacy, and therefore there is no disparity between attitude and behaviour. Although, these views seem to explain *privacy paradox*, we think that they are not applicable to all situations requiring privacy decisions. Perhaps people are happy to share their information to enhance social ties and ensure belonging to the community. However, accordingly to the previously mentioned reports, people are worried about the lack of control over their information and they express general concerns about the personal data processing (3) (4).

1.4 Proposed approach

This research aims to investigate people's attitudes and behaviours toward privacy in order to identify whether it is possible to create personalized or preferred privacy indicators that could influence decision-making. Therefore, we propose to begin with the investigation of privacy principles/issues recognized by people, which will be contrasted with principles defined by experts and legislation, such as the GDPR. This will allow for assessment of individual privacy requirements and enable creation of appropriate privacy indicators. Additionally, we aim to examine whether it is possible to change the way Sys 1 decides about the individual's privacy decisions by re-directing it to the analytical and reflective Sys 2.

Additionally, we will perform a series of studies focused on the affect heuristics, emphasizing their role in the decision-making process. The concepts obtained from the psychological research, such as Finucane et al. *affect heuristics and risk and benefits calculation* (34) and Loewenstein's *risk as feelings* (47) may be applied. This will enable research to concentrate on cognitive processes accompanying HCI, in the manner similar to Wakefield's study (46). The project will follow approaches borrowed from previous studies to investigate the role of positive and negative emotion in the judgment and choice process. Similarly to Kehr et al., we will consider issues of irrationality within the costs and benefit calculation (48), not only by analysing the emotions resulting from the HCI, but also the role of contexts. We will consider *routine/habit* in privacy decisions to see how such pre-disposition may influence the decision-maker. Additionally, we will study the role of *time,* which accordingly to some studies strongly influences people's choices. We want to investigate whether the attitude/behaviour change differ depending on the time/frequency of the indicators' display. The investigation of *time* may help to identify the most suitable approach to present people with privacy information and also demonstrate whether such displays are perceived differently on the mobile or web platform, and should they be tailored accordingly to the technology. Figure 1 presents high-level, conceptual approach for this research.

In order to ensure that we are able to investigate all mentioned aspects of the project, we will focus on interconnected applications available for both web and android phone. The consideration of cross-platform technologies will help to identify whether the same indicators could be used in the web and smartphone environment, ensuring one of the usability principles – consistency (49).

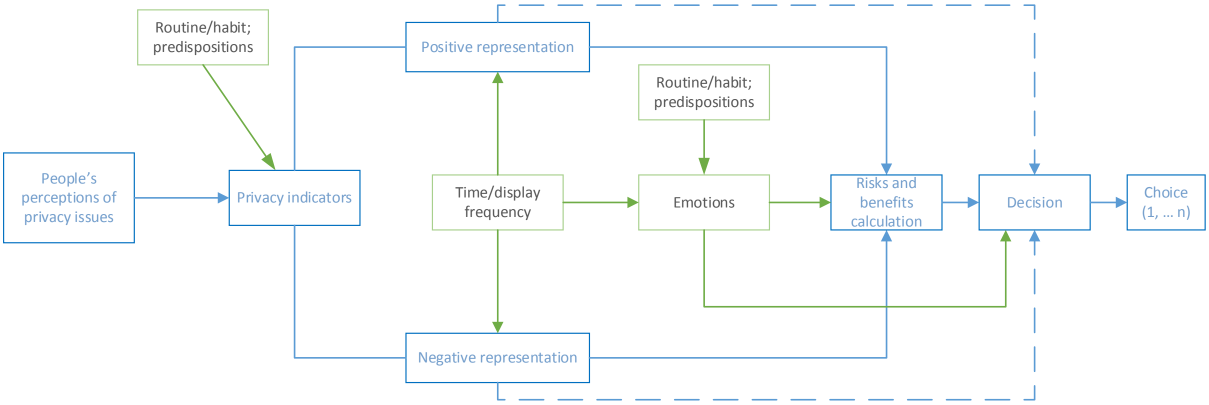

Routine/habit; predispositions
Positive representation
Routine/habit; predispositions
People's perceptions of privacy issues
Privacy indicators
Time/display frequency
Emotions
Risks and benefits calculation
Decision
Choice (1, … n)
Negative representation

Figure 1 High-level overview of the conceptual approach for this research. Due to the multiple aspects included in the proposed approach and the time constraints, it is probable that only sub-sets of this framework will be investigated.

1.5 Methodology

The research will contain qualitative and quantitative user studies analysing privacy attitudes and behaviours. As the goal is to create privacy indicators and guidelines for privacy enhancing design, the human-cantered approach will be crucial for this project. To ensure user-centrism in the project, both users' studies and UI prototypes will be preceded by PACT analysis (people, activities, contexts, technologies) (50). The overview of methods planned for this research is presented in Figure 2.

1.5.1 Quantitative methods

We plan to use online surveys/questionnaires allowing inclusion of a broad population, covering wide geographic areas, and increasing the sample's diversity. We aim to collect data representing various ethnic and cultural groups, enabling identification of potential demographic differences.

Statistical analysis

Quantitative studies will be statistically analysed. The choice of the statistical tests will depend on the study's design and goals. As the project aspires to build models of behaviour, both descriptive and exploratory models may be derived from the statistical analysis. The descriptive models will be created to summarize relations between variables without ascribing mechanics and the functional roles of the parameters. The exploratory models will be derived with use of statistical methods, such as the Exploratory Factor Analysis.

First user study

As a starting point, the project aims identify people's privacy perceptions and attitudes. We created an online survey built upon the *privacy harms* identified by Daniel Solove (51). Solove divided privacy harms into four groups:

- Information collection including *surveillance* and *interrogation*.
- Information processing including *aggregation*, *identification*, *insecurity*, *secondary use*, *exclusion*.
- Information dissemination including *breach of confidentiality*, *disclosure*, *exposure*, *increased accessibility*, *blackmail*, *appropriation*, *distortion*.
- Invasions including *intrusion* and *decisional interference*.

The categorization of *privacy harms* originates from the court cases. Because Solove's extraction was based on the real-life privacy violations, we assumed that the identified harms should be representative to how people perceive privacy issues. Therefore, following 16 *privacy harms*, we created 48 items scale to collect data about the general perceptions of online privacy issues. The first study resulted in the high volume of interval data. The parametric tests will be used to analyse the results and identify relationships between the variables, and possibly create the new index for perception of privacy issues.

1.5.2 Qualitative methods

We hope that the results of quantitative studies will form a base for a study collecting user interface requirements. Based on the identified privacy issues, we plan to perform qualitative user study aiming to identify peoples' visual representations of privacy issues. We plan to use scenario-based contextual interviews. The interviews will be transcribed and will contribute to creation of affinity diagrams and establishment of hierarchical grouping accordingly to the level of difficulties users may have. The results of qualitative studies will be used to define UI requirements and the design of the indicators.

1.5.3 Prototypes testing and experiments

Following the user-centred design, usability heuristics (49) as well as the PACT analysis, gathered UI requirements will be applied to develop privacy indicators suitable for both web and mobile platforms. The privacy indicators aim to inform users about possible risks related to the use of applications, ensuring that users understand potential harms resulting from the data collection and processing, and are fully aware of the services providers' privacy procedures. Overall, the role of indicators is to provide preferred choice, subsequently enabling control over personal data.

Ideally, the simulation of a real-like environment will be generated in order to perform the experiments evaluating privacy indicators. This will enhance testing the privacy indicators during the interaction, enabling inclusion of factors such as affect heuristics (emotions), context, and time. At this stage of the project, only a generic concept of privacy indicators exists. Presumably, they will be in the form of images (possibly icons) rather than text descriptions, reducing cognitive workload and enabling faster and intuitive recognition. The images will be associated with real-life risks indicators, such as commonly recognizable representations of hazards or harms.

From the technical point of view, due to the time constrains prototypes or mock-ups will be created with the use of existing prototyping tools, such as InVision, Moqups, Axure or similar. This will allow building a fully functional, responsive prototype with customized interaction methods. To enable precise measurements of interaction, additionally to the traditional usability methods such as observation, interviews and think-aloud exercises, this research plans to include the accessibility testing and eye tracking experiments. The experiments will provide insights into the users' attention points, choices and interaction movements.

Ethics

As the project is a part of EU H2020 'Privacy\&Us' all studies will be performed according to the requirements from EU, such as:

- Voluntary participation and informed consent. Participants will be selected from healthy and adult population. Participation in the research will be voluntary, and subject studies will be able to end it at any time. Informed consent clearly stating:
    - the identity of the data controller and which other parties will get access to data;
    - purpose of the data processing and expected duration of the usability study;
    - potential risks (if any) and benefits of participating in the study;
    - what personal data will be collected in the study, and to what degree (and how) confidentiality of such data will be ensured;
    - what kind of processing will be performed on the collected data and for how long the collected data will be retained;
    - contact persons for the study, who can answer any questions the volunteer may have;

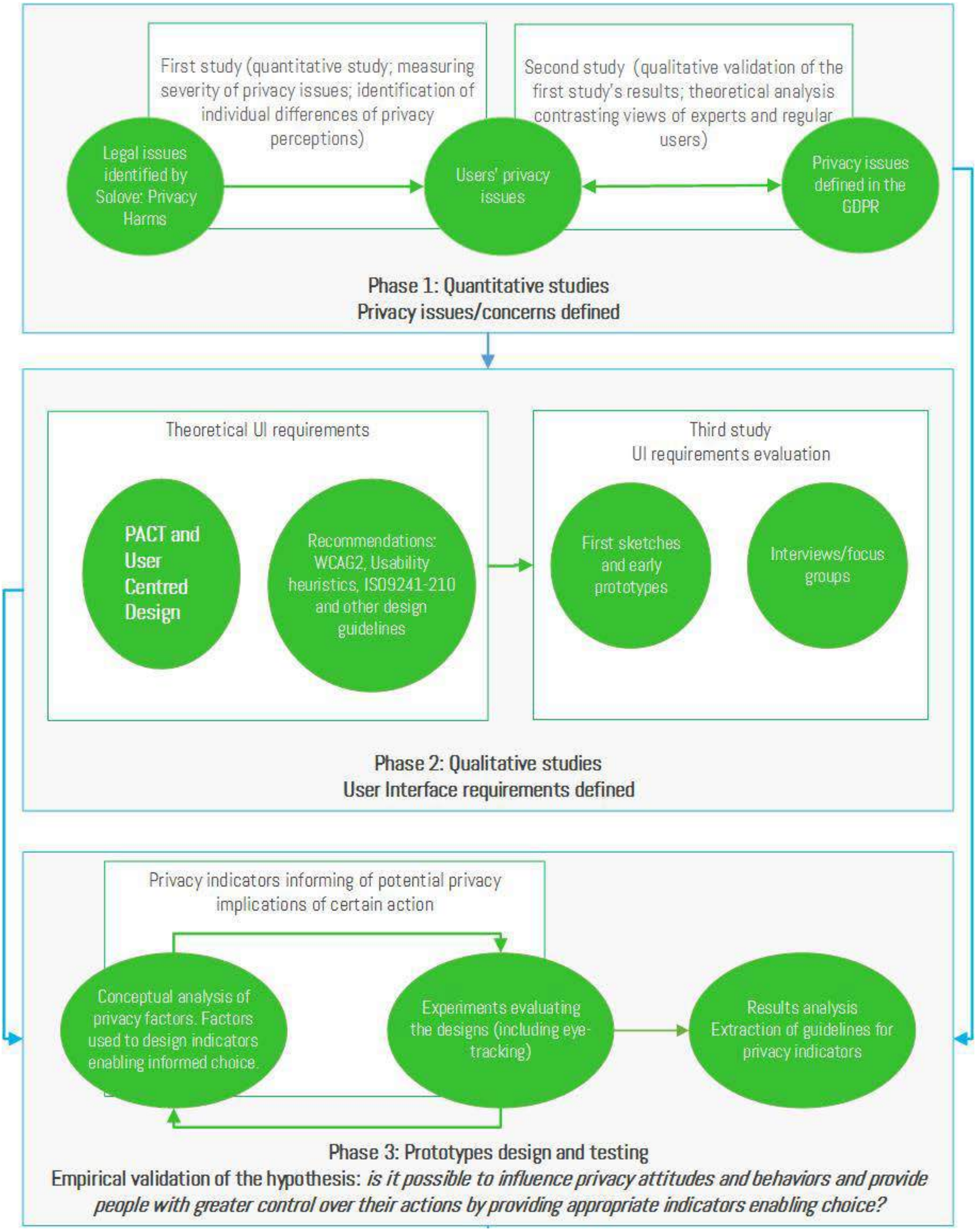

First study (quantitative study; measuring severity of privacy issues; identification of individual differences of privacy perceptions)
Second study (qualitative validation of the first study's results; theoretical analysis contrasting views of experts and regular users)
Legal issues identified by Solove: Privacy Harms
Users' privacy issues
Privacy issues defined in the GDPR
Phase 1: Quantitative studies
Privacy issues/concerns defined
Theoretical UI requirements
PACT and User Centred Design
Recommendations: WCAG2, Usability heuristics, ISO9241-210 and other design guidelines
Third study
UI requirements evaluation
First sketches and early prototypes
Interviews/focus groups
Phase 2: Qualitative studies
User Interface requirements defined
Privacy indicators informing of potential privacy implications of certain action
Conceptual analysis of privacy factors. Factors used to design indicators enabling informed choice.
Experiments evaluating the designs (including eye-tracking)
Results analysis Extraction of guidelines for privacy indicators
Phase 3: Prototypes design and testing
Empirical validation of the hypothesis: is it possible to influence privacy attitudes and behaviors and provide people with greater control over their actions by providing appropriate indicators enabling choice?

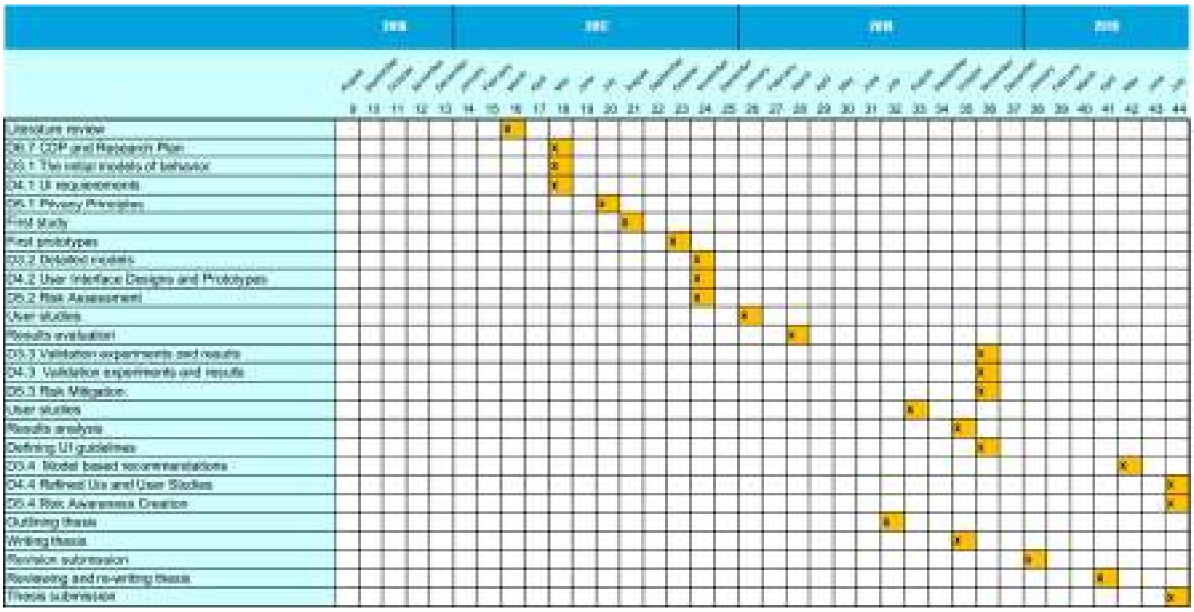
Figure 2 General overview of the methods proposed for the research.

  - contact persons for the study, who can answer any questions the volunteer may have;
  - legal rights of the test subjects to access, correct, block or delete their data;
  - the fact that participation is fully voluntary and participants can withdraw at any time.
- During the project, personal data, if obtained, will be collected, processed and protected in accordance with the Charter of Fundamental Rights of the European Union, the EU Data Protection Directive 95/46/EC, the European General Data Protection Regulation once it will be enacted , the EU ePrivacy Directive 2002/58/EC and Swedish data protection legislation.

- Any studies, which may collect personal data or potentially raise any ethical issues will be prepositioned with ethical approval request send to the Ethics Review Board at Karlstad University.

1.6 Work plan

Figure 3 presents the PhD research plan. As not all of the studies are entirely designed, there may be minor changes in the time scale. Similarly, the names of certain parts of the plan will be amended accordingly to the development of the users' studies.



	[illegible]					[illegible]												[illegible]												[illegible]						
	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
Literature review								x																												
D6.7 CDP and Research Plan										x																										
D3.1 The initial models of behavior										x																										
D4.1 UI requirements										x																										
D5.1 Privacy Principles												x																								
First study													x																							
First prototypes															x																					
D3.2 Detailed models																x																				
D4.2 User Interface Designs and Prototypes																x																				
D5.2 Risk Assessment																x																				
User studies																		x																		
Results evaluation																				x																
D3.3 Validation experiments and results																												x								
D4.3 Validation experiments and results																												x								
D5.3 Risk Mitigation																												x								
User studies																									x											
Results analysis																											x									
Defining UI guidelines																												x								
D3.4 Model based recommendations																																		x		
D4.4 Refined UIs and User Studies																																				x
D5.4 Risk Awareness Creation																																				x
Outlining thesis																								x												
Writing thesis																											x									
Revision submission																														x						
Reviewing and re-writing thesis																																	x			
Thesis submission																																				x

Figure 3 Proposed research plan including work packages' deliverables and potential schedule for studies planned for the research ("x" indicates the completion date).

2 Bibliography

1. **Brown, B.** *Studying the Internet experience. .* s.l. : HP Laboratories Technical Report HPL, 2001.
2. **Sasse, A.** There is no privacy paradox - just services and technologies that do not support users' privacy preferences. Edinburgh : This work was not published, 2015.
3. **Union, European.** *Special Eurobarometer 431 "Data Protection.".* s.l. : European Commission, 2015.
4. **Madden, M., & Rainie, L.** *Americans' attitudes about privacy, security and surveillance.* s.l. : Pew Research Center, 2015.
5. **Commission, European.** *EuroDirective 1995/46/EC on protection of individuals with regard to the processing of personal data on the free movement of such data.* s.l. : European Commission, 1995.
6. *Directive 2009/136/EC of the European Parliament and of the Council.* **Union, European Parliament & Council of the European.** 11, s.l. : Official Journal of the European Union, 2009, Vol. 337. 11-36.
7. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.* **EU.** s.l. : Official Journal of the European Union, 2016.
8. *Disagreeable privacy policies: mismatches between meaning and users' understanding.* **Reidenberg, J. R., Breaux, T. D., Cranor, L. F., French, B., Grannis, A., Graves, J. T., Schaub, F.** 1, s.l. : Berkley Technology Law Journal, 2015, Vol. 30. 39-68.
9. *Through a Glass Darkly : From Privacy Notices to Effective Transparency.* **Bruening, P. J., & Culnan, M. J.** s.l. : Nroth Carolina Journal of Law & Technology, 2015, Vol. June. 1-46.
10. *Misplaced Confidences: Privacy and the Control Paradox.* **Brandimarte, L., Acquisti, A., & Loewenstein, G.** 3, s.l. : Social Psychological and Personality Science, 2013, Vol. 4. 340-347.
11. *A Contextual Approach to Privacy Online.* **Nissenbaum, H.** 4, s.l. : Dædalus, the Journal Ofthe American Academy of Arts & Sciences, 2011, Vol. 140. 32-48.

12. *Standardizing privacy notices : an online study of the nutrition label approach. .* **Kelley, P., Cesca, L., Bresee, J., & Cranor, L.** s.l. : Human Factors in Computing Systems, 2010.
13. *"I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment.* **Steinfeld, N.** s.l. : Computers in Human Behavior, 2016, Vol. 55.
14. *A Design Space for Effective Privacy Notices.* **Schaub, F., Balebako, R., Durity, A. L., & Cranor, L. F.** Ottawa : Symposium on Usable Privacy and Security (SOUPS) 2015 , 2015.
15. **DeCew, Judith.** Privacy. *The Stanford Encyclopedia of Philosopy .* [Online] 2015. https://plato.stanford.edu/archives/spr2015/entries/privacy/.
16. *History of Privacy.* **Holvast, J.** s.l. : The Future of Identity in the Information Society, 2009.
17. *The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing .* **Xu, H., Luo, X., Carroll, J. M., & Beth Rosson, M.** s.l. : Decision Support Systems, 2011.
18. *Privacy attitudes and privacy behavior.* **Acquisti, A., & Grossklags, J.** s.l. : Economics of Information Security, 2004.
19. *The Privacy Paradox : Personal Information Disclosure Intentions versus Behaviors.* **Norberg, P. A., Horne, D. R., & Horne, D. A.** s.l. : The Journal of Consumer Affairs, 2007, Vol. 41.
20. *Unwillingness to pay for privacy: A field experiment.* **Beresford, A. R., Kübler, D., & Preibusch, S.** s.l. : Economics Letters, 2012, Vol. 117.
21. *When 25 Cents is too much : An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information.* **Grossklags, J., Hall, S., & Acquisti, A.** s.l. : Information Security, 2007, Vols. 7-8.
22. *Your browsing behavior for a big mac: Economics of personal information online.* **Carrascal, J., & Riederer, C.** s.l. : Proceedings of the WWW 2013, 2013.
23. *An Extended Privacy Calculus Model for E-Commerce Transactions.* **Dinev, T., & Hart, P.** s.l. : Information Systems Research, 2006, Vol. 17.
24. *Internet privacy concerns and their antecedents - measurement validity and a regression model.* **Dinev, T., & Hart, P.** s.l. : Behaviour & Information Technology, 2004, Vol. 23.
25. *Overcoming Online Information Privacy Concerns: An Information Processing Theory Approach.* **Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., Png, I. P. L.** s.l. : Journal of Management Information Systems, 2014.
26. *Information Privacy Research: An Interdisciplinary Review.* **Xu, H.** s.l. : MIS Quarterly, 2016, Vol. 23.
27. *Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model.* **Malhotra, N. K., Kim, S. S., & Agarwal, J.** s.l. : Information Systems Research, 2004, Vol. 15.
28. *My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns.* **Baek, Y. M., Kim, E. M., & Bae, Y.** s.l. : Computers in Human Behavior, 2014.
29. *Determinants of Behavioral Responses to Online Privacy: The Effects of Concern, Risk Beliefs, Self-Efficacy, and Communication Sources on Self-Protection Strategies.* **Cho, H.** s.l. : Journal of Information Privacy & Security, 2010.
30. *Privacy practices of Internet users: Self-reports versus observed behavior.* **Jensen, C., Potts, C., & Jensen, C.** s.l. : International Journal of Human Computer Studies, 2005.
31. *Golden Eggs and Hyperbolic Discounting.* **Laibson, D.** s.l. : The Quarterly Journal of Economics, 1997.
32. *Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. .* **Acquisti, A., & Grossklags, J.** s.l. : 2nd Annual Workshop on "Economics and Information Security", 2003.
33. **Kehr, F., Wentzel, D., Kowatsch, T., & Fleisch, E.** Rethinking Privacy Decisions: Pre-Existing Attitudes, Pre-Existing Emotional States, and a Situational Privacy Calculus. *ECIS 2015 Completed Research Papers.* 2015.
34. *The affect heuristic in judgments of risks and benefits.* **Finucane, M. L., Alhakami, A., Slovic, P., & Johnson, S. M.** s.l. : Journal of Behavioral Decision Making, 2000, Vol. 13.
35. *Feeling and Thinking. Preferences Need No Inferences.* **Zajonc, R. B.** 2, s.l. : American Psychologist, 1980, Vol. 35.
36. *The Affect Heuristic.* **Slovic, F.** s.l. : Heuristics and Biases; The Psychology of Intuitive Judgement ,Cambridge University Press, 2002.
37. **Tversky, A., Kahneman, D., Tversky, A., & Kahneman, D.** The Framing of Decisions and the Psychology of Choice. *Science.* 1981.
38. **Kahneman, D., & Frederick, S.** Representativeness revisited: Attribute substitution in intuitive judgment. *Heuristics of Intuitive Judgment: Extensions and Applications.* January 2002, 2002.

39. **Denes-Raj, V., & Epstein, S.** Conflict Between Intuitive and Rational Processing: When People Behave Against Their Better Judgment. *Journal of Personality and Social Psychology.* 1994, Vol. 66, 5.
40. **Ajzen, I., & Fishbein, M.** Attitudes and the Attitude-Behavior Relation: Reasoned and Automatic Processes. *European Review of Social Psychology.* 2000, Vol. 11, 3.
41. **Bentler, P. M., & Speckart, G.** Models of Attitude-Behavior Relations. *Psychological Review.* 1979, Vol. 86, 5.
42. **Bentler, P. M., Speckart, G.** Attitudes "cause" behaviors: a structural equation analysis. *Journal of Personality and Social Psychology.* 1981, Vol. 40, 2.
43. **Betsch, T., Haberstroh, S., & Höhle, C.** Explaining Routinized Decision Making. A Review of Theories and Models. *Theory & Psychology.* 2002, Vol. 12, 4.
44. **Cheung, W., Chang, M. K., & Lai, V. S.** Prediction of Internet and World Wide Web usage at work: A test of an extended Triandis model. *Decision Support Systems.* 2000, Vol. 30, 1.
45. **Lutz, C., & Strathoff, P.** Privacy concerns and online behavior – Not so paradoxical after all? . *Multinationale Unternehmen Und Institutionen Im Wandel – Herausforderungen Für Wirtschaft, Recht Und Gesellschaft.* 2013.
46. **Wakefield, R.** The influence of user affect in online information disclosure. *Journal of Strategic Information Systems.* 2013, Vol. 22, 2.
47. **Loewenstein, G., Hsee, C. K., Weber, E. U., & Welch, N.** Risk as Feelings. *Psychological Bulletin.* 2001, Vol. 127, 2.
48. *Rethinking the Privacy Calculus: On the Role of Dispositional Factors and Affect.* **Kehr, F., Wentzel, D., & Mayer, P.** Milan : Thirty Fourth International Conference on Information Systems, 2013.
49. **Nielsen, J.** Heuristic Evaluation. *Usability Inspection Methods.* 1994.
50. **Benyon, D.** *Designing interactive systems A comprehensive guide to HCI and interaction design.* s.l. : Citeseer, 2010.
51. *A taxonomy of privacy.* **Solove, D.** s.l. : University of Pennsylvania Law Review, 2006, Vol. 477.
52. *Privacy by Design Resolution.* **Cavoukian, A.** Jerusalem : 32nd International Conference of Data Protection and Privacy Commissioners, 2010.

Agnieszka Kitkowska (ESR02), Karlstad University (KAU)

Career Development Plan ESR 2

Personal and Organizational Information ESR:

ESR
Agnieszka Kitkowska
Phone: +46 54 700 2402
agnieszka.kitkowska@kau.se

Hosting institution:

Karlstad University (KAU)
Universitetsgatan 2
651 88, Karlstad, Sweden

Supervisors
Docent Leonardo Martucci (KAU)
-technical supervisor advising on work progress

Phone: +46 54 700 1153
leanardo.martucci@kau.se

Docent Erik Wästlund (KAU)
-responsible for advice regarding user studies, design and evaluation

Phone: +46 54 700 2528
erik.wastlund@kau.se

Conduct of supervision: When possible, supervision is conducted in the form of regular, bi-weekly meetings. Additionally, constant communication between supervisors and ESR is kept over the email and informal meetings. The approximate time dedicated to the meetings is 60 hours per 12 months.

First secondment
Supervisor:

Prof Joachim Meyer
Tel Aviv University (TAU)
Carter Building, Ramat Aviv 6997801, Israel
Phone: 03-6405994
jmeyer@tau.ac.il

Research project No 2: Measuring and manipulating privacy related attitudes and behaviours.

Privacy in the digital systems appears to be ineffective in terms of its usability. Despite existing data protection rights and regulations, end users are frequently unaware of the risks related to data collection. Control of data becomes cumbersome due to increasing amounts of data, the number of internet users, and diversity of devices and applications. Due to the lack of control and understanding of data collection processes users make uninformed decisions. In effect, they place themselves and their acquaintances at risks, such as identity theft, physical and mental harms, surveillance, distortion and many more.

Complex and multidimensional structure of digital privacy and privacy related decision-making attracted the interest of investigators and researchers from various fields including governments, lawmakers, social sciences, psychology, as well as computer science. The privacy research often concentrates on privacy policies and visual notifications communicating information necessary for informed decision-making. Some studies demonstrated that users disregard these indicators. Among the main concerns associated with reception of privacy messages and policies are language ambiguities, length, contextual dependencies, development methods, and display.

In order to improve privacy indicators it is necessary to gain an in depth knowledge and understanding of decision-making processes. Existing privacy decision-making studies resulted in identification of privacy paradox phenomena, where users' attitude toward privacy varies from their behaviour. Thus, important revelation became a subject of multiple studies that frequently focus on one individual problem within the decision-making process, such as one type of information disclosure or one type of privacy concern. In effect, privacy paradox research results in unclear and undefined causes of the attitude-behaviour gap.

The main goal of this research is to investigate privacy decision-making process, stressing identification of factors affecting attitudes and behaviours, such as emotion, context and time. The series of studies planned for the project aim to clarify whether the attitude-behaviour gap identified in previous research exists and how to diminish it. In order to achieve it, this research will produce empirical models of behaviour and decision-making. The research will focus on determination, which contextual factors (such affect heuristics or others) have the strongest, if any, influence privacy attitude and behaviour. The project aims to analyse whether privacy decisions are solely a result of behavioural economics, such as costs and benefit calculus, or whether emotions and affection impact human judgment process over rationale.

Based on existing research and this project's findings we will produce the new privacy indicators, accordingly to the best practices of usability and accessibility. They will be tested and evaluated qualitatively and quantitatively. We will try to determine whether the indicators can change the decision-making process, increase risk awareness, and provide people with choice and control.

This research hopes to have an impact beyond the academia by extraction of the privacy indicators design guidelines, and best practices for designers, and developers. The guidelines intend to integrate usability, accessibility and legal compliance. In a greater spectrum, this research's goal is to influence people and enable informed privacy decisions reducing risks and harms associated with online activities.

Long-Term Career Objectives (over five years)
As this is an early stage of the project, the long-term objectives are not entirely defined. However, the current preference is to continue researching privacy and usability with an emphasis on the accessibility.
Currently, the researcher's desire is to return to work within the industry. This would allow for implementation of methods and skills gained at academia into the real-life research and enhance academia-industry knowledge exchange. Despite the desire to work in industry, it will be preferred to engage academic sector into the future projects enabling hands-on experience for students and researchers.

The researcher is open to continue the career at academia. However, due to the lack of teaching experience and appropriate skills, at this stage only managerial positions are considered.

Short-term objectives
Project research results

- Research Plan and CDP - Clear identification of project goals, research approach and methodology.
- First quantitative study - Initial model of behaviour; Index of people's privacy perceptions; Publication of the results in a journal or conference presentation.
- User Interface requirements and mock-ups - First designs of the privacy indicators.

Project deliverables

- WP3 Models of Behaviour - D3.1 The Initial Models (month 18)
  - The report including the relevant models and specifying initial modelling approach. This approach will be used to create the models built accordingly to the results of the first study.
- WP4 Interaction Design - D4.1 User Interface Requirements (month 18)
  - The report presenting user interface requirements for the project. Identification of the high-level user interface requirements based on usability best practices, such as Norman, Nielsen and Shneiderman and on the academic research on online privacy.
- WP5 Risk Analysis, Risk Perception and Law - D5.1 Privacy Principles (month 20)
  - The report clarifying privacy targets for the cloud ecosystem of applications. This will enable better understanding of possible harms resulting from using the interconnected applications. The analysis of legal requirements and users rights will be beneficial for creation of user studies.

Anticipated publications

- SOUPS 2017 – poster for People's perceptions and attitudes towards privacy (working title) (submission deadline 29th May 2017)
- CHI 2018 (Montreal, April 21-26)– full paper about People's perceptions and attitudes towards privacy (working title) (submissions deadline 19th September 2017)

Anticipated Conference/Workshop Attendance & Courses/Seminar Presentations

- IFIP Privacy and Identity Management Summer School 2016 (Karlstad, Sweden 21—26 August 2016)
- NordiCHI 2016 (Gothenburg, Sweden, 23-27 October 2016)
- Privacy by Design Workshop (Haifa & Yehud, Israel 25-26 April 2017)

- SOUPS 2017 (Santa Clara, CA, USA, 12-1 July 2017 – participation dependant on the poster submission)
- IFIP Summer School on Privacy and Identity Management (Ispra, Italy, 4-8 September 2017)

Training

a. Research and Technical Training – none
b. Interdisciplinary training
   - A global view of legal aspects of privacy and information privacy (Privacy&Us 1st Training)
   - Privacy in eHealth (Privacy&Us 1st Training)
c. Professional Training
   - Scientific paper writing & publication process (Privacy&Us 1st Training) 4 ECTS (included in the Privacy&Us 1st Training awarded points)
   - Networking: how to create and maintain contacts at conferences and scientific organizations (Privacy&Us 1st Training)
d. Other training activities:
   - Philosophy and History of scientific Thought (KAU) 7.5 ETCS
   - Computer Security I & II (KAU) 8 ECTS
   - Empirical Research Methods for Human Computer Interaction (NordiChi tutorial) – no points
   - Visual research dissemination (NordiChi tutorial) – no points

Networking activities

- IFIP Summerschool 2016 and Privacy&Us frist training event in Karlstad University
- NordiCHI 2016 in Goteborg
- Privacy by Design Workshop 2016 at Haifa University and HP Headquarters in Yehud, Israel
- Big Data and Education: Ethical and Moral Challenges 2017, Haifa University
- Privacy&Us Second Training, Vienna, May 2017
- SOUPS2017

Other activities

- Participation in online courses about research methods, statistics and probability models offered by free learning platforms such as Coursera and EdX.
- Participation in licentiate and docent defences.

Secondment plan

The focus of the project is measuring and manipulating privacy attitudes and behaviours. Precisely, it concentrates on privacy paradox phenomenon. In short, the privacy paradox can be described as the dichotomy between people's attitudes and behaviours during their exposure to privacy-related decisions. Therefore, this project considers examination of decision-making processes, risks and identification of factors influencing people's judgments and choices. The in-depth analysis of the role of affect heuristics and psychological biases is planned for the project to recognize whether they can be implemented on the user interface design as factors triggering change and shaping people's behaviours.

The project is still at the early stage. However, the first qualitative study has been designed and its results will be available for the analysis in the near future. Thus may affect the activities during the secondment. Additionally, the secondment interferes with Privacy&Us second training event taking place in Vienna (29th May - 2nd June), therefore one week of secondment will be dedicated to traveling and participation in the aforementioned event.

- Overview of the Privacy perceptions study

The online questionnaire has been developed to assess peoples' perceptions and concerns about privacy. The study designed was based on privacy harms identified by Daniel Solove. Additionally, the survey incorporated previously developed scales for privacy protection behaviours, information disclosure and Westin's index. The study desires to identify the way people think of privacy, investigate any correlations between variables, and explore demographics such as age, education, geographical location (the study was distributed throughout 5 regions: UK, USA, Germany, Italy and Nordic countries).

- Writing publication

The desire of the first study was to collect material for publication. Therefore, it is probable that during the secondment ESR will work on the publishable analysis of the results.

- Models of behaviour

Overview of the state-of-art within the field of models of behaviour. Discussion of the modelling approach proposed in the D3.1. The ESR hopes to learn opinions of experts regarding behaviour models and gain knowledge about the best practices for creation and evaluation of both conceptual and mathematical models of privacy decision making.

- Additional activities
    - Participation in Privacy by Design Workshop 25-26 April
    - Preparation of research plan and presentation
    - The second Privacy&Us event requires each ESR to prepare the research plan and present it during the event.
    - Familiarizing with the Tel Aviv university research group.
    - Taking the opportunity of discovering current projects running at the University and methods applied in the research. Establishing new contacts and possibilities for future collaboration.
    - Preparing poster for the SOUPS2017.

Poornigha Santhana Kumar (ESR04), Usecon (USE)

Designing for Privacy & Security at Point of Sale Commercial Transactions

Aim

This PhD thesis aims to deliver a secured and privacy enhanced experience [1] for users at point of sale commercial transactions. We focus on Near Field Communication (NFC) payments as it is emergent technology and as forecasted by some authors [3] [2] NFC payments are commonly used in retail shops now-a-days. We also choose to work on retail shop checkouts as it involves wide range of customers (age, gender and profession) and accepts all types of payment (cash, credit/debit card, NFC in cards and mobile phones).

State-of-art

NFC

As mentioned above NFC is an emergent technology and it is currently being used for contactless payments in some countries [4].The user can pay by holding either their NFC card or NFC enabled mobile phone against the payment terminal. If the distance between the payment terminal and NFC card / NFC mobile is less than 4 cm a connection is establishes and payment is proceeded [5].

We have a rich literature which portrays that researches is being conducted on NFC's in various directions. To begin with, the advantages and possibilities of NFC technology has been well explored [5]. The main advantage pointed by various studies [5] [6] [7] states that NFC payment is faster than other payment methods (credit/debit card and cash payment) and reduce the hassles faced by the user. NFC payment also over comes shoulder surfing attack as the user need not input their PIN (Personal Identification Number) for purchases less than 25 euro. Given the above advantages, NFC payment seem to serve as a perfect alternative for existing payment methods. But there exists few others factors which obstruct NFC's success which are as follows.

Acceptance of NFC

The acceptance of mobile payment has been studies in the literature. Some studies [8] [9] [10] also specifically studies the acceptance of NFC payments. Most of these studies [8] [9] use TAM (Technology Acceptance Model) to evaluate the acceptance of mobile payment and NFC payment. Some studies also incorporate other psychological dimensions like trust [10] [11], social influence [9], perceived risk [9] and cost [9]. The acceptance of NFC payments has also been studied based on locations. [12] and [13] studies the state of NFC payments in Switzerland and Korea respectively. The above studies concludes by projecting the acceptance NFC's in those locations. Even though several studies has explored the acceptance of NFC's payments based on various dimensions, some aspect like usability and user experience of NFC remains as an unknown side in literature.

Research Questions

This leads us to the research questions of the thesis:

Usability and User Experience

There are only few researches studies in this direction of usability and user experience of NFC's payment in the literature. For example: [14] studies the usability and user experience issues related to NFC payment and suggests to improve the system such that proper feedback is delivered. Another usability study [15] in the field of NFC explores the usability of NFC based interactions. The studies points out the existing usability issues such as visibility and accessibility in NFC based interaction and also states that there is not enough research in this direction.

As stated by [16] “technology is deeply embedded in our ordinary everyday experience”. Each service, technology or product we use in our everyday life delivers us an experience which plays an important role in accessing that particular service, technology or product. Many existing literature [16] [17] highly recommends us to design based on user experience. NFC payment system lacks research and designing in this direction. Any user would prefer to feel secured and privacy assured at any point of sale (POS).

Q1: How does a specific design of the transaction affect the experience of felt security and privacy by the user?

Based on literature, we would like to investigate the following hypothesis for the first research question.

H1: Less information on NFC cards provide secured and privacy enhanced experience

H2: Visible and audible feedback delivers secured and privacy enhanced experience

H3: Context of POS affects the user experience gained

NFC Cards Vs NFC mobiles

In the existing rich set of NFC literature, we were not able to find a study which differentiated mobile and card NFC. Most related literatures concentrate only on mobile NFC [8] [9]. Now-a-days NFC’s are also be used in credit/debit cards. Based on factors like feedback delivered, information revealing and security mobile NFC and card NFC greatly differs. Mobile NFC delivers additional feedback on mobile screen whereas NFC card remains passive. Also the amount of information displayed via any NFC application is higher than NFC cards as cards contains only the traditional basic information (Card number, name, expiry date and CVV). Unlike NFC cards NFC mobile application can be protected by pin or pattern or biometric lock of the mobile phone. Given the difference between Mobile and card NFC, treating both similarly in research may not be appropriate. Using mobile NFC or card NFC can influence the experience gained by the user.

Q2: How does mobile NFC and card NFC differ in terms of usability and user experience gained?

Personality

The vast available psychology literature states that personality plays an important role in many aspects such as lifestyle, behaviour, motivation, performance etc. The “Big five” personality traits is widely accepted and used as a standard model in psychology researches as it is simple [18] and cross-cultural [19] [24]. Researches states that personalities has either a direct or indirect effect on job performances, motivation and behavior. [20] shows which variables aggressive behavior variables are directly and indirectly related to personalities. Similarly [21] shows correlation between personality and motivation performance.

From the above examples it is clear that personality affects human behavior and performance. There are only few literatures available on HCI and personalities. For example [22] shows the relationship between colours used in interfaces and personalities. Similarly [23] designs and evaluates the user interfaced based on personalities. With few literatures, correlation between personality and user design and user experience is still unexplored. To explore this we would to answer the below research question

Q3: What is the role of personality on perceived experience of felt security and privacy of the user?

Based on [25] the following hypothesis has been framed and will be explored in research question 3.

H1: Users with extraversion accept NFC payment quicker compared to other personalities

H2: Users with openness to experience have little to no effect on experience gained from different designs

H3: Users with neuroticism have higher effect on experience gained form different designs

Research Design

Will base the development of the experience prototypes on principles of the User Centred Design (UCD) process (ISO 9241-210) [1]. Figure 1 shows the UCD process.

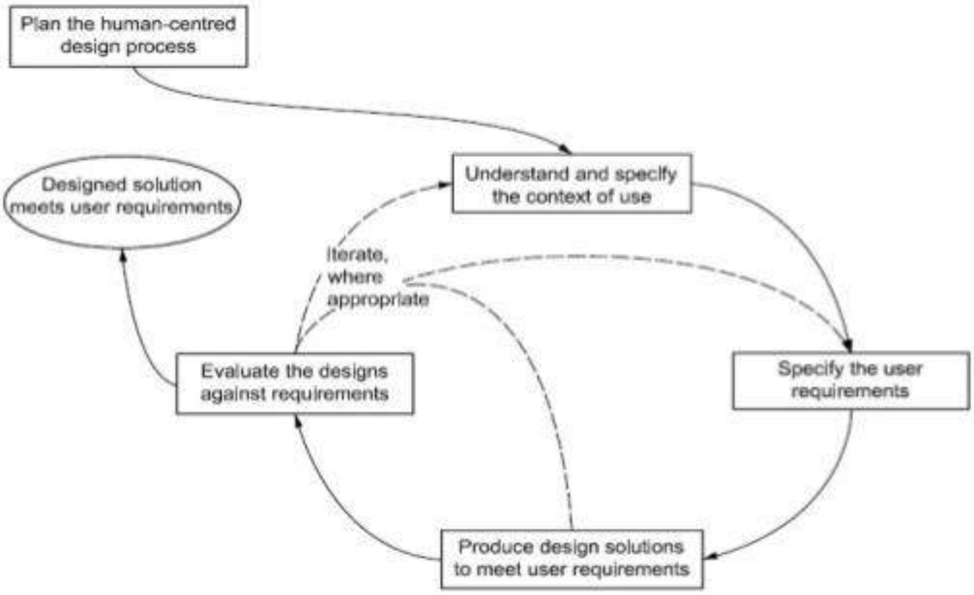
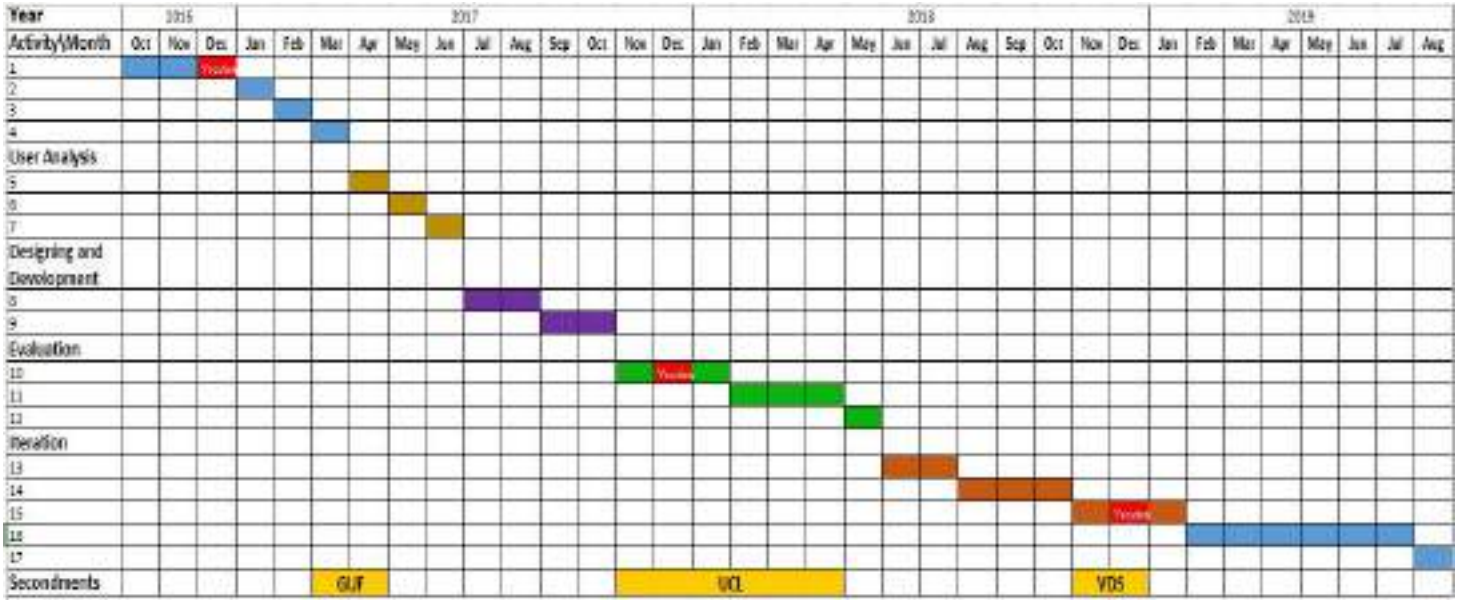

Plan the human-centred design process
Understand and specify the context of use
Designed solution meets user requirements
Iterate, where appropriate
Evaluate the designs against requirements
Specify the user requirements
Produce design solutions to meet user requirements

Figure 1: User Centered Design process ISO 9241-210 [1]

Phase	Goals	Methods
Understanding and specify the context of use	Understand the existing practice	Observation, Interviews
	Understand users' mental model	Observation, Questioners
	Understand existing security and privacy related issues	Interviews
	Understand the context (types of card, payment terminals etc.)	Observation
Specify user requirements	Clear documentation of user requirements	Documentation
Design solution	Design various transaction prototypes	Low fidelity sketches, High fidelity sketches
	Develop various transaction prototypes	Real-time prototypes

Evaluation	Capture the security and privacy related experience felt by the user for each prototype (Lab setting)	Interviews, Questioners
	Capture the effect of personality on the perceived experience (Lab setting)	Interviews, Questioners
	Capture the difference between mobile and card NFC (Real-time)	Observation and exit interviews

Work Plan:



Key

1	Literature study
2	Preliminary interviews
3	Real-time observation
4	Research question and research proposal
	User Analysis
5	Understand the existing practice
6	Understand users' mental model, Understand existing security and privacy related issues
7	Clear documentation of user requirements
	Designing and Development
8	Design various transaction prototypes
9	Develop various transaction prototypes
	Evaluation
10	Evaluation 1

11	Evaluation 2
12	Evaluation 3
	Iteration
13	Final designing
14	Final development
15	Final evaluation
16	Thesis writing
17	Defense and presentation
	Secondments

Reference

[1] International Organization for Standardization (2010). Ergonomics of human system interaction - Part 210: Human-centered design for interactive systems. ISO 9241-210:2010

[2] Lee, Zon-Yau, Hsiao-Cheng Yu, and Pei-Jen Ku. "An analysis and comparison of different types of electronic payment systems." *Management of Engineering and Technology, 2001. PICMET'01. Portland International Conference on*. IEEE, 2001.

[3] Staib, Philippe, James Helm, and Thierry Renard. "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.

[4] Leong, Lai-Ying, et al. "Predicting the determinants of the NFC-enabled mobile credit card acceptance: A neural networks approach." *Expert Systems with Applications* 40.14 (2013): 5604-5620.

[5] Ok, Kerem, et al. "Current benefits and future directions of NFC services." *Education and Management Technology (ICEMT), 2010 International Conference on*. IEEE, 2010.

[6] Pasquet, Marc, Joan Reynaud, and Christophe Rosenberger. "Secure payment with NFC mobile phone in the SmartTouch project." *Collaborative Technologies and Systems, 2008. CTS 2008. International Symposium on*. IEEE, 2008.

[7] Massoth, Michael, and Thomas Bingel. "Performance of different mobile payment service concepts compared with a NFC-based solution." *Internet and Web Applications and Services, 2009. ICIW'09. Fourth International Conference on*. IEEE, 2009.

[8] Schierz, Paul Gerhardt, Oliver Schilke, and Bernd W. Wirtz. "Understanding consumer acceptance of mobile payment services: An empirical analysis." *Electronic commerce research and applications* 9.3 (2010): 209-216.

[9] Tan, Garry Wei-Han, et al. "NFC mobile credit card: the next frontier of mobile payment?." *Telematics and Informatics* 31.2 (2014): 292-307.

[10] Lu, Yaobin, et al. "Dynamics between the trust transfer process and intention to use mobile payment services: A cross-environment perspective." *Information & Management* 48.8 (2011): 393-403.

[11] Boes, Kim, Larissa Borde, and Roman Egger. "The Acceptance of NFC Smart Posters in Tourism." *Information and Communication Technologies in Tourism 2015*. Springer International Publishing, 2015. 435-447.

[12] Ondrus, Jan, and Yves Pigneur. "An assessment of NFC for future mobile payment systems." *Management of Mobile Business, 2007. ICMB 2007. International Conference on the*. IEEE, 2007.

[13] Shin, Seungjae, and Won-jun Lee. "The effects of technology readiness and technology acceptance on NFC mobile payment services in Korea." *Journal of Applied Business Research* 30.6 (2014): 1615.

[14] Geven, Arjan, et al. "Experiencing real-world interaction: results from a NFC user experience field trial." *Proceedings of the 9th international conference on Human computer interaction with mobile devices and services*. ACM, 2007.

[15] Tomitsch, Martin, Thomas Grechenig, and Richard Schlögl. "Real-world tagging in the wild: On the usability and accessibility of NFC-based interactions." *Workshop on Future Mobile Experiences: Next Generation Mobile Interaction and Contextualization, Co-Located with the Nordic Conference on Human-Computer Interaction, NordiCHI*. 2008.

[16] McCarthy, John, and Peter Wright. "Technology as experience." *interactions* 11.5 (2004): 42-43.

[17] Garrett, Jesse James. *Elements of user experience, the: user-centered design for the web and beyond*. Pearson Education, 2010.

[18] Zillig, Lisa M. Pytlik, Scott H. Hemenover, and Richard A. Dienstbier. "What do we assess when we assess a Big 5 trait? A content analysis of the affective, behavioral, and cognitive processes represented in Big 5 personality inventories." *Personality and Social Psychology Bulletin* 28.6 (2002): 847-858.

[19] McCrae, Robert R., and Paul T. Costa Jr. "Personality trait structure as a human universal." *American psychologist* 52.5 (1997): 509.

[20] Barlett, Christopher P., and Craig A. Anderson. "Direct and indirect relations between the Big 5 personality traits and aggressive and violent behavior." *Personality and Individual Differences* 52.8 (2012): 870-875.

[21] Judge, Timothy A., and Remus Ilies. "Relationship of personality to performance motivation: a meta-analytic review." *Journal of applied psychology* 87.4 (2002): 797.

[22] Karsvall, Arvid. "Personality preferences in graphical interface design." *Proceedings of the second Nordic conference on Human-computer interaction*. ACM, 2002.

[23] Karsvall, Arvid. "Design and Evaluation of a Personality Inspired Digital TV Interface." *Unpublished Master’s Thesis, Cognitive Science Program, Linköping University* (2000).#

[24] Schmitt, David P., et al. "The geographic distribution of Big Five personality traits: Patterns and profiles of human self-description across 56 nations." *Journal of cross-cultural psychology* 38.2 (2007): 173-212.

[25] Devaraj, Sarv, Robert F. Easley, and J. Michael Crant. "Research note—how does personality matter? Relating the five-factor model to technology acceptance and use." *Information Systems Research* 19.1 (2008): 93-105.

Poornigha Santhana Kumar (ESR04), Usecon (USE)

I. Personal and Organizational Information

ESR´s Personal Information			
Name:	**Poornigha Santhana Kumar**	**ID number**:	ESR 04
Office Address:	Modecenterstraße 17 / Objekt 2, 1. Stock, 1110 Vienna, Austria	**Phone**:	
Mobile:	+43 6608366515	**E-Mail:**	kumar@usecon.com

ESR´s Host Organization Information			
Name:	**USECON**	**Phone**:	+43 (0) 7435451407
Address:	Modecenterstraße 17 / Objekt 2, 1. Stock, 1110 Vienna, Austria		
***If enrolled organization is different from host organization, please specify:**			
Name:	**University of Salzburg**	**Phone:**	**+43 66280440**
Office Address:	Kapitelgasse 4-6, 5020 Salzburg, Austria		

II. Supervision

Supervision			
Supervisor´s Name:	Manfred Tscheligi	**Title**:	Prof. Dr.
Place of Employment:	University of Salzburg	**Phone**:	+43 662 8044-4811
Responsibility Distr.:	75%	**E-Mail:**	manfred.tscheligi@sbg.ac.at
Co-Supervision			
Co-Supervisor´s Name:	M. Angela Sasse FREng	**Title**:	Prof.
Place of Employment:	University College London	**Phone**:	+44 020 7679 7212
Responsibility Distr.:	25%	**E-Mail:**	a.sasse@ucl.ac.uk
Conduct of Supervision (per activity describe form of supervision and estimated supervision hours)**:**			
Supervisor – Mag. Michael Bechinie • Weekly meetings on progress – 1 hour • Biweekly meeting for Brainstorming and feedbacks – 1.5 hours **Supervisor – Prof. Dr. Manfred Tscheligi** • Biweekly update and feedback via email (Approx. 4 hours per month) **Co-supervisor – Prof. M. Angela Sasse FREng** • Feedbacks on research idea and proposal via email			

III. Secondment

ESR´s Secondment			
Supervisor's Name:	Jetzabel Serna-Olvera	**Position**:	Dr.
Organization´s Name:	Goethe University Frankfurt	**Phone**:	+49 (0) 69 / 798-34667
Address:	60323 Frankfurt, Germany	**E-mail:**	Jetzabel.Serna@m-chair.de

IV. Research Project

ESR´s Project			
Title:	**Designing for privacy and security at POS commercial transactions**	**Ref. No:**	ESR 04

Overview and background

Near field Communication (NFC) is one of the emergent technologies. It has been used recently for contactless payments at retail shops in various countries [1]. Communication between the NFC card/mobile and the payment terminal is initiated when the distance between the payment terminal and the NFC card/mobile is less than 4 cm to 10 cm [2]. Using NFC technology for payments has various advantages as it is faster and reduces the hassle faced by the users [2] [3]. Given the technological side of NFC being well explored in the literature, the usability and user experience related to NFC remains a dark side [4]. Since user experience plays an important role in success of any technology, this thesis aims to provide privacy and security enhanced experience to the users while using NFC payment.

Personality plays an important role in many aspects of our life such as lifestyle, behaviour, motivation, performance etc [5] [6]. The user experience felt by the user can also be influenced by the personality of the user. This thesis also aims to find the effect of personality on the perceived experience on felt privacy and security.

V. Long-Term Career Objectives

Long-Term Career Objectives (over five years)

I aim to remain in HCI research either in academia or industry. I would like to build my career in usability and user interfaces. Since I am perfectly located in an industry I would like to use this opportunity to develop my designing and evaluation skills. I am confident that I will also receive enough hands on experience during the course of my PhD which will help me in achieving my career goals.

I am believe that other professional trainings provided by Privacy & Us will help me to adapt and excel in academic or industrial environment in the future.

VI. Short-Term Career Objectives

A. Project Research Results

Project Research Results
Presented according to Privacy & Us project Plan.

Milestones	Expected Results
Complete user analysis	Clear documentation of existing practises and problems
Requirement analysis	Clear documentation of user requirements
Prototypes	Various designs for a commercial transaction

Deliverables
D 2.1 - Requirements Analysis D 3.1 - The Initial Models D 4.1 - User Interface Requirements D 6.7 - Researcher Declarations and Career Development Plan

Anticipated Publications
During my first year I will be performing user analysis and prototyping. I expect to either publish my user analysis (Existing mental model of the user) or the methodological approach used for my research.

Anticipated Conference/Workshop Attendance & Courses/Seminar Presentations
• IFPI – summer school 2017 (Abstract accepted) • Privacy Enhancing Techniques Convention (PET – CON 2017.1), March 2017 (Attended)

B. Training

Research and Technical Training
• Introduction to PETs, August 2016 • Privacy Enhancing Technologies, January 2017 • USECON – Usability training, February 2017

Secondment Plan

Date: March 2017 – April 2017
Institution name: Goethe University Frankfurt
Work performed:

- Received feedback on research questions and research proposal
- Explored a collaboration opportunity
- Networking

Interdisciplinary Training

- Privacy of Personal Health Data, August 2016
- General Data Protection Regulation – Next Step?, August 2016
- Introduction to Usability, August 2016
- Legal Privacy Workshop – Privacy by Design, August 2016
- The Future of Privacy and Identity Management, August 2016

Professional Training

- Scientific Paper Writing, August 2016
- Professional Networking, August 2016

Other Training Activities

No trainings

C. *Networking Activities*

- Had brainstorming session with USECON employees
- Had discussion and received feedback on research idea from AIT (Austrian Institute of Technology) employees
- Meet PhD students from Centre for human computer interaction, University of Salzburg and discussed collaboration opportunities

D. Research Management

- Received Finding talent: Relocation grant

E. Other activities

Other Activities (professional relevant)
Under going local language (German) course to aid interviews in the later stages of the project

VII. Signatures

Date & Signature of fellow

Date & Signature of supervisor

VIII. Reference

[1] Leong, Lai-Ying, et al. "Predicting the determinants of the NFC-enabled mobile credit card acceptance: A neural networks approach." *Expert Systems with Applications* 40.14 (2013): 5604-5620

[2] Ok, Kerem, et al. "Current benefits and future directions of NFC services." *Education and Management Technology (ICEMT), 2010 International Conference on*. IEEE, 2010.

[3] Pasquet, Marc, Joan Reynaud, and Christophe Rosenberger. "Secure payment with NFC mobile phone in the SmartTouch project." *Collaborative Technologies and Systems, 2008. CTS 2008. International Symposium on*. IEEE, 2008.

[4] Tomitsch, Martin, Thomas Grechenig, and Richard Schlögl. "Real-world tagging in the wild: On the usability and accessibility of NFC-based interactions." *Workshop on Future Mobile Experiences: Next Generation Mobile Interaction and Contextualization, Co-Located with the Nordic Conference on Human-Computer Interaction, NordiCHI*. 2008.

[5] Barlett, Christopher P., and Craig A. Anderson. "Direct and indirect relations between the Big 5 personality traits and aggressive and violent behavior." *Personality and Individual Differences* 52.8 (2012): 870-875.

[6] Judge, Timothy A., and Remus Ilies. "Relationship of personality to performance motivation: a meta-analytic review." *Journal of applied psychology* 87.4 (2002): 797.

Privacy Indicators in Smartphone Ecosystems

Majid Hatamian (ESR05), Goethe University Frankfurt (GUF)

Abstract. Smartphone ecosystems have evolved to support the ever-increasing need of usability for the users in different domains such as transportation or e-health, which results from the rapidly-evolving and wide-adoption of smartphone apps. However, despite the tremendous benefits, most apps rely on the use of personal data, making privacy one of the most critical challenges to be addressed. To date, this area has not been explored sufficiently mainly because privacy-preserving methods in smartphone apps entail specific requirements with respect to users' rights. This Ph.D. project focuses on the theory, design and experimental validation of privacy indicators in smartphone apps, with an emphasis on novel approaches and alarming components to adequately and appropriately inform users of the consequences of their decisions regarding their privacy which will support and allow them to make informed decisions regarding their privacy. We first consider an approach to figure out the privacy threats of apps, considering that data-flows and types of data to be processed are becoming more complex. We next consider user comments on app markets as an important source to extract knowledge regarding the privacy invasiveness of apps. We believe this will increasingly help and support users to perceive the potential privacy violations of apps. There is also the possibility to consider matadata (app description, ratings, etc.) on app stores as an important entity to identify over-privileged apps. This will enable us to warn users about the hungry apps which use permissions that do not related to their functionalities.

1 Introduction

Privacy have always been a serious concern in the field of information technology. Privacy is an extensive concept that captures various aspects of our life and, therefore, several definitions of privacy exist. In the information security context, 'privacy' usually refers to the expectations and rights that people have concerning their personal information in order to securely and adequately handle this information [1]. Keeping this in mind, while smartphone apps provide tremendous benefits to users, especially in terms of personalised and context-sensitive services (e.g. online booking, location searching, etc.), having access to a multiplicity of sensitive resources also poses a series of privacy and security risks [2]. In this regard, current smartphone ecosystems reflect a fundamental tension between privacy and usability. The more smartphone apps need to provide usability, the more they require to have access to data. Above all, users are often unaware of the data collected by their apps. Accordingly, they express discomfort once they realise that their data are being collected without their consent. This brings us to the recently approved General Data Protection Regulation (GDPR) [3] of EU which is supposed to provide individuals with a stronger control on their personal data, one important challenge is the recognition of *privacy by design* and *privacy by default* which are strongly emphasising on the strength and unification of data protection for individuals [4]. Additionally, PbD is aimed to ensure the adoption of the critical role of transparency and informed consent and it explicitly claims that users should understand the risks inherited to the procedure of data sharing and data collection.

2 Background

In this section, we first introduce the concept of smartphone ecosystems (Section 2.1). We then briefly discuss the privacy motivations and issues regarding the smartphone ecosystems (Section 2.2). Finally, in Section 2.3 we review Android operating system as the basis of our study.

2.1 Smartphone Ecosystems

Basically, the term 'smartphone ecosystem' comprises smartphones' hardware and software platform including apps running on top of the platform, as well the infrastructural components such as app markets (e.g. Google Play, App Store) [5]. In principle, three entities play an important role in smartphone ecosystems:

Users are directly or indirectly benefiting from app stores by downloading and using apps.

App Developers are involving in the mass market (app stores) of apps by developing apps for smartphones, mobile devices, etc.

App Stores are rich sources of apps and it directly or indirectly communicates with app developers and users.

2.2 Privacy in Smartphone Ecosystems

If we look at the history, there have been several definitions for privacy. As the widely renowned publication in the US which advocated the right to privacy for the first time, privacy was introduced as the right to be let alone [6]. However, by the beginning of information age, privacy was defined as the claim of individuals, groups, or institutions to decide for themselves when, how, and to what extent information about them is communicated to others [7]. After the incremental advances in information technology at the end of 1990s, privacy was defined as the ability of the individuals to protect personal information about themselves [8].

Additionally, with the rapid growth of technology in recent years, our life is now significantly surrounded by or even dependent on the use of technological devices, especially smartphones. As a consequence, the number of mobile apps available has exploded over the past few years. For instance, the number of available apps in the Google Play Store surpassed 1 million apps in July 2013 and was most recently placed at 2.4 million apps in September 2016. At the same time, the number of cumulative apps which were downloaded from the Google Play app store reached by 15 million from 50 to 65 million between July 2013 and May 2016 [9, `website4?`].

Accordingly, with the growing proliferation of smartphone apps, smartphone ecosystems are envisaged to provide remarkable value for both users and app developers. Smartphone ecosystems, however, are considered as a unique source due to the large number of apps which in turn makes an extensive use of personal data. As a consequence, smartphone users are often unaware of the data which are being accessed by different installed apps. Specifically, they do not know by whom and to which extent these data are collected, transferred and processed [11]. Moreover, the lack of reliable permission information may allow app developers request unnecessary permissions, resulting in overprivileged apps. Moreover, the lack of risk information of permissions confuses the users with regards to determining whether to install the app or not. Above all, there is a lack of transparency for the users since they do not understand the implications and consequences of sharing different types of data. Accordingly, they feel disappointed once they realise that their data are being accessed without providing a transparent privacy indicator [12].

2.3 Android Operating System

Android [1] is an open source and Linux-based OS for mobile devices like smartphones and tablets and the first commercial version of it (Android 1.0) was released in September 2008 [13]. In this Ph.D. project we mainly focus on Android OS. There are several reasons behind this selection. Firstly, Android has been an impressive prosperity in smartphone market and it has dominated with a share of 87.6% in 2016Q2 [14]. Secondly, the source code for Android is available under free and open source software licenses and due to its open source nature, it provides access to a mixed variety of useful libraries and tools that can be used by developers to build rich apps. Lastly, 97% of malicious mobile malware targets Android [15]. This is why we found Android as a more challenging and attractive platform compared with other OSs (such as iOS, Windows Phone, etc.) which requires more precise attention in terms of privacy and security.

[1] https://developer.android.com/index.html

3 Research Objective

The main objective of this Ph.D. project is to preserve the users' privacy and enhance the methodologies that are currently being used to increase the users' awareness of privacy in smartphone ecosystems. In the following, we clarify what is the problem, why it is important to be tackled, and how our objective can meet such problem:

1. Providing transparency for smartphone apps:

   As it was investigated in the literature (see Section 4), smartphone users often pay limited attention to privacy indicators and they do not take care of the privacy invasiveness consequences that might be happened because of using a certain app. Additionally, current smartphone apps are suffering from a lack of transparent component to appropriately inform users of the activities that they are doing.

   This is important because when a user installs an app, she has to grant many permissions (even dangerous ones, e.g. Camera, Microphone, etc.). If the app would be a privacy invasive app, then the user can never infer this.

   We will aim to propose a transparency tool that its ultimate goal is to provide a transparent and visible interface which informs users of the real behaviour of the apps, e.g. which information is accessed, at which frequency, etc.

2. Providing a fair comparison of apps regarding privacy:

   In the current smartphone ecosystems (e.g. Google Play), users can compare apps by analysing the scoring system. However, this scoring system is only related to the functionalities of apps (e.g. user interface, how fast it runs, beauty, etc.). As a result, there is no way for the users to compare apps regarding their privacy levels.

   This is highly important since if there would be a scoring system in current smartphone apps which could show to which extent an app might be privacy invasive for the user, then users would be able to decide whether they feel comfortable to install that app or not. Also they could make a comparison between apps with the same functionality but with different privacy scores.

   User comments on app stores are valuable sources that sometimes claim issues regarding apps' privacy. We will aim to explore these comments in order to classify them and extract knowledge based on the facts evident in users' claims. This would ultimately enable us to provide a scoring system which takes the privacy sensitiveness level of apps into consideration by analysing user comments.

3. Increasing user awareness of privacy:

   Smartphone users usually pay limited attention to the privacy indicators.

   This happens due to many reasons, e.g. poor understanding of what privacy indicators mention, ambiguity of the indicators, unaware of potential risks of sharing personal sensitive information, etc.

This is increasingly challenging to understand whether the smartphone users are aware of the potential risks of using certain apps or not. If we could do a mapping between users' perceptions regarding their privacy, and the real behaviour of the apps being used by the users, then we would be able to increase user awareness of privacy. Therefore, we aim to capture the users' perceptions, concerns, and experience regarding their privacy. Then, we will aim to use the proposed artifacts as the basis in order to understand the users' perceptions, concerns, and experience regarding their privacy after interacting with the proposed artifacts. We believe if the users see the results obtained regarding the analysis of the real behaviour of installed apps, then they would be most likely to revise/review their privacy settings. In fact, this study is supposed to support users to review their perception about privacy. Furthermore, it is also aimed to help users to change their privacy behaviour, e.g. restricting permission settings, uninstalling privacy invasive apps, choosing and installing privacy-friendly apps, reporting privacy invasive activities, etc.

4 Related Work

In general, when we look at the literature, we see a diverse number of approaches for increasing awareness of privacy and supporting users to make informed decisions. After having an in-depth look at them, we decided to categorise the proposed solutions in the literature into three categories. They are introduced as follows:

Data Flow Analysis & Risk Communication-based Methods: These approaches are mostly focused on the analysis of data flows and permissions. They are mainly based on the fact which prioritises the consciousness of users. To be more clear, they are focusing on providing efficient privacy controllers over the permissions (e.g. indicators, recommendations, etc.) by analysing and excavating data flows to raise the consciousness of privacy.

User-centred Methods: These approaches are concentrated on user profile. In other words, they consider a privacy preservation solution based on the users' preferences.

Crowdsourcing-based Methods: These approach are based on crowdsources. More specifically, the main idea of these approaches is to extract knowledge from crowdsources (e.g. user comments on Google Play) to figure out the privacy invasiveness level of apps.

4.1 Data Flow Analysis & Risk Communication-based Methods

Privacy controls are currently provided in the form of permission warnings to inform users about the accesses. However, they often fall insufficient especially for communicating risk during app installation. To increase user awareness of privacy and showing the capability of privacy consciousness methods, researchers argue that people should easily understand risk indicators which could help people to make low risk decisions regarding their privacy. These methods are based on extensively examination and analysis of data flows and permissions. As a result, they are supposed to identify privacy and security violations with regards to the respective analysis.

For this purpose, several efforts have been done to improve the privacy awareness of users and help them to make rational decisions. In [16], the authors proposed a mobile app recommender system with privacy and security awareness. They aimed to enable their proposed recommender system to automatically detect and evaluate the security risk of mobile apps. Their method generates app recommendations by considering both the apps' popularity and the users' security preferences. Although the method is promising since they highlighted the importance of app recommendation as an important phenomenon to increase the awareness of privacy. But, we will consider the applicability of a decision-making based approach to intelligently perform the risk assessment.

In [17], the authors introduced a method to make smartphone apps more secure through automated testing, detecting and analysing privacy violations. They suggested the use of an automated privacy-testing system to efficiently explore an app's functionality, logging relevant events at multiple levels of abstraction as the app executes, and using these logs to accurately characterise an app's behavior. Their method sounds good, however, there is no practical implementation to evaluate the functionality of their approach.

In [18], the authors tried to better understand smartphone apps security by studying 1,100 popular free Android apps. They further proposed a decompiler which recovers Android apps source code directly from its installation image. This is done to figure out the misuse of privacy sensitive information, particularly phone identifiers and geographic location. Moreover, they analysed 21 million lines of recovered code from these 1,100 free apps using automated tests and manual inspection. This analysis revealed the use/misuse of personal/phone identifiers, and deep penetration of advertising and analytics networks. This is an interesting study, however, the main challenge regarding this approach is that the authors selected 1,100 free apps with a bias towards popularity.

In [19], the authors investigated the privacy of smartphone apps in a different way. Instead of looking at single permissions individually, they suggested to monitor a set of sensitive permissions, e.g. location, gallery, contacts, phone number, etc. As a particular case, an app which accesses Internet, camera, and microphone is able to record audio and video from the user and send it to a third party. In a sample of 311 of the most popular applications downloaded from Google Play, they found five apps that implement dangerous functionality and therefore should be installed with extreme caution. Although this method sounds interesting and opens a new door to other researcher for simultaneous analysis of permissions, but it was narrowed down to a limited number of samples (311), and there is no concrete evidence to make sure whether their approach is actually applicable.

TaintDroid [20] is a method in which the behavior of 30 popular Android applications was studied. This method is capable of simultaneously tracking multiple sources of sensitive data. The analyses revealed that two-third of the apps show suspicious handling of sensitive data and that 15 of them reported users' locations to remote advertising servers. This work is important since it enabled authors to further criticise the lack of transparency on how apps use individuals' private data. Complementary to this, we aim to propose a monitoring tool for log analysis which does not require any modification to the OS or root access. This makes our approach unique and affordable.

Styx [21] is the name of a conceptual model which inspired us to propose an actual and realistic approach for privacy preservation in Android. Styx is aimed to properly and efficiently communicate the privacy impacts of smartphone apps to its users. Generally, it is a privacy risk communication system that provides users with meaningful privacy information based on the actual behavior of apps. Basically, it consists of five main components, including monitoring, log, pattern collection, pattern detection, and notification. The results obtained through a user study showed that Styx is able to increase user trust into smartphone platforms and also reduce privacy concerns through communicating efficient privacy warnings. Irrespective of Styx's benefits, an important question regarding its functionality is that the authors suggested the use of TaintDroid (a log analyser tool) for their monitoring component. But using this tool imposes some serious limitations on the applicability of their approach since TaintDroid needs root access and some changes to OS which is not affordable and acceptable from the users' side. By contrast, we aim to propose a tool for monitoring logs which does not require neither change to the OS nor root access.

4.2 Assessing Privacy Risks using User-Centric Methods

Many of the existing solutions for assessing privacy risks in smartphone ecosystems do not consider a privacy per user-based approach. In fact, they are suffering from a lack of user input. For this reason, some studies have been done to according to the value of each smartphone sub-asset (e.g. contact list, usage history)

The authors in [22] suggested the use of a user-centric approach for privacy risk communication in smartphones. Therefore, authors consider users' profiles as an important principle while assessing the privacy risk of each user. They first provide a taxonomy of user data found on a smartphone and their respective Android permissions and discuss ways to assess the impact of their disclosure for a given user. Next, they figure out the potential threats to user data. For each threat, they consider the permissions required for the threat to occur. This is done by analysing the times that a user grants permission to an app. As a result, they are able to identify the vulnerabilities. However, the main important question that must be sought is how the authors decreased the threat likelihood, which could be considered as an important limitation of this work. By contrast, we do not focus on finding potential threats. Instead, by exploiting a rule-based approach, we examine a combination of permissions requests from each installed app to figure out their vulnerability.

In [23], another user-centric scenario for smartphone user has been investigated. Clearly, smartphone OSs (e.g. latest versions of Android) warn users when a application tries to access sensitive functions or data. However, sometimes they fail to provide a fine-grained warning about different application actions. For this reason, authors performed a user study by surveying 3,115 smartphone users about 99 risks associated with 54 smartphone privileges. They asked users to rate how upset they would be if given risks occurred and used this data to rank risks by levels of user concern. This is why this work potentially propose a basis about the selection of of warnings regarding the users' concerns. However, we believe such approaches cannot guarantee a fine-grained selection of privacy warnings. Since participants might have failed to list their negative experiences with apps due to forgetfulness or uncertainty over the open-ended question. By contrast, we intend to apply a machine learning approach on user comments to figure out the extent to which each comment can be exploited as an informative element regarding users' privacy.

In [24], the authors proposed a novel concept called privacy bubble. The main goal of the authors is to target scenarios in which the data are being shared with strangers in a controlled fashion. They suggested the use of privacy bubbles which metaphorically represent the private sphere of the users. In this metaphor, each user occupies the center of her bubble and can share pictures with users located outside her bubble. The privacy bubbles are able to automatically confine the access to the content generated by the bubble creator to people within the bubble. They also validated the user acceptance of their approach through surveying 175 participants, and proposing a prototype which shows the technical applicability their method. The authors only considered the protection of sharing pictures among users having no social ties in a controlled fashion. This points to the need for helping users to preserve the privacy of all kinds of sensitive information, not just pictures.

4.3 Learning from Crowds Methods

Crowdsourcing approaches are often used to extract knowledge from crowdsources (e.g. user comments in Google Play Store). However, dealing with the problem of learning from crowds is not an easy task to be tackled [25].

So far, various methods for classification of user comments have been proposed. In [26], the authors used a supervised multi-label learning method to identify different types of user comments with security/privacy issues. A label system is also implemented to provide precise task for the learning process. In [27], a method has been proposed to investigate the most informative user reviews from a large and rapidly increasing pool of user reviews. The authors used a review ranking scheme to prioritise the informative user reviews. Furthermore, a filtering process is utilised to filter out non-informative comments. Although our method also entails a filtering process, but we do not focus on the quality of information, but whether the user comments are PSI or not.

In [28], a theoretical analysis of crowdsourced content curation has been proposed. The authors studied crowd-curation mechanisms that rank articles according to a score which is a function of user comments. Although their theoretical approach is not especially investigated for smartphone ecosystems, but it is able to quantify the dynamics of which articles become popular regarding the scores obtained from user comments. In [29], an in-depth analysis of commenting and comment rating behavior in social web has been proposed. In this work, the authors examined the dependencies of comment ratings with textual content (e.g. videos and their meta data) to collect a comprehensive understanding of the community commenting behavior. They also exploited the applicability of machine learning and data mining to identify the acceptance of comments by the community. In [30], a crowdsourcing ranking method for user comments in smartphone ecosystems was proposed. The authors suggested to use risk assessment of an app from its user comments as a crowdsourcing problem in order to provide a ranking model. They used a security labeling system from user comments to automatically rank the risks of app based on these learned labels as features. All the discussed methods did not consider the influence of sentiment and lifetime analysis while performing the learning algorithm. We believe considering sentiment and lifetime analysis in the feature vector will help us to better differentiate user comments with privacy and security signs.

5 Proposed Approach

This Ph.D. project mainly has two dimensions: 1) privacy preservation by data analysis (Section 5.1), and 2) privacy preservation by user comments analysis (Section 5.2). We also highlight the importance of usability while designing and implementing both dimensions. Thus, Section 5.3 is introduced as a supportive section for both dimensions of the study.

5.1 Dimension 1: Privacy Preservation by Data Analysis

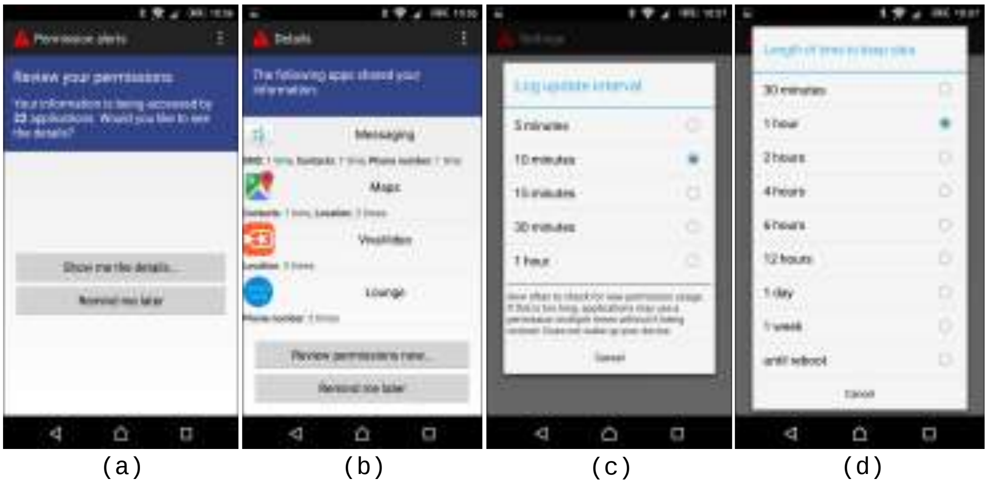
5.1.1 Coarse-grained Privacy Indicator

Initially, we aim to implement a coarse-grained indicator, meaning that we try to provide users with a detailed view of accesses to resources. This will be done by proposing a log analysis tool. This log analyser will enable users to figure out to which extent and by whom their resources (camera, microphone, contacts, SMSs, etc.) are being accessed. This log analyser is aimed to appropriately inform users of the data which are being accessed by installed apps. Current tools for monitoring logs require root access to the devices. However, we do not want to rely on this fact. Furthermore, the log analyser should benefit from a user-friendly GUI. This supports users to revise/adjust their apps' permissions. Basically, we will behaviourally analyse the installed apps because our final goal is to amend the awareness of misconduct behaviours and accessing to sensitive data. An important question that is sought to be investigated is how can we capture the user's attention to the privacy indicators? From a psychological point of view, the perceived log analyser should be able to attract the user's attention [31]. Accordingly, we will ask users to revise (review) their apps' permissions with convenient and optional settings that can be adjusted according to users' preferences. Figure 1 shows different screens of the potential log analyser.

In Figure 1(a), the user will be notified by the alarming notification. The interface of this alarming structure will be implemented in such a way to efficiently attract the user's attention. Additionally, Figure 1(b) demonstrates the details of accessing to sensitive information. These details will be shown with respect to the app's name, and the number of apps accessing different types of information flows in a given period. In Figure 1(c) and (d) we give the ability to the users to optionally select their desirable time preferences for monitoring the permissions.

5.1.2 Fine-grained Privacy Indicator

In the next step, we will intend to provide a find-grained metric for the users to more accurately inform them of the risks of using different installed apps. This could be done according to the information obtained from the log analyser, e.g. to define some rules by a combination of accesses to sensitive resources to infer potential privacy invasive activities. This information then will be used as the input for a decision-making system, to estimate a privacy risk score for each installed app. As a result, we will provide users with a more accurate criterion which



Permission alerts

Review your permissions

Your information is being accessed by 22 applications. Would you like to see the details?

Show me the details...

Remind me later

(a)

Details

The following apps shared your information

Messaging

Maps

VivaVideo

Lounge

Review permissions now...

Remind me later

(b)

Log update interval

5 minutes ○
10 minutes ●
15 minutes ○
30 minutes ○
1 hour ○

Cancel

(c)

Length of time to keep data

30 minutes ○
1 hour ●
2 hours ○
4 hours ○
6 hours ○
12 hours ○
1 day ○
1 week ○
until reboot ○

Cancel

(d)

Figure 1: The proposed log analyser (a) first screen (b) notifications (c) log update interval, and (d) length of time to keep data

supports them for an informed and intelligent decision. The perceived approach will have the following features:

- Restrict permissions: By providing fine-grained information, we will enable users to restrict their permissions if they do not feel comfortable granting a certain permission.
- Semi-automated reporting mechanism: By initiating a semi-automated reporting scheme, we will enable users to send feedback/report to our server. This will enable us to use these reports for the second dimension of our study.
- Selection of apps to be monitored: We will enable users to optionally and selectively choose apps that they are interested to be monitored.
- Mapping permissions to common language definition: We will map all the technical terms regarding permissions to understandable terms for the end user.
- Optionally changing the scan intervals: We will enable users to optionally decide the scan intervals by which the log analyser will scan the phone, e.g. 1 day, 2 days, 4 days, 1 week, etc.
- Showing the results of the scans in a sorted list: We will show the results of the scans in a sorted list, thus the users can easily search through that list.

5.2 Dimension 2: Privacy Preservation by User Comments Analysis

According to the first principle of PbD, in every IT system, the privacy invasiveness activities should be anticipated and prevented before happening. This brings us to the point of how can we embed this important principle into smartphone ecosystems?

User comments on app stores (Google Play, App Store, etc.) are considered as an important source which can describe many interesting facts regarding each app. Having considering this fact, we intend to analyse the privacy sensitiveness level of apps regarding the user comments. For this reason, we come up with a challenging problem called classification. To overcome this challenge, we aim to exploit machine learning algorithms (e.g. SVM, ANN, etc.) to classify user comments based on their privacy sensitiveness level. This enables us to support users for making informed-decisions before installing apps which is totally aligned with the first principle of PbD. This is why we found user comments as the core element for our approach.

The first step that we will take into consideration is data collection. Usually, user comments are publicly available on smartphone ecosystems. For this purpose, a crawler could be used for crawling the user comments. As the second step, we will try to propose some features for comments to make the maximum differentiation between them. This will help us to efficiently do the training phase of our machine learning algorithm. We believe sentiment analysis and lifetime analysis of comments could be significantly helpful for us. However, to avoid any underfitting or overfitting issue, we will consider validation of our algorithm based on a limited number of user comments [32]. Accordingly, the testing phase will be performed.

Currently, in app stores (e.g. Google Play) there is a scoring system (star-based) by which the users are able to see to which extent an app is rated by other users. However, this scoring system is related to the functionality of the apps. We believe such a mechanism must be initiated in every smartphone ecosystems for demonstrating the privacy issues of apps in the form a scoring system. That is why we will propose a privacy risk score according to the user comments analysis which can inform users about the privacy invasiveness level of apps. Thus, the users can decide whether they feel comfortable to install that app or not.

As an important notion, in addition to the analysis of user comments on Google Play, we will also use the reports obtained from the first dimension of our study to extract knowledge regarding the privacy invasiveness level of apps.

5.3 Special Focus on Usability

In this section, we point out the importance of usability in designing and implementing both dimensions of the Ph.D. studies. So this section is aimed to support the proposed approach in terms of usability. The design of interactive smartphone apps does not necessarily require technical requirements. This brings us to the question of how we can amend the usability while proposing novel privacy preservation approaches. More specifically, the proposed artifacts have to work correctly and interact with users properly. That is why the GUI (which is a part of Human-Computer Interaction (HCI)) plays an important role in our privacy preservation methodology since it is what users see, hear, touch, talk to or control. Users expect apps to work but will choose those that are easier to use. Thus, we take the Nielsen's definition [33] regarding usability into account, and consider five attributes for a usable system:

Learnability The system should be easy to learn;

Efficiency The system should be efficient to use;

Memorability The system should be easy to remembe;

Errors The system should have a low error rate;

Satisfaction The system should be pleasant to use.

That is why apart from the privacy preservation approaches and methodologies that we are aiming to implement during the Ph.D. studies, we will not neglect the crucial role that usability and GUI play in smartphone apps. To this end, in order to achieve and include the aforementioned attributes in our methodology, we will extensively focus on usability from two different perspectives: technical and psychological.

5.3.1 Technical Perspective of Usability

From a technical point of view, we should take some important considerations into account. We initially define some important technical properties for the potential GUI to increase usability. Therefore, the proposed GUI should [33]:

- satisfy users' data protection needs
- be easy to use and intuitive
- allow user to focus on tasks and information provided regarding her privacy, and not the mechanism of the GUI
- fast response time
- have good text - focused, task oriented, not too long, not too short
- work the same on all Android versions
- reduce memory work, intellectual work, and minimise burdens imposed by technology

5.3.2 Psychological Perspective of Usability

It is evident that most of the users usually remember the one thing that went wrong, not the many that go right. Due to this fact, it is an essential need to focus on usability from a psychological perspective. To achieve a concrete solution, we identified the following psychological defects that must be addressed [34]:

- **Tedium**. It happens when the user is not able to quickly interact with app (e.g. long response times).
- **Length**. The amount of texts in each screen of apps should be balanced. This is also the case for privacy policies, since they are usually too long.
- **Ambiguity**. The different component of app should be clear and understandable to every user with different kinds of knowledge, age, education, etc.
- **Attractiveness**. The app should be attractive. People do not want to follow what they do not like. Also, privacy indicators should concentrate the users' attention and they should not overwhelm users with meaningless indications.

- **Annoyance**. App should not limit users' freedom. Importantly, privacy indicators should not annoy users with inappropriate information which prevents a normal task being completed. Difficulties in quickly finding information, out-dated information, and visual screen distractions are a few examples of the things that may annoy users.
- **Fear**. Unavailability of app or some of its components which affect the users' normal routines may impose fear. Importantly, when user confronts with inappropriate privacy indicator which targets her sensitive personal data.

As it can be seen, there is a strong relationship between technical and psychological perspectives and some of the features are common in both perspectives.

6 Work Plan

In this section, we first explain the proposed time plan for the doctoral studies (Section 6.1). Then we describe the ways by which the dissemination of the results take place (Section 6.2).

6.1 Time Table

Figure 2 shows the proposed time plan for the whole duration of the doctoral studies. The first phase is started by doing an in-depth literature review to understand the similar proposed approaches. This will enable us to better identify the advantages and disadvantages of previous work. As a result, the gaps will be recognised and the our proposed solutions will be aligned according to these gaps. Requirement analysis and writing the Ph.D. proposal are done in parallel with literature review. In the next step, the design of both dimensions of the doctoral study will be started. While we have finished the design of each dimension, we will start the implementation of it. The next stage is to validate the results obtained from both dimensions by performing user study. Finally, the thesis will be written and submitted.

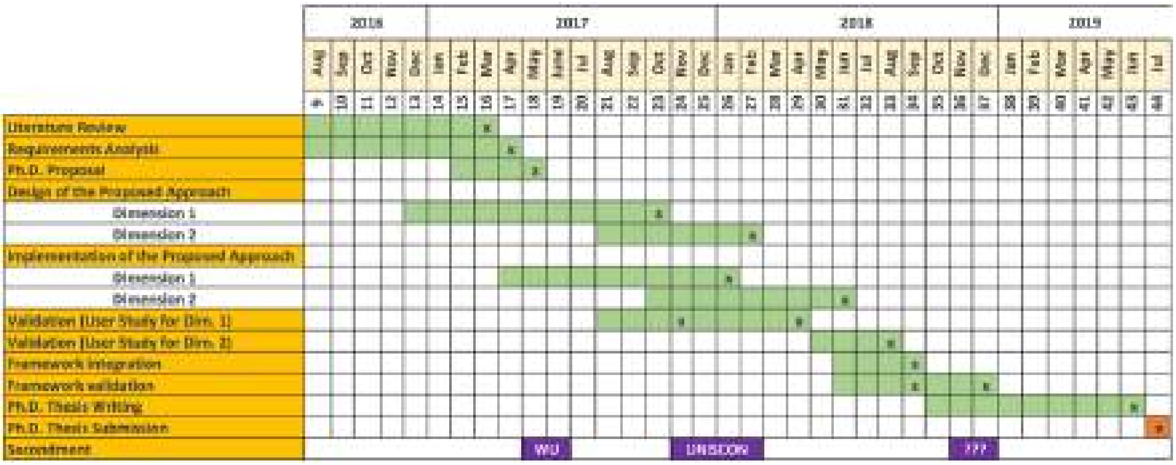


Figure 2: Time plan for the whole duration of the Ph.D. studies.

6.2 Dissemination of the Results

We will ensure the dissemination of the research progress and final results. For this reason, the dissemination of the results will take place by three methods:

- Production of several reports in form of deliverables that will be sent to the Supervisiory Board, Management Board, as well as the European Commission;
- Publishing papers in specialist international journals and magazines such as Computer & Security Journal, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Consumer Electronics, IEEE Security & Privacy Magazine, etc.;
- Presentation of papers at international conferences such as European Symposium on Research in Computer Security (ESORICS), IEEE Symposium on Security and Privacy, IEEE International Conference on Consumer Electronics, IFIP ICT Systems Security and Privacy Protection, International Conference on Trust, Privacy & Security in Digital Business (TrustBus), etc.

Appendix

Published Papers

- M. Hatamian and J. Serna, “Beacon Alarming: Informed Decision-Making Supporter and Privacy Risk Analyser in Smartphone Applications," in *Proceedings of the* 35^{th} *IEEE International Conference on Consumer Electronics (ICCE 2017)*, Las Vegas, USA, 468–471 (January 2017)

Accepted Papers

- M. Hatamian, J. Serna, and K. Rannenberg, “FAIR: Fuzzy Alarming Index Rule for Privacy Assessment in Smartphone Applications," To appear in *Proceedings of the* 14^{th} *International Conference on Trust, Privacy & Security in Digital Business (TrustBus 2017)*, Lyon, France, (August 2017)

References

[1] R. Turn, and W. H. Ware, Privacy and security issues in information systems. RAND Corporation (1976)

[2] G. Bal, and K. Rannenberg, “User control mechanisms for privacy protection should go hand in hand with privacy-consequence information: The case of smartphone apps," in *Proceedings of W3C Workshop on Privacy and User-Centric Controls*, Germany, 1–5 (2014)

[3] “EU general data protection regulation," accessed December 6th, 2016, http://eur-lex.europa.eu/legal- content/EN/TXT/HTML/?uri= CELEX:32016R0679&from=EN

[4] A. Cavoukian, “Privacy by design: The 7 foundational principles," in *Information and Privacy Commissioner of Ontario*, Canada, (2010)

[5] X. Wei, “Understanding and improving the smartphone ecosystem: measurements, security and tools," *Doctoral Dissertation*, University of California, (2013)

[6] S. Warren, and L. Brandeis, “The right to privacy," Harvard Law Review, vol. 4, no. 5, 193–220 (1890)

[7] A. F. Westin, “Privacy and freedom," Administrative Law Review, vol. 22, no. 1, 101–106 (1967)

[8] I. Goldberg, D. Wagner, and E. Brewer, “Privacy-enhancing technologies for the Internet," in *Proceedings of IEEE COMPCON*, USA, 103–109 (1997)

[9] "Number of available applications in the Google Play Store from December 2009 to February 2016," accessed September 29, 2016, http://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/

[10] "Cumulative number of apps downloaded from the Google Play as of May 2016 (in billions)," accessed September 29, 2016, http://www.statista.com/statistics/281106/number-of-android-app-downloads-from-google-play/

[11] B. Liu, J. Lin, and N. Sadeh, “Reconciling mobile app privacy and usability on smartphones: Could user privacy profiles help?," in *Proceedings of the World Wide Web Conference*, Korea, 201–212 (2014)

[12] I. Liccardi, J. Pato, and D. J. Weitzner, “Improving mobile app selection through transparency and better permission analysis," Journal of Privacy and Confidentiality, vol. 5, no. 2, 11–55 (2013)

[13] “Android version history," accessed January 26th, 2017, https://en.wikipedia.org/wiki/Android_version_history

[14] “Smartphone OS Market Share, 2016 Q2," accessed December 6th, 2016, https://www.idc.com/prodserv/smartphone-os-market-share.jsp

[15] “97% of malicious mobile malware targets Android," accessed December 6th, 2016, http://www.scmagazineuk.com/updated-97-of-malicious-mobile-malware-targets-android/article/422783/

[16] H. Zhu, H. Xiong, Y. Ge, and E. Chen, “Mobile app recommendations with security and privacy awareness," in *Proceedings of the* 20^{th} *ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* , USA, 951–960 (2014).

[17] P. Gilbert, B. G. Chun, L. Cox, and J. Jung, “Automating privacy testing of smartphone applications," Technical Report CS-2011-02, Duke University (2011)

[18] W. Enck, D. Octeau, P. Mcdaniel, and S. Chaudhuri, “A study of android application security," in *Proceedings of the* 20^{th} *ACM USENIX Conference on Security*, USA, 8–12 (2011)

[19] W. Enck, M. Ongtang, and P. Mcdaniel, “On lightweight mobile phone application certification," in *Proceedings of the* 16^{th} *ACM Conference on Computer and Communications security* , USA, 235–245 (2009)

[20] W. Enck, P. Gilbert, B. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth, “TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones," in *Proceedings of the* 9^{th} *ACM USENIX Conference on Operating Systems Design and Implementation*, Canada, 393–407 (2010)

[21] G. Bal, K. Rannenberg, and J. Hong, “Styx: Privacy risk communication for the Android smartphone platform based on apps' data-access behavior patterns," Computers & Security, vol. 53, 187–202 (2015)

[22] A. Mylonas , M. Theoharidou , and D. Gritzalis, “Assessing privacy risks in Android: A user-centric approach," in *Proceedings of the* 1^{th} *International Workshop on Risk Assessment and Risk-Driven Testing*, Turkey, 21–37 (2013)

[23] A. P. Felt, S. Egelman, and D. Wagner, “IâĂŹve got 99 problems, but vibration ainâĂŹt one: A survey of smartphone usersâĂŹ concerns," in *Proceedings of the* 2^{nd} *ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, USA, 33–44 (2012)

[24] D. Christin, P. S. Lopez, A. Reinhardt, M. Hollick, and M. Kauer, “Privacy bubbles: User-centered privacy control for mobile content sharing applications," in *Proceedings of the* 6^{th} *IFIP WG 11.2 International Workshop on Information Security Theory and Practice: Security, Privacy and Trust in Computing Systems and Ambient Intelligent Ecosystems*, UK, 71–86 (2012)

[25] V. C. Raykar, S. Yu, L. H. Zhao, G. H. Valadez, C. Florin, L. Bogoni, and L. Moy, “Learning from crowds," The Journal of Machine Learning Research, vol. 11, 1297–1322, 2010.

[26] L. Cen, L. Si, N. Li, and H. Jin, “User comment analysis for android apps and CSPI detection with comment expansion," in *Proceedings of the* 1^{st} *International Workshop on Privacy-Preserving IR (PIR)*, Australia, 25–30, (2014)

[27] N. Chen, J. Lin, S. C. H. Hoi, X. X. Nanyang, and B. Z. Nanyang, “Ar-miner: Mining informative reviews for developers from mobile app marketplace," in *Proceedings of the* 36^{th} *International Conference on Software Engineering*, India, 67–778, (2014)

[28] G. Askalidis, and G. Stoddard, “A theoretical analysis of crowdsourced content curation," in *Proceedings of the* 3^{rd} *Workshop on Social Computing and User Generated Content*, USA, (2013)

[29] S. Siersdorfer, S. Chelaru, J. S. Pedro, I. S. Altingovde, and W. Nejdl, “Analyzing and mining comments and comment ratings on the social web," Journal ACM Transactions on the Web, vol. 8, no. 3, Article no. 17, (2014)

[30] L. Cen, D. Kong, H. Jin, and L. Si, “Mobile app security risk assessment: A crowdsourcing ranking approach from user comments," in *Proceedings of SIAM International Conference on Data Mining*, Canada, 658–666, (2015)

[31] W. O. Galitz, “The essential guide to user interface design: An introduction to GUI design principles and techniques," *John Wiley & Sons, Inc.*, Second Edition, Printed in the USA, (2002)

[32] E. Alpaydin, “Introduction to Machine Learning," MIT Press, 2009. ISBN: 9780262529518.

[33] J. Nielsen, “Usability Engineering," CA, USA: Morgan Kaufmann Publishers Inc., 1993. ISBN: 0125184050.

[34] J. Johnson, “Designing with the Mind in Mind, Second Edition: Simple Guide to Understanding User Interface Design Guidelines," CA, USA: Morgan Kaufmann Publishers Inc., 2010.

Majid Hatamian (ESR05), Goethe University of Frankfurt (GUF)

I. Personal and Organizational Information

ESR´s Personal Information			
Name:	**Majid Hatamian**	**ID number**:	
Office Address:	R. 237, RuW Building, Theodor-W.-Adorno-Platz 4, D-60323 Frankfurt am Main, Germany	**Phone**:	+496979834662
Mobile:	+4916090528263	**E-Mail:**	majid.hatamian@m-chair.de

ESR´s Host Organization Information			
Name:	**Goethe University of Frankfurt**	**Phone**:	+496979834701
Address:	Building "RuW", 2nd Floor, Room 2.257 (Secretary)Theodor-W.-Adorno-Platz 4, 60323 Frankfurt am Main, Germany		

II. Supervision

Supervision			
Supervisor´s Name:	**Jetzabel Maritza Serna-Olvera**	**Title**:	Dr.
Place of Employment:	Goethe University of Frankfurt	**Phone**:	+496979834667
Responsibility Distr.:	%60	**E-Mail:**	jetzabel.serna@m-chair.de
Co-Supervision			
Co-Supervisor´s Name:	**Sabrina Kirrane**	**Title**:	Dr.
Place of Employment:	Vienna University of Economics and Business	**Phone**:	+431313364494
Responsibility Distr.:	%40	**E-Mail:**	sabrina.kirrane@wu.ac.at
Conduct of Supervision (per activity describe form of supervision and estimated supervision hours)**:**			

- Estimated supervision by supervisor:

- Technical supervisions (privacy-related): 1.5 hrs per week (36 meetings – 54 hrs)
- Organisational supervisions (scientific and research oriented): 1 hr per week (36 meetings – 36 hrs)

- Estimated supervision by co-supervisor:

- Progress monitoring and scientific discussions via conference calls: 1 hour/two weeks (4 meetings – 4 hrs)
- Interdisciplinary (usability-related): 1 hour/week (8 meetings – 8 hrs)

III. Secondment

ESR´s Secondment			
Supervisor's Name:	**Sabrina Kirrane**	**Title**:	Dr.
Organization´s Name:	Vienna University of Economics and Business	**Phone**:	+431313364494
Address:	Welthandelsplatz 1 1, 1020 Wien, Austria	**E-mail:**	sabrina.kirrane@wu.ac.at

IV. Research Project

ESR´s Project			
Title:	**Privacy indicators in smartphone ecosystems**	**Ref. No:**	5

Overview and background

With the rapid growth of technology, our life is now significantly surrounded by or even dependent on the use of smartphones. Similarly, the number of mobile applications available has exploded over the past few years. For instance, the number of available applications in the Google Play Store surpassed 1 million applications in July 2013 and was most recently placed at 2.4 million applications in September 2016. At the same time, the number of cumulative applications which were downloaded from the Google Play app store reached by 15 million from 50 to 65 million between July 2013 and May 2016 [1], [2]. However, while smartphone apps provide tremendous benefits to users, especially in terms of personalized and context-sensitive services; having access to a multiplicity of sensitive resources also poses a series of privacy and security risks. Specifically, security and privacy have always been a serious concern in the field of information technology. Privacy is an extensive concept that captures various aspects of our life and, therefore, several definitions of privacy exist. In the information security context 'privacy' usually refers to the expectation and rights that people have concerning their personal information in order to securely and adequately handle this information. In this regard, the current smartphone ecosystems reflect a fundamental tension between privacy and usability. The more smartphone apps need to provide usability, the more they require to have access to data. Above all, users are often unaware of the data collected by their applications. Accordingly, they express discomfort once they realise that their data are being collected without their consent [3]. On the other hand, Android has been an impressive prosperity in the smartphone market and it has dominated with a share of 87.6% in 2016Q2. Not surprisingly, 97% of malicious mobile malware targets Android.

For this reason, applying a privacy preservation approach, plays an increasingly important role in data protection. More importantly, under the new EU General Data Protection Regulation (GDPR), one important challenge is the recognition of privacy by design and privacy by default which are strongly emphasising on the strength and unification of data protection for individuals. Therefore, one common approach for preserving privacy is to give the ability to the users to evaluate the permissions requested by an application and determine whether they feel comfortable granting it or not. In fact, in such solutions a privacy control approach is prepared for Android to enable selectively granting, denying or confining access to specific permissions on a certain application. However, it has been demonstrated that these approaches cannot efficiently operate. Especially, since many users do not understand the implications of their decisions [4]. In fact, permission granting approach can be confusing for users because they usually pay limited attention to permission screens and have poor understanding of what the permissions mention. On the other hand, several works have been proposed to extract the privacy risk from metadata on smartphone ecosystems, including user comments, ratings, application descriptions, etc. An important fundamental constraint is that this kind of information is inexpressive and sometimes fails to support a fine-grained measurement about how and to which extent the data are being accessed.

This Ph.D. project has been focused on the theory, design and experimental validation of privacy indicators in smartphone apps, with an emphasis on novel approaches and alarming components to adequately and appropriately inform users of the consequences of their decisions regarding their privacy which will support and allow them to make informed decisions regarding their privacy. We first consider an approach to figure out the privacy threats of apps, considering that data-flows and types of data to be processed are becoming more complex. We next consider user comments on app markets as an important source to extract knowledge regarding the privacy invasiveness of apps. We believe this will increasingly help and support users to perceive the potential privacy violations of apps. There is also a possibility to consider matadata (app description, ratings, etc.) on app stores as an important entity to identify over-privileged apps. This will enable us to warn users about the hungry apps which use permissions that do not related to their functionalities.

V. Long-Term Career Objectives

Long-Term Career Objectives (over five years)
After completing the PhD program, my long-term objective is to seek a teaching and research position in a research or academic institution where I can share my experience and knowledge with other experts/researchers about privacy-oriented issues. Ideally, I would like to research, identify, and provide new challenges, perspectives, and approaches to ameliorate the way of science in the field of privacy in smartphone applications. To be more specific, I would like to develop, implement, and disseminate privacy preservation approaches for reducing the risk of personal data communication. Since I believe during my doctoral study, I will receive a considerable amount of technical supports which are significantly beneficial to achieve this goal. That is why I believe my technical experience, including extensive working knowledge of computer science, privacy and security, and networking, and my exposure to various disciplines of interdisciplinary fields through my bachelor and master degrees, will lay a sound foundation for my career after finishing the doctoral degree. However, I believe the progress toward my career goals requires to also develop some non-technical skills which are increasingly necessary to amend the way that I am going to follow after my doctoral studies. For this reason, Privacy&Us can help me by providing the possibility to broaden my knowledge about non-technical aspects of privacy and security such as psychological and societal aspects. This will give me the opportunity to get in touch with a trans-disciplinary expertise. As a result, the skills and experience that I will acquire carrying out the research in Privacy&Us will prepare me for my career after finishing the doctoral studies. Additionally, to perfectly benefit from Privacy&Us network and achieve my goals long-term goals, I need to improve some personal skills essential for my future career. In this regard, I believe Privacy&Us can help me to improve my presentation skills, while at the same time increasing my confidence, as well as my interpersonal and communication skills.

VI. Short-Term Career Objectives

A. Project Research Results

Project Research Results
Presented according to Privacy & Us project Plan.

Milestones	Expected Results
Investigating literature (M12)	Finding the gaps between the proposed solutions in the literature
Writing Ph.D. proposal (M18)	Proposing novel approaches to address the gaps identified in the literature
Career development plan (M18)	Preparing career development plan toward my career after the Ph.D. studies
Privacy requirement analysis (M18)	Analysing the privacy requirements and privacy principles which are essential for smartphone apps in the form of a report
User interface requirement analysis (M18)	Analysing the user interface and usability requirements which are essential for smartphone apps in the form of a report

Deliverables
2.1: Requirements Analysis (M18) 4.1: User Interface Requirements (M18) 5.1: Privacy Principles (M20) 6.7: Researcher Declarations and Career Development Plan (M18)

Anticipated Publications

- IEEE 35th International Conference on Consumer Electronics (ICCE 2017) – Las Vegas, US
  Submission: *A work-in-progress paper including the main ideas with the initial results regarding the monitoring tool*

- 14th International Conference onTrust, Privacy & Security in Digital Business (TrustBus 2017) – Lyon, France
  Submission: *A full-paper with concrete and more informative results regarding the privacy risk score*

- 51st IEEE International Carnahan Conference on Security Technology – Madrid, Spain
  Submission: *An initial version of the approach for analysis user comments for privacy related information*

Anticipated Conference/Workshop Attendance & Courses/Seminar Presentations

- Workshop on Internet Privacy Engineering Network 2016, 9th Sep 2016, Frankfurt, Germany (attended)
- Annual Privacy Forum 2016 – 7th-8th Sep 2016, Frankfurt, Germany (attended)
- IFIP International Conference on New Technologies, Mobility and Security, 21st-23rd Nov 2016, Larnaca, Cyprus (attended)
- Annual Privacy Forum 2017 – 6th-7th June 2017, Vienna, Austria (will be attended)

B. Training

Research and Technical Training

- Introduction to PETs, August 2016 (Karlstad, Sweden)
- Privacy Enhancing Technologies, January 2017 (Online Module)
- Cyber Security Basics: A Hands-on Approach, March 2017 (Online Module)

Secondment Plan

Please see Annex 1

Interdisciplinary Training

- Privacy of Personal Health Data, August 2016 (Karlstad, Sweden)
- General Data Protection Regulation – Next Step?, August 2016 (Karlstad, Sweden)
- Introduction to Usability, August 2016 (Karlstad, Sweden)
- Legal Privacy Workshop – Privacy by Design, August 2016 (Karlstad, Sweden)
- The Future of Privacy and Identity Management, August 2016 (Karlstad, Sweden)
- Privacy’s wider context: Values in IT, August 2017 (Vienna, Austria)
- Economics of privacy, August 2017 (Vienna, Austria)

Professional Training

- Scientific Paper Writing, August 2016 (Karlstad, Sweden)
- Professional Networking, August 2016 (Karlstad, Sweden)

Other Training Activities

- Since the chair hosted both APF 2016 and IPEN 2016 (7th-9th Sep 2016, Frankfurt, Germany) I contributed with discussions and opinion related to the scientific sessions and had the opportunity to explain to the attendees about my research project by having a poster in the event.
- Getting feedback regarding the analysis done with regard to privacy requirements from a group of four master students at the Goethe University of Frankfurt (Sep 2016)
- Increasing impact of research results, August 2017 (Vienna, Austria)
- Peer Reviewing – Editor's view, August 2017 (Vienna, Austria)

C. *Networking Activities*

- First network wide event (25th-27th August 2016, Karlstad, Sweden)
- Attended APF 2016, and IPEN 2016 (7th-9th Sep 2016, Frankfurt, Germany)
- IFIP International Conference on New Technologies, Mobility and Security, 21st-23rd Nov 2016, Larnaca, Cyprus
- Attended a workshop on Next Generation of Online Anonymity, 1st- 2nd Dec 2016, Frankfurt, Germany
- Attended a 2 day workshop on Personalised Privacy by Default Settings with KDDI, 13th-14th Feb 2017, Frankfurt, Germany
- Second network wide event (30th May - 2nd June 2017, Vienna, Austria)

D. Research Management

There is no activity

E. Other activities

Other Activities (professional relevant)

Contributed as sub-reviewer in journals such as:

- Computer Networks (Granted recognised reviewer award, ELSEVIER)
- Wireless Personal Communications (Springer)
- Signal, Image, and Video Processing (Springer)
- Adhoc Journal (ELSEVIER)
- The Computer Journal (Oxford)

And conferences like:

- European Wireless 2017 (orgnised by IEEE), Dresden, Germany
  Link: http://ew2017.european-wireless.org/
- IFIP Sec 2017, Rome, Italy
  Link: http://ifipsec.org/2017/
- Annual Privacy Forum 2017, Vienna, Austria
  Link: http://privacyforum.eu/
- 2017 International Workshop on Privacy Engineering
  Link: http://www.ieee-security.org/TC/SPW2017/IWPE/index.html

VII. Signatures

Date & Signature of fellow Date & Signature of supervisor

Annex 1 Secondment Plan

1. Main Goal

The main goal is to investigate suitable HCI techniques to provide transparency and improve privacy awareness in smartphone ecosystems. To this end, and, as a continuation of ongoing research, the secondment will be focused on improving the usability aspects of the Android Apps Behaviour Analyzer (A3) and reporting tool. The aim of these tools is to make users aware of the privacy invasiveness of apps and help them to better understand the associated privacy implications. The tools also support users to easily control the permission related to those access and encourages them to potentially report privacy aggressive practices of apps. Having considering this fact, one goal is to find a way to balance the usability and privacy aspects of A3, and as a second goal to evaluate its acceptability and its actual effectiveness.

2. Expected Results

- A reliable framework which enables us to provide a flexible, efficient, and usable GUI that guarantees improved usability and improved privacy of A3;
- A reliable foundation to highlight the importance of psychological and technical aspects in designing of privacy indicators for smartphone apps;
- Designing and performing a first user study in order to figure out to which extent A3 tool is usable and effective. This study will be focus on validating the functionality of both our proposed GUI and the classified attributes (features) that we have extracted for the GUI.

3. Time Plan - 8 weeks

- Literature Survey (1 week)
- Design of a n-phase user study (2 weeks)
- Recruitment of participants and implementation of the first phase (2 weeks)
- Analysis of results and initial adjustments of the tool (1 week)
- Implementation of the second phase of the user study (1 week)
- Analysis of initial results (publication preparation) and road-map for future study phases (1 week)

References

[1] http://www.statista.com/statistics/281106/number-of-android-app-downloads-from-google-play/

[2] http://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/

[3] M. Nauman, S. Khan, and X. Zhang, ”Reconciling mobile app privacy and usability on smartphones: could user privacy profiles help?,” in Proceedings of the 23th International Conference on World Wide Web, China, pp. 201–212, 2014.

[4] P. G. Kelley, S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, and D. Wetherall, ”A conundrum of permissions: installing applications on an android smartphone,” in Proceedings of the 16th International Conference on Financial Cryptography and Data Security, Bonaire, pp. 68–79, 2012.

Usable Privacy in the Internet of Things and Smart Spaces

Alexandr Railean (ESR06), Unabhängiges Landeszentrum für Datenschutz (ULD)

Abstract. This document summarizes the planned research activities of ESR06 and the expected outcomes, covering a 3-year periodred[1]. The research is aimed to analyze, understand and suggest improvements in the field of usable privacy for the Internet of Things (IoT) and smart spaces. The need for such an analysis stems from the fact that the IoT undergoes a significant expansion around the world, thus it is important to consider the potential privacy implications of using such technology.

The document points out the facts which indicate that IoT goes through a rapid growth phase and refers to scientific literature that discusses the privacy-related issues raised by such technology. It also offers an overview of current attempts to address these privacy concerns.

Finally, this document lays out the proposed research approach, and explains how it is different from prior research.

1 Introduction

The Internet of Things (IoT) is composed of *"devices or sensors [...] - that connect, communicate or transmit information with or between each other through the Internet"* [8]. It is going through a rapid growth phase, as the number of connected devices is estimated [5] to increase from 25 billion in 2015 to 50 billion in 2020, while the number of connected devices[2] per person increased from 0.08 in 2003 to 1.84 in 2010 [5], and to 3.3 in 2016 [19].
As a result of this trend, a wide range of consumer-grade IoT devices such as light bulbs, power switches, air quality monitors or fitness trackers are available to a broad audience. Currently there are 402 ready for purchase retail products on Iotlist.co; and there is strong support for IoT in the "do it yourself" community - as of this writing, there are 21714 projects on Github.com and 49000 hits on Instructables.com when searching for "IoT".
Some major appliance manufacturers have committed to making their product line IoT-enabled, for instance Samsung's CEO stated that in 2020 *"... every single piece of Samsung hardware will be an IoT device, whether it is an air purifier or an oven."*[3]
A growing interest among end users is also supported by the frequency of the term *#iot* used in search queries, it has experienced a steady growth[4] over the past 5 years. Governments have expressed interest in IoT as well; for example, the FTC[5] issued a privacy and security guide [6] for businesses involved in IoT development, while the European Commission is working on regulations [17] that have provisions for IoT communications (the document you are reading right now is another indication of how much the EU is committed to the study of this issue). This indicates that IoT is on the path of becoming an indispensable part of our daily lives, having attracted the attention of enterprises, governments and end users.

The proliferation of IoT may inadvertently expose owners to privacy risks. They occur at the interplay of factors like (1) resource-constrained hardware, (2) poor usability, (3) deployment in locations with access to highly personal data (e.g. in a home or on the body) or (4) the availability of vast pools of data that facilitate deanonymization (i.e. the identification of users by linking multiple data points).

Studies show that information about a person can be derived by correlating data from disparate sources, such as smartphone sensors [11, 2], social media [10] or online reviews [13]. Research discussed in [13] yielded an approach for deanonymizing large data sets of multi-dimensional micro-data. To illustrate the predictive power of small bits of data, we can refer to a model [10] that uses social media "likes" to accurately differentiate *"between homosexual and heterosexual men in 88% of cases, African Americans and Caucasian Americans in 95% of cases, and between Democrat and Republican in 85% of cases."*

IoT devices have the potential to enhance the predictive power of such algorithms, feeding them with even more data that is intimately connected to a person's private life. The effect is amplified by the end users' lack of awareness - they do not suspect that information that appears trivial at the first glance, such as the temperature in their house, reveals a lot about

[2] This includes laptops, smartphones, tablets and PCs, not just IoT
[3] mashable.com/2015/01/05/samsung-internet-of-things/
[4] https://trends.google.com/trends/explore?q=iot
[5] Federal Trade Commission

them and their habits (e.g. when they are away from home, their daily routine, which room they are in, etc). Thus, if the growth of the number of IoT devices is not accompanied by an improved understanding of implications, protecting our privacy in the future will be even more challenging.

2 State of the art

There are several general perspectives that IoT-related research has taken:

- Technical - with an emphasis on protocols, algorithms and technical implementations thereof.
- User-centered - focusing on usability and interface design.
- Legal - focusing on what the legislation in different states has to say about privacy and how IoT can be regulated, the implications of the use of trans-national service providers.
- Similarities with related fields - such research draws on the experience from other contexts (e.g. location sharing in smartphones) and compares it with the IoT ecosystem.

Ziegeldorf, Morchon, and Wehrle performed a privacy-focused analysis of IoT in [22]. They define privacy as a set of three guarantees: (1) data subject's awareness of risks, (2) individual control over data collection and processing, (3) awareness of subsequent use and dissemination. A person's interaction with IoT devices is divided into several phases, referred to as information flows: (1) *interaction* - the data subject interacts with the device, either directly or indirectly, (2) *collection* - information is collected and transmitted, (3) *processing* - a backend analyses the data and potentially triggers some actions, (4) *dissemination* - information is sent back to the data subject and possible other parties, (5) *presentation* - when the surrounding smart things provide a service to the data subject. They identify the following privacy risks: (1) identification, (2) location tracking, (3) profiling, (4) privacy-violating interactions[6], (5) lifecycle transitions[7], (6) inventory attacks[8] and (7) linkage. Their work also includes a review of the legal basis, pointing out the deficiencies in current legislation.

Williams, Nurse, and Creese argue that the privacy paradox applies to IoT [20] and point out the contributing factors - usability and configuration, ubiquity and physicality, resource constraints, unfamiliarity and market forces. Further, they suggest approaches to handle these issues, namely improving user interfaces, simplifying privacy policies and rethinking the default settings.

Elkhodr, Shahrestani, and Cheung review the implications of location data sharing in the context of IoT [4], drawing on the experience from location privacy in smartphone ecosystems.

[6] E.g. a person getting feedback from a public smart space can be observed by passers-by.

[7] When IoT devices are resold or serviced by third parties - the owner's privacy can be violated.

[8] Fingerprinting other devices in a person's home, e.g. a burglar would benefit from knowing what sensors a target's home is equipped with.

They analyze the user interface and the user experience of apps (smartphone programs) that request permissions to detect and share the location. They conclude that IoT location privacy is more complex, given that location data can be transmitted via device-to-device communication without a person's awareness. This effect is amplified by the fact that enormous amounts of telemetry data points are generated, facilitating correlation via data mining.

Exploratory research by Minch [12] digs deeper into the big data aspect of IoT, by looking at *volume* - how much information is accumulated, *velocity* - how fast it grows, and *variety* - diversity of data sources. Further, the author devises a taxonomy of IoT information flows, based on the following phases: sensing, identification, storage, processing, sharing and use. For each phase, some technical, social and legal privacy controls are suggested as starting points.

Peppet provides a comprehensive overview of the legal aspects of IoT in [14], identifying four main problems: discrimination, privacy, security and consent. The author highlights several issues, for example the threat of de-anonymization via correlation of sparse data sets makes the definition of "personally identifiable information" of limited use[9]; lack of privacy policies[10].

Other resources are focused on the security of IoT, as these are the low-level primitives that are required for privacy protection. For example, the FTC (Federal Trade Commission of the USA) published a guide for IoT vendors [6] that addresses basics such as rate-limiting or secure default passwords. While these best practices of security are not related to privacy per se, they must be implemented - otherwise other measures to protect privacy are futile.

Further on the technical spectrum, Wu et al. analyze protocols for IoT device discovery, with a focus on the privacy aspects [21]. They cite a study [9] that found that "59% of all devices advertise their owner's name in the clear, which is considered harmful by more than 90% of the owners", which has obvious privacy implications. Their work establishes the desired features for a privacy-preserving discovery protocol: mutual privacy, authentic advertisements, no out-of-band pairing for participants, no cloud dependency during protocol execution. The proposed protocol that combines these qualities is available as an open-source implementation.

Fernandes, Jung, and Prakash analyze the security of Samsung's ”SmartThings” platform, and succeed in exploiting the vulnerabilities they discovered [7]. This enabled the research team to accomplish things like adding new door lock codes, which would allow a burglar to effortlessly enter a target's home. These prospects are especially worrying, given the statements of Samsung's CEO, referenced in the introduction.

A survey by the Pew Research Center [15] interviewed 1867 experts and other stake-holders, asking them about the future of privacy in the context of IoT. There is a great diversity in points of view, though several patterns have emerged. Most interviewees believe that by 2025

[9] Some scholars argue that in these circumstances the concept of PII should be dropped altogether, whereas others propose a refined definition along a spectrum.

[10] The author purchased and examined 20 IoT devices and none of them included privacy-related information in the box, nor did they refer to such information on the manufacturer's web-site.

IoT will become “A global, immersive, invisible, ambient networked computing environment built through the continued proliferation of smart sensors, cameras, software, databases, and massive data centers in a world-spanning information fabric” and that there will be “tagging, databasing, and intelligent analytical mapping of the physical and social realms”. Further, the survey participants identified the following areas where IoT will play an important role: bodies, homes, communities, goods and services, the environment.

Atzori, Iera, and Morabito published a survey of the IoT [1], highlighting its enabling technologies, applications and open issues, identifying privacy as one of them. The authors point out that for (1) IoT devices that lack a user interface - providing a notice and eliciting consent is a challenge. The suggestion is to collect coarse data (less precision in scanners, blurring people's faces in video recordings, etc). Another referred solution is a (2) “privacy broker” that would negotiate a person's privacy preferences with an automated system. The survey also raises the concern of digital forgetting - the capability to assure that after a period of time certain information will be deleted.

The proposed approach differs in several ways from the related research. First of all, unlike the data-centered phases suggested in [22] and [12], where the information flow focuses on what happens to one's data, we take a *user-centered* approach, focusing on what a person does with an IoT device in various phases of the device lifetime. By concentrating on how people interact with the hardware, we directly explore the usability component of the interaction. Second, we place an emphasis on consumer-oriented IoT product prototypes, therefore the research should yield results that are more likely to have immediate benefits for a general audience. Thirdly, we consider the legal aspects from the perspective of the GDPR, with an emphasis on the following protection targets: transparency, intervenability and unlinkability.

3 Proposed approach and methodology

In accordance with the *grant agreement*, the research targets three main privacy protection goals: unlinkability, transparency and intervenability.

My intention is to focus on consumer-oriented IoT devices, because they are directly handled by people. Smart spaces are treated as a special case of IoT, where ”things” are embedded into the environment. I intend to focus on spaces that are accessible to the general public (e.g. in squares, parks, gallerias or installed in their households).

At this point my research has brought me to the study of privacy attitudes throughout the lifecycle of an IoT device. The cycle is divided into the following main stages and the transitions between them (marked with green in 1):

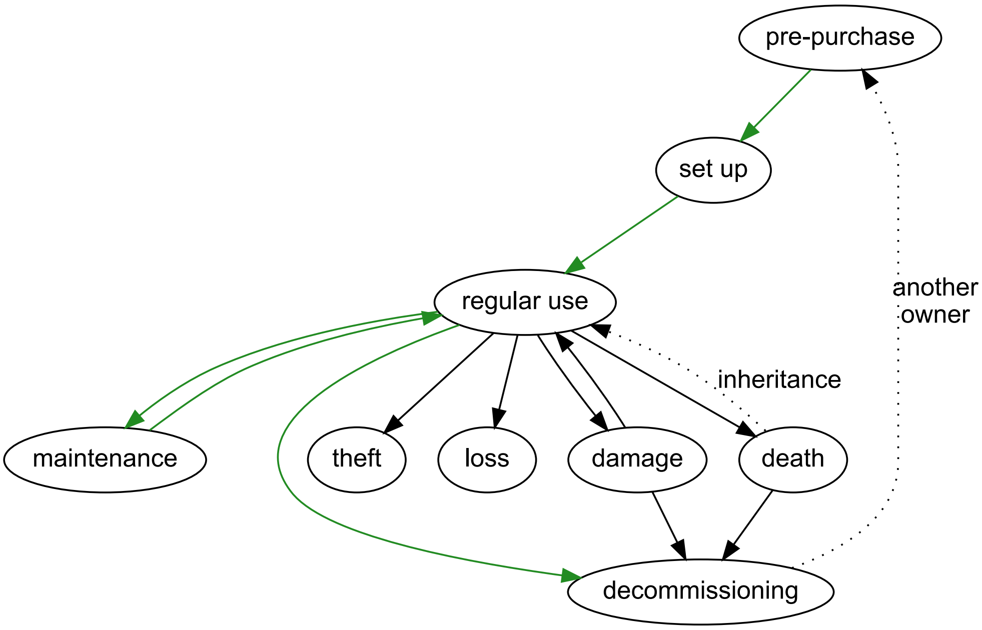
- Pre-purchase - choosing a device out of a set of candidates
- Set-up - setting up the device and programming its behaviour
- Usage - normal device operation
- Maintenance - updating the device to address new issues

- Decommissioning - what happens when the device is sold or given to someone else

A full lifecycle addresses additional scenarios that can occur: loss, theft, damage and death. In each of these cases, an IoT device can end up in wrong hands, which could violate the privacy of the original owner or that of other people they have interacted with.

The complete cycle includes several loops, to accommodate the possibility that a decommissioned device becomes someone's new purchase (e.g. after refurbishing, or a resale).

Figure 1: IoT device life-cycle



Further, the main privacy protection goals are projected onto this lifecycle.

Here is an example that illustrates the utility of understanding privacy attitudes. If we answer the question *"do people think about privacy before they purchase a device, or does this become an issue only in a subsequent stage?"* we can determine which ways of increasing privacy awareness are more appropriate. If there is no awareness of it before the purchase, it means that later the person will deal with the consequences[11] of using a device that violates their privacy. Factors such as loss aversion or procrastination might convince people to take the path of minimum resistance and leave things as they are (which hinders privacy). If, on the other hand, privacy is on people's radars in the pre-purchase phase, what makes them choose devices that are known to have a bad reputation when it comes to privacy? Is it because people didn't know about it? Or did they buy it despite having that awareness? If so - what made them do it? Was it because of a cognitive bias? A misinterpretation of the factual information they had at their fingertips?

Asking, analyzing and answering such questions enables us to examine (and hopefully understand) human nature, then find ways to balance the technical benefits of IoT and the privacy

[11] Much like the difference between preventive and curative medicine

of an individual and society as a whole.

To this end, an online-based study was launched in April and it is currently collecting data from participants. The information will be used to create a more detailed map of privacy in each of the aforementioned phases.

These phases form the skeleton of my planned dissertation - it will be a comprehensive guide on usable IoT privacy; device manufacturers, legislators or hobbyists can rely on it to make sense of the context and make informed decisions based on my findings.

3.1 Planned prototypes

The experimental side of this research will revolve around a basic IoT device - a *temperature and humidity sensor*. This device starts from a hypothetical construct, then it is gradually refined on its way towards an actual, tangible artifact. Multiple variations of the product will be created to conduct A/B tests and explore the difference in people's attitudes towards each version.

- Imaginary prototype - a product with some hypothetical features that will be described and illustrated in on a pseudo-store on the Internet. The intention is to observe which ones are preferred by prospective buyers and find the rationale behind their choice. This will provide insights into the *pre-purchase* phase of the IoT lifecycle model. I will explore what factors contribute to a person's purchase decision (e.g. privacy-related labels, icons, reviews, price, etc). This phase will most likely be conducted online.
- Paper prototype - people will be invited to interact with paper prototypes of several variations of the device, enabling us to examine the *set-up* phase of the lifecycle. At this point we will determine how to best convey the information needed to ensure transparency, in accordance with the GDPR. For now, the proposed method is to expose participants to different variations of the IoT device design and let them interact with it, then ask questions about its behaviour via a survey[12]. The data will indicate which representation method was best-understood. The same participants will be asked similar questions (phrased in a different way) later, to see if their knowledge has degraded over time, or if their attitudes have changed.
- Software prototype - instruments such as Kivy and PyQt will be used to create a graphical interface that mimics the behaviour of an actual IoT device.
- Hardware prototype - an actual device implementation based on development boards such as *Microbit* or *RaspberryPi*.

The last two prototype categories will be used to get a better view on the *regular use*, *maintentance* and *decommissioning* phases of the life-cycle; they also provide the chance to see how to best implement *intervenability* and *unlinkability*.

[12] Very similar to how a teacher would assess if their pupils understood a subject, but without the psychological pressure

3.1.1 Information efficiency

Attempting to understand what interface is the best choice for conveying information to the end user will be done in accordance with the tenets of information efficiency [16]. At first we shall establish what the actual amount of information that has to be shared with end-users is, then we will measure how much information each prototype actually transmits through its interface. These results will be used to calculate the information efficiency of an interface (by analogy with the efficiency of an internal combustion engine), which will then indicate whether we can do better.

3.1.2 Question-oriented UI design

When constructing prototypes and their control interfaces, the starting point will be a list of questions that people are asking themselves while interacting with a device. Once this list of questions is established, we can ensure that the UI does not contain redundant information, and does not attempt to tell people more than what they need to know.

Variations in visualization will be used to understand how well the interface is perceived by users, including non-tech-savvy ones. For example, suppose that a survey revealed that the end users ask themselves the following questions during the set-up phase:

1. What information is this device transmitting into the cloud?
2. How often are data transmitted?

One interface can answer them by writing a label on the screen that says “the device reads your temperature and transmits it to the cloud every 5 minutes”. An alternative implementation will say the same, but also include a data sample, e.g. “March 20th 15:23, 30 °C, 40%” - which of them provides the clearest answer to the person’s questions?

The same ideology will be applied to ensure that the interface does not say more than what it was asked for. An example - suppose the interface also has a paragraph that says “The data are transmitted in encrypted form, with military-grade, 1945-bit quantomorphic keys”. On one hand, this makes the device seem very sophisticated, but should this information be mentioned, given that our initial survey revealed that people are not asking themselves this question?

3.1.3 Goal-oriented UI design

Another approach would address the problem from the opposite direction - we start by making a list of important points that a person must be aware of as they interact with the device, e.g. what is transmitted, how it is transmitted, where it will be stored, how it will be used and who will have access to it.

These are the questions a person *should* have the answer to at the time of consent. Different interface prototypes will answer these questions in different ways, then we shall compare which prototype provided better results. Attention shall be paid to immediate results, i.e. what the person understood right away, as well as a long-term perspective (what people still remember after a time period).

3.2 Basic principles

These principles constitute the foundation of the research:

- *empiricism* - conduct experiments that provide an opportunity to collect data, and derive conclusions from it
- *human interaction* - experiments should involve human subjects, as humans are the ultimate end-users of the output of my research
- *rapid prototyping* - construction of low-fidelity paper-prototypes, with a gradual transition to software interfaces or hardware gadgets when ideas reach maturity
- *behaviour* - learn from actual behaviour and held beliefs, rather than from stated preferences and goals
- *cross-disciplinary research*

3.2.1 Empiricism

My vision is to base findings on data that can be quantified and compared, drawing conclusions that anyone else can double-check and test, by replicating the experiment and (hopefully) reaching the same conclusion.

To facilitate this, all the experiments are to be accompanied by detailed descriptions on how to set up a test environment and replicate the results (very similar to ”howto” guides for software deployment). This also implies that all the custom-written software tools that are developed for these purposes have be made available to the public, to minimize the effort required to rerun an experiment.

3.2.2 Human interaction

Given that the focus of my research is usable privacy, it is important to involve end-users of such technology in order to validate the results. This becomes especially important when studying *transparency* and *intervenability*. These targets cannot be adequately protected, unless people understand how their data are acquired and processed, and unless they are aware of the implications of their choices.

This involvement can be of different types:

- surveys
- interviews
- observing people interacting with a prototype
- eye-tracking
- A/B testing

- psychometrics

I would like to place an emphasis on A/B testing, because it makes it easy to apply incremental improvements to an idea and quickly compare the results.

3.2.3 Rapid prototyping

Paper-based prototypes are a cost-effective way to test an idea for an interface and determine its strengths and shortcomings. After several iterations, higher-fidelity prototypes will be constructed, by leveraging my (strong) software and (intermediate) hardware engineering skills. This would make the experiment more attractive to the participants, due to the hands-on nature of the interaction, as they are not dealing with hypothetical scenarios - but with tangible artifacts. This also strengthens the link with the Human interaction element - offering diverse opportunities to collect measurable data. Ideally, I would like to cooperate with industry partners and gain more experience of this type.

3.2.4 Behaviour

Although it is a sub-component of Human interaction, this aspect requires a separate discussion. Drawing on the experience of the field of behaviour economics [18, 3], we know that people's real life behaviour is influenced by their cognitive biases and beliefs. We routinely ignore objective evidence that is produced by science, even when it is against our own interests.

It is not sufficient to demonstrate that something is true; if we want to encourage certain behaviour (e.g. privacy-conscious decisions), we should take additional steps towards that.

Thus, to avoid the trap of doing research about *"perfectly spherical horses moving through a vacuum"*, I intend to apply the knowledge I have from the field of cognitive psychology, and ideally - have joint projects with researchers who are experienced in this area.

3.2.5 Cross-disciplinary research

This is the foundation of my approach - I hope that there will be opportunities to run joint experiments with other ESRs, giving me a chance to learn from them and share whatever knowledge I have.

The most important cross-disciplinary component is continuous attention to the legal aspects, given that my host institution is an organization specialized in such matters. Thus, it is expected that the results of the research will be in tune with the requirements of the GDPR.

3.3 Future applications

Technological progress will inevitably bring us to a stage when space exploration[13] will become the norm. In those circumstances, humans will live in extremely complex environments, the complexity being a prerequisite for maintaining habitable conditions. It is extremely important to have detailed telemetric data about the environment (e.g. temperature, pressure, concentration

[13] This applies to life in exploration habitats at the bottom of seas

of various gases, etc) as well as its occupants (e.g. heart-rate, pulse-oxymetry, psychological state, and so on).

This will be in direct conflict with the human need for privacy. How shall these be reconciled? I hope that my research about IoT and smart spaces will address present day challenges, but also set the foundation for the distant future.

4 On dissemination

An important component of my approach is to produce materials that appeal to a broad audience, attracting the interest of the general public, especially young people. The inspiration for this comes from scientists like Richard Feynman, Carl Sagan, Richard Dawkins or Brian Cox; their ability to wrap complex subjects into a clear message influenced me very much.

A step towards this goal is to produce ”plain English”, illustrated summaries of my findings. Another instrument is the commitment to lower the entry barrier for the use of any software that is written in the context of my research (e.g. by including ”howto” guides or demonstration screencasts), thus encouraging hobbyists to participate in science

5 Work plan

In the timeline below, the timestamps are relative to the beginning of the Privacy & Us project (i.e. M1 is December 2015, M9 is August 2016, etc).

Timeline	Activity	Notes
M9 - M14	Literature review	This is a continuous process, that will extend the accumulated knowledge beyond M14.
M12 - M14	Explorative study	Assess the potential of using social media and public web-resources for gauging privacy attitudes towards IoT, including both - vendors and end users.
M13 - M14	Uniscon secondment	Familiarization with the “sealed cloud” concept pioneered by Uniscon.
M15 - M20	Survey	Online survey to evaluate the attitudes towards privacy throughout the lifecycle of IoT devices.
M20	First publication	A paper based on the findings of the study, submitted to the IFIP summer school.
M15 - M20	Contribute to D5.1	An analysis of the legal aspects of IoT with respect to the protection targets stipulated by the GDPR.
M16 - M18	Contribute to D4.1	An analysis of usability requirements for the IoT.
M21 - M26	Karlstad secondment	Build and evaluate IoT device prototypes, aiming to understand whether end-users are aware of what happens to their collected data and in what ways the data are subsequently processed.
M33 - M34	Usecon secondment	
M39	Write thesis	
M44	Thesis submission	

Table 1: Planned activities

References

[1] Luigi Atzori, Antonio Iera, and Giacomo Morabito. “The Internet of Things: A survey”. In: *Computer Networks* 54.15 (Oct. 2010), pp. 2787–2805. ISSN: 13891286. DOI: 10.1016/j.comnet.2010.05.010. URL: http://linkinghub.elsevier.com/retrieve/pii/S1389128610001568 (visited on 06/06/2017).

[2] Delphine Christin. “Privacy in mobile participatory sensing: Current trends and future challenges”. In: *Journal of Systems and Software* 116 (June 2016), pp. 57–68. ISSN: 01641212. DOI: 10.1016/j.jss.2015.03.067. URL: http://linkinghub.elsevier.com/retrieve/pii/S0164121215000692 (visited on 10/20/2016).

[3] Julie Downs, Jessica Wisdom, and George Loewenstein. "Simple Strategies For Communicating Health Information". In: *NA-Advances in Consumer Research Volume 38* (2011). URL: `http://www.acrwebsite.org/volumes/v38/acr_v38_16228.pdf` (visited on 11/28/2016).

[4] Mahmoud Elkhodr, Seyed Shahrestani, and Hon Cheung. "A Review of Mobile Location Privacy in the Internet of Things". In: *ICT and Knowledge Engineering (ICT & Knowledge Engineering), 2012 10th International Conference on*. IEEE, 2012, pp. 266–272. URL: `http://ieeexplore.ieee.org/abstract/document/6408566/` (visited on 05/14/2017).

[5] Dave Evans. *The Internet of Things - How the Next Evolution of the Internet Is Changing Everything*. Cisco, Apr. 2011. URL: `http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf` (visited on 04/25/2017).

[6] FTC Federal Trade Commission. "Careful Connections: Building Security in the Internet of Things". Jan. 2015. URL: `https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf` (visited on 05/02/2017).

[7] Earlence Fernandes, Jaeyeon Jung, and Atul Prakash. "Security Analysis of Emerging Smart Home Applications". In: IEEE, May 2016, pp. 636–654. ISBN: 978-1-5090-0824-7. DOI: `10.1109/SP.2016.44`. URL: `http://ieeexplore.ieee.org/document/7546527/` (visited on 04/27/2017).

[8] *Internet of things: Privacy & Security in a Connected World*. Staff report. FTC, Jan. 2015. URL: `https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf`.

[9] Bastian Könings et al. "Device names in the wild: Investigating privacy risks of zero configuration networking". In: *Mobile Data Management (MDM), 2013 IEEE 14th International Conference on*. Vol. 2. IEEE, 2013, pp. 51–56. URL: `http://ieeexplore.ieee.org/abstract/document/6569062/` (visited on 06/13/2017).

[10] M. Kosinski, D. Stillwell, and T. Graepel. "Private Traits and Attributes Are Predictable From Digital Records of Human Behavior". In: *Proceedings of the National Academy of Sciences* 110.15 (Apr. 9, 2013), pp. 5802–5805. ISSN: 0027-8424, 1091-6490. DOI: `10.1073/pnas.1218772110`. URL: `http://www.pnas.org/cgi/doi/10.1073/pnas.1218772110` (visited on 05/08/2017).

[11] Nicholas D. Lane et al. "On the Feasibility of User De-anonymization From Shared Mobile Sensor Data". In: *Proceedings of the Third International Workshop on Sensing Applications on Mobile Phones*. ACM, 2012, p. 3. URL: `http://dl.acm.org/citation.cfm?id=2389151` (visited on 04/27/2017).

[12] Robert P. Minch. "Location Privacy in the Era of the Internet of Things and Big Data Analytics". In: IEEE, Jan. 2015, pp. 1521–1530. ISBN: 978-1-4799-7367-5. DOI: `10.1109/HICSS.2015.185`. URL: `http://ieeexplore.ieee.org/document/7069994/` (visited on 05/14/2017).

[13] Arvind Narayanan and Vitaly Shmatikov. “How to Break Anonymity of the Netflix Prize Dataset”. In: *arXiv preprint cs/0610105* (2006). URL: https://arxiv.org/abs/cs/0610105 (visited on 04/27/2017).

[14] Scott R. Peppet. “Regulating the internet of things: First steps toward managing discrimination, privacy, security and consent”. In: *Tex. L. Rev.* 93 (2014), p. 85. URL: http://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/tlr93&section=5 (visited on 10/17/2016).

[15] Lee Rainie and Janna Anderson. *The future of privacy*. Pew Research Center. Washington, 2014. URL: http://cm.1-s.es/~admissions/12-2014/future-of-privacy.pdf (visited on 10/17/2016).

[16] Jef Raskin. *The humane interface: new directions for designing interactive systems*. 13. print. OCLC: 797157885. Boston: Addison-Wesley, 2011. 233 pp. ISBN: 978-0-201-37937-2.

[17] *REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*. Jan. 2017. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN (visited on 05/02/2017).

[18] Uri Simonsohn and Dan Ariely. “When Rational Sellers Face Nonrational Buyers: Evidence from Herding on eBay”. In: *Management Science* 54.9 (Sept. 2008), pp. 1624–1637. ISSN: 0025-1909, 1526-5501. DOI: 10.1287/mnsc.1080.0881. URL: http://pubsonline.informs.org/doi/abs/10.1287/mnsc.1080.0881 (visited on 11/28/2016).

[19] *Trends 17*. Globalwebindex, 2016. URL: http://insight.globalwebindex.net/hubfs/Reports/Trends-17.pdf (visited on 04/25/2017).

[20] Meredydd Williams, Jason RC Nurse, and Sadie Creese. “The perfect storm: The privacy paradox and the Internet-of-Things”. In: *Workshop on Challenges in Information Security and Privacy Management at the 11th International Conference on Availability Reliability and Security (ARES). IEEE*. 2016. URL: http://www.cs.ox.ac.uk/files/8366/ARES2016-author-final.pdf (visited on 10/31/2016).

[21] David J. Wu et al. “Privacy, Discovery, and Authentication for the Internet of Things”. In: *arXiv preprint arXiv:1604.06959* (2016). URL: http://arxiv.org/abs/1604.06959 (visited on 10/31/2016).

[22] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, and Klaus Wehrle. “Privacy in the Internet of Things: Threats and Challenges”. In: *Security and Communication Networks* 7.12 (Dec. 2014), pp. 2728–2742. ISSN: 19390114. DOI: 10.1002/sec.795. URL: http://doi.wiley.com/10.1002/sec.795 (visited on 05/14/2017).

Career Development Plan Year 1
ESR 6 Alexandr Railean

I. Personal and Organizational Information

ESR´s Personal Information			
Name:	**Alexandr Railean**	**ID number**:	
Office Address:	Unabhängiges Landeszentrum für Datenschutz, Holstenstr 98, 24143 Kiel	**Phone**:	+49-431-988-1285
Mobile:	+1-443-351-7987	**E-Mail:**	uld610@datenschutzzentrum.de

ESR´s Host Organization Information			
Name:	Unabhängiges Landeszentrum für Datenschutz	**Phone**:	+49-431-988-1200
Address:	Holstenstraße 98, 24143 Kiel, Germany		
***If enrolled organization is different from host organization, please specify:**			
Name:		**Phone:**	
Office Address:			

II. Supervision

Supervision			
Supervisor´s Name:	**Delphine Reinhardt**	**Title**:	Jun.-Prof. Dr.-Ing.
Place of Employment:	University of Bonn	**Phone**:	+49-228-73-60551
Responsibility Distr.:	Academic guidance	**E-Mail:**	delphine.reinhardt@cs.uni-bonn.de
Co-Supervision			
Co-Supervisor´s Name:	**Harald Zwingelberg**	**Title**:	
Place of Employment:	Unabhängiges Landeszentrum für Datenschutz	**Phone**:	+49-431-988-1222
Responsibility Distr.:	Reviews of written materials, legal advice	**E-Mail:**	uld6@datenschutzzentrum.de
Conduct of Supervision (per activity describe form of supervision and estimated supervision hours)**:**			

Supervision is carried out in mainly via interactions over email, ad-hoc phone conferences, occasional face to face meetings, as well as collaborative paper editing

The approximate time dedicated to the meetings is 60 hours per 12 months.

III. Secondment

ESR´s Secondment			
Supervisor's Name:	**Hubert Jäger**	**Position**:	
Organization´s Name:	**Uniscon GmbH**	**Phone**:	+49-1525-318-2209
Address:	Agnes-Pockels-Bogen 1, 80992 München, Germany	**E-mail:**	hubert.jaeger@uniscon.net

IV. Research Project

ESR´s Project			
Title:	**Usable privacy in the Internet of Things and smart spaces**	**Ref. No:**	6

Overview and background

The Internet of Things (IoT) is composed of *"devices or sensors - other than computers, smartphones, or tablets - that connect, communicate or transmit information with or between each other through the Internet"*. It is going through a rapid growth phase, as the number of connected devices is expected to reach 50 billion in 2020. Many consumer-grade IoT devices such as light bulbs, power switches, air quality monitors or fitness trackers are available to a broad audience.

Such products may expose owners to privacy risks that occur at the interplay of factors like resource-constrained hardware, poor usability, deployment in locations with access to highly personal data or the availability of vast pools of data that facilitate deanonymization.

Smart spaces are a special case of IoT, where the technology is embedded into the surrounding environment. This creates additional challenges, such as handling the interaction with a large flux of people moving through a public place.

It is important to address these privacy issues before Pandora's box is open, because otherwise the cost of dealing with them will be far greater.

V. Long-Term Career Objectives

Long-Term Career Objectives (over five years)

Five years from now I plan to return to my earlier activities (software engineering and lecturing at a university), but with an extended arsenal of skills.

Specifically, I plan to learn how to conduct usability studies that involve observing end-users, A/B testing, surveys, psychometrics and rapid prototyping. This will help me take my projects to the next level. In addition to that, I hope I will be able to continue publishing papers based on my continued research.

I am open to other ideas as well and I am sure that as Privacy&Us progresses, other opportunities will arise.

VI. *Short-Term Career Objectives*

A. *Project Research Results*

Project Research Results

Presented according to Privacy & Us project Plan.

Milestones	Expected Results
Research Plan and CDP	Clear identification of project goals, research approach and methodology.
Continuous literature review	Stay up to date with current research and keep an eye on emerging trends
M14	Complete first secondment, understand the concept of a sealed cloud
M18	Contribute to D4.1
M20	Finish collecting and processing data from my IoT privacy survey and prepare materials for a publication
M21	Make a plan for my upcoming secondment

Deliverables

WP4 Interaction Design
D4.1 User Interface Requirements (M18)
This report includes my contribution with an analysis of requirements for IoT and smart spaces, to ensure they are usable and privacy-friendly.

WP5 Risk Analysis, Risk Perception and Law
D5.1 Privacy Principles (M20)
The report offers an analysis of legal implications that concern the research areas of several other ESRs.

Failed or stalled endeavours
So far I have had several projects that were not successful, so they did not yield any deliverables per se; however, I will list them here because failure is also a way to learn:

- Perception of IoT via sentiment analysis of data from Twitter
- A study of awareness of IoT privacy issues among end users, via the analysis of product reviews on Amazon
- Analysis of privacy-related details given by IoT manufacturers on their product pages on Amazon.

In the projects above I have written initial versions of software that would collect and analyse the data; however, these endeavours were frozen because of complicated and non-research-friendly terms of use on the aforementioned resources.

Anticipated Publications

- **IFIP summer school 2017 –** a paper that examines privacy attitudes throughout the life-cycle of an IoT device (submission deadline 15th May 2017)

Anticipated Conference/Workshop Attendance & Courses/Seminar Presentations

Past events/conferences attendance:

- *IFIP Privacy and Identity Management Summer School 2016* (Karlstad, Sweden 21—26 August 2016)

Future conferences/workshop attendance:

- *IFIP Summer School on Privacy and Identity Management* (Ispra, Italy, 4-8 September 2017)

B. Training

Research and Technical Training

- **Privacy Enhancing Technologies online training (Privacy&Us)**

Secondment Plan

- For my first secondment – the plan was to understand the sealed cloud concept and its benefits (when compared to a traditional cloud).
- The second secondment – the plan is yet to be defined, it will be a function of my current research results.

Interdisciplinary Training

- **A global view of legal aspects of privacy and information privacy** (Privacy&Us 1st Training)
- **Privacy in eHealth** (Privacy&Us 1st Training)

Professional Training

- **Scientific paper writing & publication process** (Privacy&Us 1st Training)
-

Other Training Activities

- **Learning the German language** (University of Kiel) – no points

C. *Networking Activities*

- **IFIP Summerschool 2016 and Privacy&Us training event in Karlstad**
- **Privacy&Us training event, Vienna, May 2017**

D. *Research Management*

E. *Other activities*

Other Activities (professional relevant)

- Self-study (via online courses and books) of tools related to scientific data analysis:
  - NLTK – natural language toolkit for Python
  - Pandas – Python data analysis library
- Learned how to use LaTeX to write scientific papers
- Interacting with the group of hardware/software enthusiasts from a hackerspace in Kiel
- Familiarized myself with the *sealed cloud* concept (during my secondment)
- Participated in the authoring of a paper (though it was not accepted, I learned a lot from the process)

VII. *Signatures*

Date & Signature of fellow

Date & Signature of supervisor

Juan Quintero (ESR07), Uniscon GmbH (UNI)

Ph.D. Research Proposal

EU H2020 - “Privacy&Us”

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

Juan Quintero

Supervisor: Dr. Zinaida Benenson
Industrial Supervisor: Dr. Hubert Jäger
Co-supervisor: Dr. Ben Wagner

Department of Computer Science
Friedrich-Alexander-University of Erlangen-Nurnberg
Erlangen, Germany

June 2017

Table of Contents

Abstract

This document describes an outline of the research of ESR7 in the Privacy&Us project on “The Role of Sealed Cloud Concept and Technology in User Acceptance and Usability of Privacy Applications”. The research aims to study the impact of Sealed Cloud on the usability and user acceptance of privacy-sensitive applications, when these applications are built using this technology.

In this research, the finals goals are to build a user acceptance model, based on identified user acceptance factors,and write recommendations on how to improve the usability and user acceptance of privacy application using Sealed Cloud. The user acceptance model will contribute to understanding of the impact of Sealed Cloud.

Introduction / Motivation

This Ph.D. project has been focused on the impact of Sealed Cloud technology (Jäger et al., 2014) on the user acceptance of privacy-sensitive applications, when these applications are built using this technology. According to Figure 1, to reach this main goal, a concrete privacy-sensitive application scenario will be chosen. Considering the use of Sealed Cloud within the chosen scenario, a user acceptance model (Benenson et al., 2015, p. 13) will be developed.

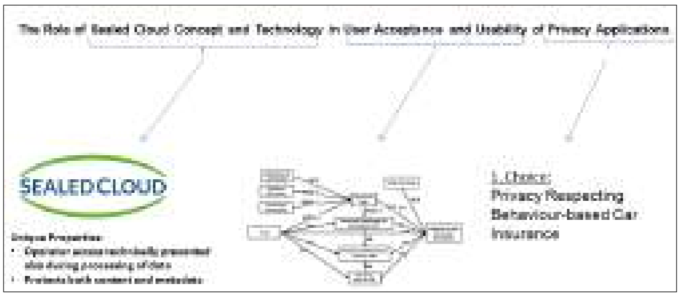

The Role of Sealed Cloud Concept and Technology in User Acceptance and Usability of Privacy Applications
SEALEDCLOUD
Unique Properties:
Operator access technically prevented also during processing of data
Protects both content and metadata
1. Choice:
Privacy Respecting Behaviour-based Car Insurance

Figure 1.Explanation of ESR7 project title

Sealed Cloud is a technology developed by Uniscon GmbH that can be used as a building block for privacy applications. It implements a tamper-proof execution environment with strong perimeter security; where trustworthy behaviour of the cloud operator is encouraged through division of power.

To choose the privacy application scenario, a review of existing privacy respecting Uniscon GmbH projects was conducted. The main goal of this review was to choose a privacy-sensitive scenario where privacy enhancing technologies can help resolving privacy issues. The scenario chosen is usage-based car insurance (UBI) (Soleymanian et al., 2016; Dijksterhuis et al., 2016), which is already a popular and widely deployed scenario in different countries (Troncoso et al., 2011). Figure 2 shows a system model for UBI, where networked cars drive through the streets using their sensors and cameras, collecting personally identifiable information (PII) and non-PII data, such as: 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 sensitive information, which may result in end-user privacy concerns.

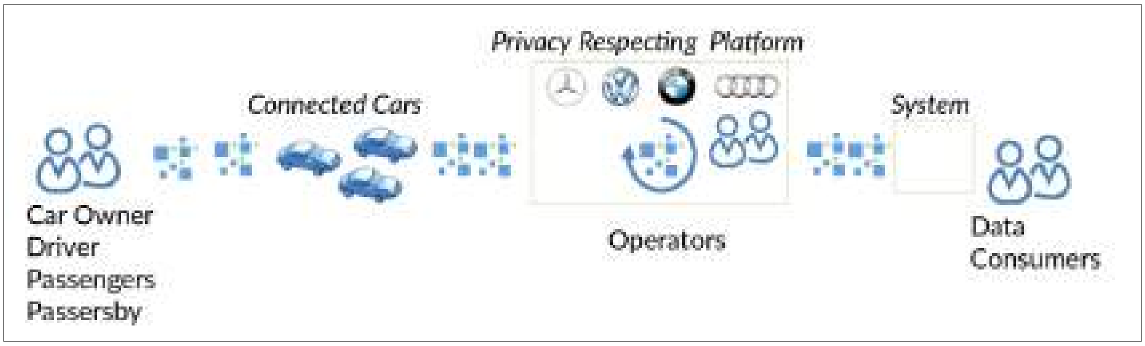


Figure 2.Connected Car system model

In this scenario, the insurance company could analyse the collected user data to find out behaviour patterns (driving style, speed, etc.) and reward the drivers for safe driving habits with new offers or discounts. The effort for privacy-preserving analysis and management of user data is higher without using PETs. To reduce this effort, using Sealed Cloud is one option.

To determine the Sealed Cloud impact in the user acceptance it is necessary to developa user acceptance model for UBI, based on identified user acceptance factors.To this end, a literature review is being conducted on Usage-based Insurance (UBI), insurance telematics, and user acceptance models. These activities are grouped in the Workspackage 3 (Model of Behaviour). The task of understanding Sealed Cloud technology and its usability aspects are being conducted in the Workspackage 2 (Technology Design and Development) and Workspackage 4 (Interaction Design), respectively.

At the end of this project, guidelines for user acceptance of the Sealed Cloud technology in the privacy respecting UBI scenario will be developed. These recommendations will further be generalized to the usage of the Sealed Cloud technology in other privacy-respecting applications.

Background

Technology Acceptance Model

Technology Acceptance Model (TAM) is a model to predict information technology acceptance and the users behavioural intention to use a technological innovation. TAM was proposed by Davis (1989), using two core constructs:

- *Perceived Usefulness* is"the degree to which a person believes that using a particular system would enhance his or her job performance" (Davis 1989, p.320).
- *Perceived Ease of Use* is"the degree to which a person believes that using a particular system would be free of effort" (Davis 1989, p.320).

TAM is based on the theory of reasoned action (TRA) (Fishbein & Ajzen, 1975). The origin of TRA is in the social psychology involving a main core constructs the Attitude toward behaviour, which is defined as: "an individual's positive or negative feelings (evaluative affect) about performing the target behaviour" (Fischbein & Ajzen, 1975, p.216).

Sealed Cloud

Sealed Cloud is a technology developed by Uniscon GmbH that can be used as a building block for privacy applications. It implements a tamper-proof execution environment with strong perimeter security, where trustworthy behaviour of the cloud operator is encouraged through division of power. This means that the operator can only access and modify the system with the help of a trusted third party (e.g., an accredited independent auditor).

Usage-Based Insurance

Usage Based Insurance (UBI) is a car insurance based on telematics. Telematics is defined as: “the use of computers to receive, store, and distribute information over atelecommunications system” (Zhao, 2002, p.10). Insurance telematics is a field within telematics, which is based on dynamic measures such as braking style, location, driving time, etc., that allow to establish the risk profile of the driver.

Pay-as-you-drive (PAYD), pay-how-you drive (PHYD), manage-how-you-drive (MHYD) among others are UBI models defined within insurance telematics (Handel et al, 2014).

State of the art

Models of technology acceptance have been studied by many authors, proposing a varieties of models, such as TAM and UTAUT, among others (Venkatesh et al., 2012; Benenson et al., 2015; Dillon & Morris, 1996). Most of these models do not consider privacy as acceptance factor. However, two models presented below integrate security and privacy issues into their technology acceptance models, and therefore will serve as a starting point for my research.

Benenson et al.,(2015) describe a theoretical development of a user acceptance model for anonymous credentials, proposing a model that extends the Technology Acceptance Model (TAM) with five new constructs: Perceived Usefulness for the Primary Task, Perceived Usefulness for the Secondary Task, Situation Awareness, Perceived Anonymity and Understanding of the PET. Its validation is conducted in a real-world trial. This model is shown in Figure 3.

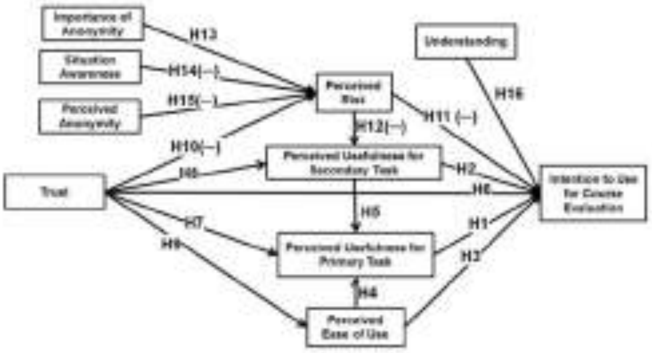


Figure 3.Research model for user acceptance of Privacy-ABCs for course evaluation(Benenson et al.,2015, p. 13)

Spiekermann (2008) develops a new acceptance model for Ubiquitous Computing which is not based on TAM, because TAM focuses on people´s intention to use a system, which “may not be enough to predict market success” (Spiekermann, 2008, p. 127). Acceptance is defined as “the intention to buy and/or use a UC service" (Spiekermann, 2008, p. 16). Figure 4describes the proposed UC-AM (UC Acceptance Model).

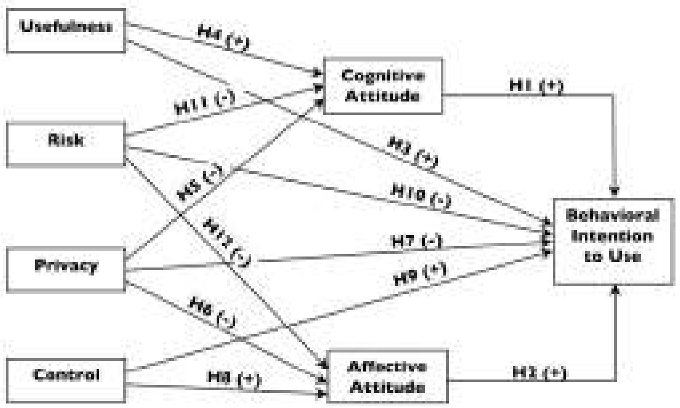


Figure 4.UC Service Acceptance Model-Hypotheses and (expected directions)(Spiekermann, 2008, p. 138)

Proposed approach

To evaluate the impact of Sealed Cloud on the User Acceptance of UBI, user acceptance has to be modelled. To this end, user acceptance factors should be identified and integrated into a model. The modelling will be iterative, refining the model based on the feedback from validation. The first user acceptance model will be formulated using the user acceptance factors obtained from a literature review. The Model will be validated by means of studies conducted via focus groups and surveys with different stakeholders, including insurance companies' representatives, consumers and data protection professionals. . Finally, based on the developed model, guidelines for improvement of the Sealed Cloud´s user acceptance in privacy applications will be developed.

The following research questions are considered:

RQ1. What are the user acceptance factors in the UBI the privacy respecting Behaviour-car in the insurance company scenario?

RQ2. How can the identified factors be combined into a user acceptance model for UBI?

RQ3. How can UBI be implemented using Sealed Cloud, and what are the key differences of these implementations compared to existing UBI solutions?

RQ4. How can the Sealed Cloud technology help in developing privacy-respecting UBI solutions with high user acceptance?

Research methodology

Figure 5depicts the activities regarding to the proposed methodology.First, a literature review will be conducted to collect information about UBI and user acceptance factors, which will be used to develop the first iteration of the user acceptance model.To develop a final model, two iterations consisting of the following phases are required: (1) user acceptance factor identification, (2) user acceptance model formulation, and (3) user acceptance model validation. Focus groups with different stakeholders and consumer surveys will be used to validate the model.

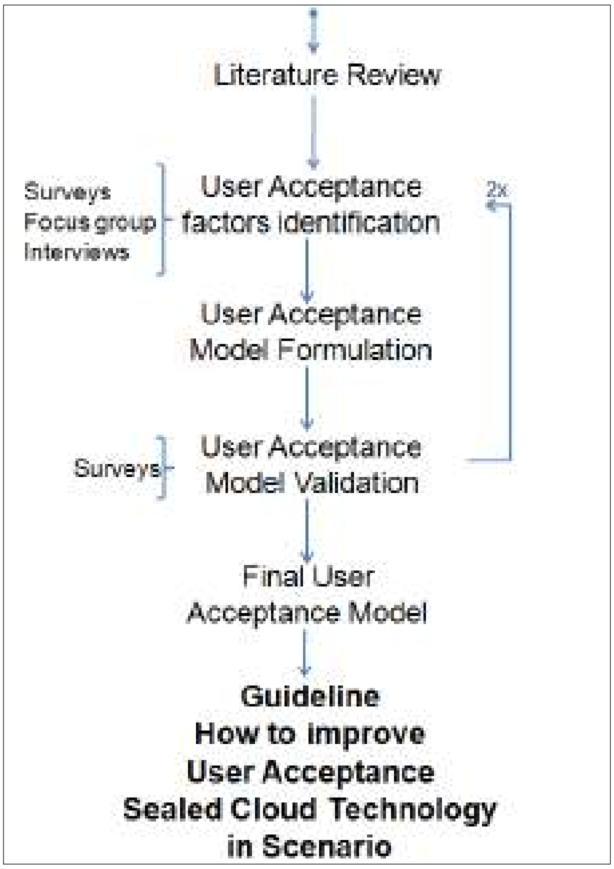

Literature Review
Surveys
Focus group
Interviews
User Acceptance factors identification
2x
User Acceptance Model Formulation
Surveys
User Acceptance Model Validation
Final User Acceptance Model
Guideline
How to improve
User Acceptance
Sealed Cloud Technology
in Scenario

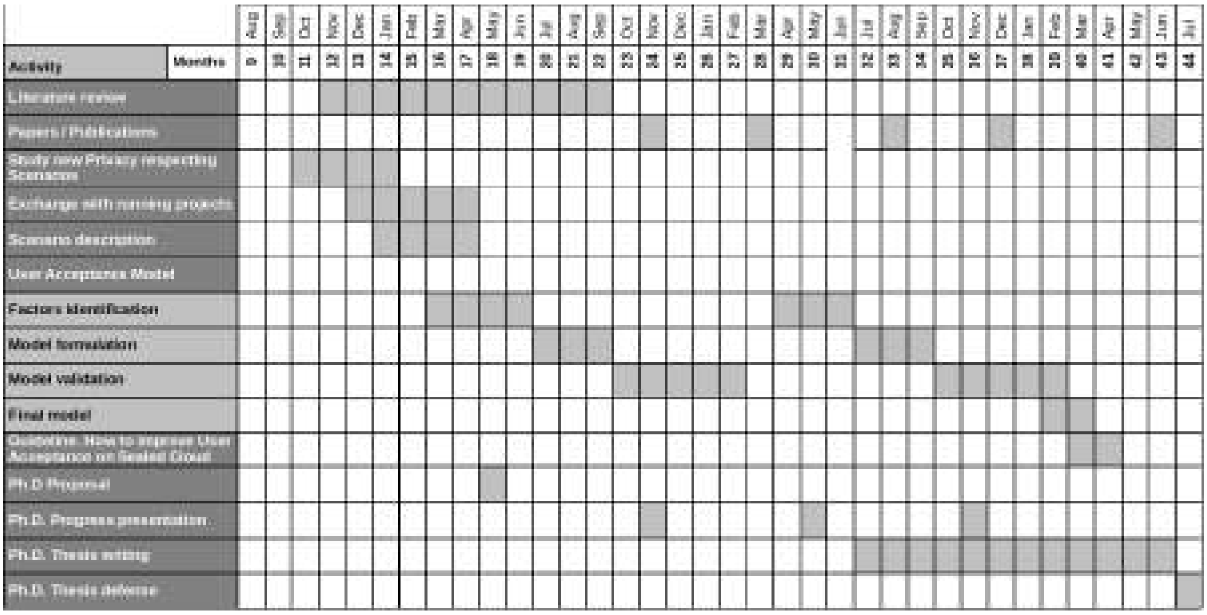
Figure 5.Research methodology

At the end, recommendations on how to improve the Sealed Cloud´s user acceptance in privacy-respecting applications will be developed by generalizing experience from the role of Sealed Cloud in the acceptance of privacy-respecting UBI.

Work plan

In the Figure 6is depicted a time plan with the activities, which will be done during this research. The first phase gathers activities towards choosing the scenario, such as: study privacy-respecting scenarios, exchange ideas with running projects at Uniscon, and conduct a literature review. Once a scenario will be chosen, activities towards developing a user acceptance model for this scenario are started, which consists of 2 iterations.

At the end, a compilation of recommendation regarding how to improve the user acceptance of Sealed Cloud in privacy-respecting applications will be written. Throughout the whole duration of the doctoral studies, dissemination activities will be done. Finally, the thesis will be written and defended.



		Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul
Activity	Months	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
Literature review					▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨																						
Papers / Publications																	▨				▨					▨				▨						▨	
Study new Privacy respecting Scenarios				▨	▨	▨	▨																														
Exchange with running projects						▨	▨	▨	▨	▨																											
Scenario description							▨	▨	▨	▨																											
User Acceptance Model																																					
Factors identification									▨	▨	▨	▨										▨	▨	▨													
Model formulation													▨	▨	▨										▨	▨	▨										
Model validation																▨	▨	▨	▨	▨								▨	▨	▨	▨	▨					
Final model																																▨	▨				
Guideline: How to improve User Acceptance on Sealed Cloud																																	▨	▨			
Ph.D Proposal											▨																										
Ph.D. Progress presentation																	▨						▨						▨								
Ph.D. Thesis writing																									▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	
Ph.D. Thesis defense																																					▨

Figure 6.Work plan

References

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

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.

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

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

Fishbein, M., &Ajzen, I. (1975). Belief, attitude, intention, and behavior: an introduction to theory and research, Addison Wesley, California.

Zhao, Y. (2002). Telematics: safe and fun driving. IEEE Intelligent Systems, 17(1), 10-14.

Handel, P.,Skog, I., Wahlstrom, J., Bonawiede, F., Welch, R., Ohlsson, J., &Ohlsson, M. (2014). Insurance telematics: Opportunities and challenges with the smartphone solution. IEEE Intelligent Transportation Systems Magazine, 6(4), 57-70.

Soleymanian, M., Weinberg, C., & Zhu, T. (2016). The Value of Usage-Based Insurance beyond Better Targeting : Better Driving, 1–45.

Dijksterhuis, C., Lewis-evans, B., Jelijs, B., Tucha, O., Waard, D. De, & Brookhuis, K. (2016). In-car usage-based insurance feedback strategies. A comparative driving simulator study. Ergonomics, 139(June 2017), 1–13. https://doi.org/10.1080/00140139.2015.1127428

Troncoso, C., Danezis, G., Kosta, E., Balasch, J., & Preneel, B. (2011). PriPAYD: Privacy-friendly pay-as-you-drive insurance. IEEE Transactions on Dependable and Secure Computing, 8(5), 742–755. https://doi.org/10.1109/TDSC.2010.71

Dillon, A., & Morris, M. G. (1996). User acceptance of new information technology: theories and models. Annual Review of Information Science and Technology Volume 31, Vol. 31, 3–32.

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology. MIS Quarterly, 36(1), 157–178. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2002388

Juan Quintero (ESR07), Uniscon GmbH (UNI)

I. Personal and Organizational Information

ESR´s Personal Information			
Name:	**Juan Quintero**	**ID number**:	
Office Address:	Agnes-Pockels-Bogen 1, Building B3. 80992, Munich, Germany	**Phone**:	+49 8941615987
Mobile:	+49 1603716183	**E-Mail:**	juan.quintero@uniscon.de

ESR´s Host Organization Information			
Name:	**Uniscon GmbH**	**Phone**:	+49 8941615987
Address:	Agnes-Pockels-Bogen 1, Building B3. 80992, Munich, Germany		

II. Supervision

Supervision			
Supervisor´s Name:	**Zinaida Benenson**	**Title**:	Dr.
Place of Employment:	Friedrich-Alexander University Erlangen-Nürnberg	**Phone**:	+49 9131-85 69908
Responsibility Distr.:	60%	**E-Mail:**	zinaida.benenson@cs.fau.de
Industrial Supervision			
Supervisor´s Name:	**Hubert Jäger**	**Title:**	Dr.
Place of Employment:	Uniscon GmbH	**Phone:**	+49 8941615987
Responsibility Distr.:	30%	**E-Mail:**	hubert.jaeger@uniscon.net
Co-Supervision			
Co-Supervisor´s Name:	**Ben Wagner**	**Title**:	Dr.
Place of Employment:	Vienna University of Economics and Business	**Phone**:	+43 1313364494
Responsibility Distr.:	10%	**E-Mail:**	ben@benwagner.org

Conduct of Supervision (per activity describe form of supervision and estimated supervision hours)**:**

Estimated supervision:

- Academic supervisions (user acceptance, usability, research proposal): 1 hr per week (37 meetings – 37 hrs)
- Scientific oriented: 0.5 hr per week (37 meetings – 18.5 hrs)
- Workpackages (Models of Behaviour, Technology Design and Development, and Interaction Design) monitoring: 1 hr per week (37 meetings – 37 hrs)

Estimated supervision by industrialsupervisor:

- Technical supervisions (sealed cloud technology, connected car): 0,5 hr per week (37 meetings – 18.5 hrs)
- Research oriented (research proposal): 0.5 hr per week (37 meetings – 18.5 hrs)

Estimated supervision by co-supervisor:

- Progress monitoring via conference calls: 1 hour per month (2 meetings – 2 hrs)

III. Secondment

ESR´s Secondment			
Supervisor's Name:	**Simone Fischer-Hübner**	**Title**:	Prof Dr.
Organization´s Name:	Karlstad University	**Phone**:	+46547001723
Address:	Universitetsgatan 2, 651 88 Karlstad, Sweden	**E-mail:**	simone.fischer-huebner@kau.se

IV. Research Project

ESR´s Project			
Title:	**The Role of Sealed Cloud Concept and Technology in User Acceptance and Usability of Privacy Applications**	**Ref. No:**	7
Overview and background			

This Ph.D. project is focusing on the impact of Sealed Cloud technology (Jäger et al., 2014) on user acceptance of privacy-sensitive applications. According to Figure 1, to reach this main goal, following steps should be accomplished: (1) learn how works Sealed Cloud technologies; (2) learn how to build user acceptance models (3) choose a particular privacy-sensitive application for the modelling purposes. Considering the use of Sealed Cloud within the chosen scenario, a user acceptance model (Benenson & Girard, 2015, p. 13) will be developed.

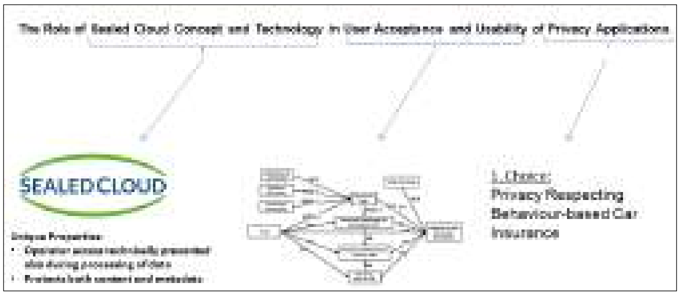

The Role of Sealed Cloud Concept and Technology in User Acceptance and Usability of Privacy Applications
SEALEDCLOUD
Unique Properties:
Operator access technically prevented also during processing of data
Protects both content and metadata
1. Choice:
Privacy Respecting Behaviour-based Car Insurance

Figure 1. Explanation of ESR7 project title

To choose the privacy application scenario, a review of existing privacy-respecting Uniscon GmbH projects was conducted. The main goal of this review was to choose a scenario where Sealed Cloud as a privacy-enhancing technology is relevant for implementation of privacy requirements. The scenario chosen was the so called Usage-Based Insurance (UBI), which is a car insurance where driver's insurance premium is calculated depending of his or her driving data. For example, customers who are label as "safe drivers" by the insurance algorithm pay lower premiums. Figure 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 lead to end-user privacy concerns and privacy invasions.

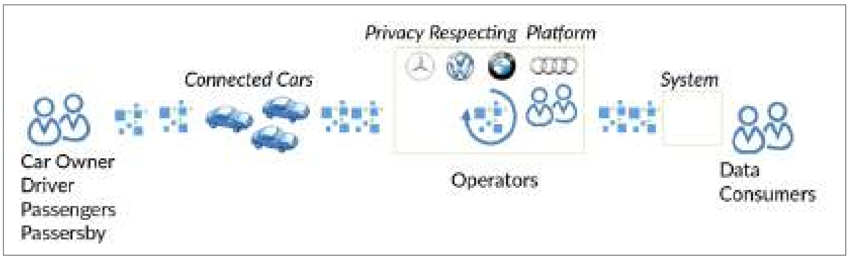


Figure 2. Connected Car system model

In this scenario, the insurance company could analyse the user data collected to find out behaviour patterns (driving style, speed, etc.) and reward him or her with new offers or discounts. The complexity of privacy-respecting management of user PII data is higher without using PETs. To reduce it, Sealed Cloud (Jäger et al., 2014) is one option.

Sealed Cloud is a technology developed by Uniscon GmbH that can be used as a building block for privacy applications. It implements a tamper-proof execution environment with strong perimeter security; where trustworthy behaviour of the cloud operator is encouraged through division of power. To determine the Sealed Cloud impact in the user acceptance it is necessary to develop a user acceptance model, based on identified user acceptance factors. To this end, a literature review is being conducted on Usage-Based Insurance (UBI), insurance telematics, and user acceptance models. These activities are grouped on the Workspackage 3 (Model of Behaviour). The task concerning understanding Sealed Cloud technology and its usability aspects belong to the Workspackage 2 (Technology Design and Development) and Workspackage 4 (Interaction Design), respectively.

V. Long-Term Career Objectives

Long-Term Career Objectives (over five years)
Once I finish the PhD program, my main goal is to work as researcher at an industrial research laboratory on projects between the industry and the academic sector in user acceptance of security and privacy technologies. As research, I want to produce new contributions and apply them to solve problems in the industry. Also, I want to reduce the gap between the academic and industrial sectors and share my experience and knowledge by applying academic contributions to resolve industry needs. During the PhD Program I will receive a lot of information, training, and support to improve my technical and non-technical skills. I am especially interested in improving my skills in documentation, presentation, and communication of ideas. In addition, project and time management will be needed to enhance my skills. Development of my technical skills will include Human Computer Interaction, Privacy, User Acceptance and Security in Cloud Computing.

VI. Short-Term Career Objectives

A. Project Research Results

Project Research Results
Presented according to Privacy & Us project Plan.

Milestones	Expected Results
Literature review (M18)	Information about technical implementations privacy issues and user acceptance of UBI
Research problem definition (M18)	Definition of the problem based on the literature review, business use cases, and user opinions
Research questions definition (M18)	Questions according to the problem definition
Research proposal document(M18)	Document with the first approach to my research proposal
Career development plan (M18)	Document about Career development plan in relation to my objectives after the PhD studies and my activities in the first year of PhD

Deliverables
2.1: Requirements analysis (M18) 3.1: The initial Models (M18) 4.1: User interface requirements (M18) 6.7: Researcher declarations and career development plan (M18)

Anticipated Publications
• **In preparation**: *A Probabilistic Model to Quantify Confidentiality in Cloud Computing*

Anticipated Conference/Workshop Attendance & Courses/Seminar Presentations
There is no activity

B. Training

Research and Technical Training

- Introduction to PETs, August 2016 (Karlstad, Sweden)
- Privacy Enhancing Technologies, January 2017 (Online Module)
- First Secondment, Februar 2017 (Karlstad, Sweden)
- Ph.D Seminar from October 2016 (Erlangen, Germany). Every 2 weeks Prof.Freiling organizes a seminar to discuss about the research of his group (Phd and post-doc students)
- Human Factors in Security and Privacy, April-July 2017 (Erlangen, Germany)

Secondment Plan

1. Goals

- Conduct literature review about user acceptance and trust factors in cloud computing and connected car scenarios to elicit a problem and research questions definition.
- Exchange ideas and organize discussions with Professors and Students to refine the scenarios, the problem definition, and the research questions.

2. Plan (8 weeks)

- Literature Survey (2 week)
- Problem and Research Questions definition (2 weeks)
- User acceptance and trust factor identification (2 weeks)
- Dissemination and discussion with Professors, Ph.D. and Post-Doc Students (2 weeks)

Interdisciplinary Training

- Privacy of Personal Health Data, August 2016 (Karlstad, Sweden)
- General Data Protection Regulation – Next Step?, August 2016 (Karlstad, Sweden)
- Introduction to Usability, August 2016 (Karlstad, Sweden)
- Data Protection by Design and Default, August 2016 (Karlstad, Sweden)
- Legal Privacy Workshop – Privacy by Design, August 2016 (Karlstad, Sweden)
- Panel: The Future of Privacy and Identity Management, August 2016 (Karlstad, Sweden)
- Values in IT- Privacy's wider context, May 2017 (Vienna, Austria)
- Economics of Privacy, June 2017 (Vienna, Austria)

Professional Training

- Scientific Paper Writing, August 2016 (Karlstad, Sweden)
- Professional Networking, August 2016 (Karlstad, Sweden)
- Self-Management, April 2017 (Online Module)
- Peer Review workshop, May 2017 (Vienna, Austria)
- Increasing impact of Research Results, June 2017 (Vienna, Austria)

Other Training Activities

- Sealed Cloud training, August 2016 (Munich, Germany). Introduction to Sealed Cloud Concept in Uniscon

C. Networking Activities

- First Privacy & Us Training Event (25th-27th August 2016, Karlstad, Sweden)
- Visit to Deutscher Commercial Internet Exchange DE-CIX, (20th January 2017, Frankfurt, Germany)
- Visit to BayLDA (Data Protection Authority of Bavariafor the Private Sector) to discuss about Privacy regulations in Telemetric Car Insurance (planned)

D. Research Management

There is no activity

E. Other activities

Other Activities (professional relevant)
Participated in meetings and contributed to discussions in Uniscon projects Sealed Freeze and Car-Bits.de

VII. Signatures

Date & Signature of fellow

Date & Signature of supervisor

References

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

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.

Yefim Shulman (ESR08), Tel Aviv University (TAU)

Tel Aviv University | Faculty of Engineering | Department of Industrial Engineering

Research Project Plan

Modelling Responses to Privacy-related Indications

Yefim Shulman

Supervised by

Professor Joachim Meyer

Co-supervised by

Karlstad University Researcher (TBD)

May 2017

Note

I joined the Privacy & Us project only in March of 2017. Hence this draft proposal is based on the first two months of my Ph.D. Obviously, the ideas are still very preliminary, and the research will probably change greatly over time and may take directions that differ from what is described here. Thus the proposal should be considered only as a very general indication of the direction my research will take.

Abstract

The Research Project Plan provides an outline of the research of ESR8 in the Privacy&Us project on “Modelling Human Responses to Privacy-related indications”. The research aims towards the development of a model of users’ decisions to perform actions that may impact privacy after users receive some indication (e.g., an alert or a notice) regarding the privacy implications of their actions. Model-based guidelines for providing privacy-related indications will be developed, based on this research. The model will be developed and later will be validated, based on existing empirical results from the research on privacy decisions, as well as dedicated web surveys and laboratory experiments, assessing the effects of different variables on user decisions. This document contains a brief review of the relevant background and of the literature on privacy-related decisions. I then describe the research approach and methodology I plan to take, followed by a general preliminary work plan for the duration of the project.

Table of Contents

1 Introduction

Privacy is a matter of growing concern for several actors. For the domain of information privacy these interested parties include: the data subjects (i.e., the users or the people, and the private entities), the regulators and controllers (i.e., governing bodies, associations in the public or private sector), the data holders (i.e., businesses and non-profit organisations, and state agencies). The increasing proliferation of Information Technology requires users to deal with Information Systems constantly. These interactions, if done invoking conscious decision-making, either can be associated with gaining tangible benefits (e.g., fulfilling work duties on a salaried job, acquiring goods and getting services online, etc.), or can derive from a user's needs or preferences (e.g., to communicate with relatives and friends, to exchange information, to access entertainment, etc.). Other interactions with technology can occur without awareness of the users, they are 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 from 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 a certain extent independent.

Modelling the privacy-related decision-making process will contribute to a better understanding of people's perception of privacy, their sense-making of information system dialogues content and their internalisation of the disclosure implications. Modelling users' decisions in terms of privacy concerns will have predictive capabilities that will provide guidance for the data holders on how to construct better ways of communicating privacy messages and privacy implications to the data subjects. Modelling the outcomes of this privacy decision-making process will also assist policy-makers in introducing and assessing regulations by improving quality of account of their implications.

2 Background

The research problem outlined above shows that it is necessary to understand how people make decisions in response to privacy concerns, and of the reasoning process behind choosing a certain decision over its alternative(s). We need to understand how people perceive and evaluate (or disregard) privacy risks and threats, as well as potential benefits, and what strategies (if any) they invoke in response to which signals, and how these signals may be interpreted.

Scholars investigated human decision-making in general, and privacy decision-making in particular, from economic perspectives, using a variety of modelling approaches. These approaches, showed in Figure 1, are closely related, often being extensions of one another. Rooted in classical Microeconomics of consumer's choice, the theory has expanded to account for such effects as bounded rationality, information asymmetries, perceptual biases and some other psychological features.

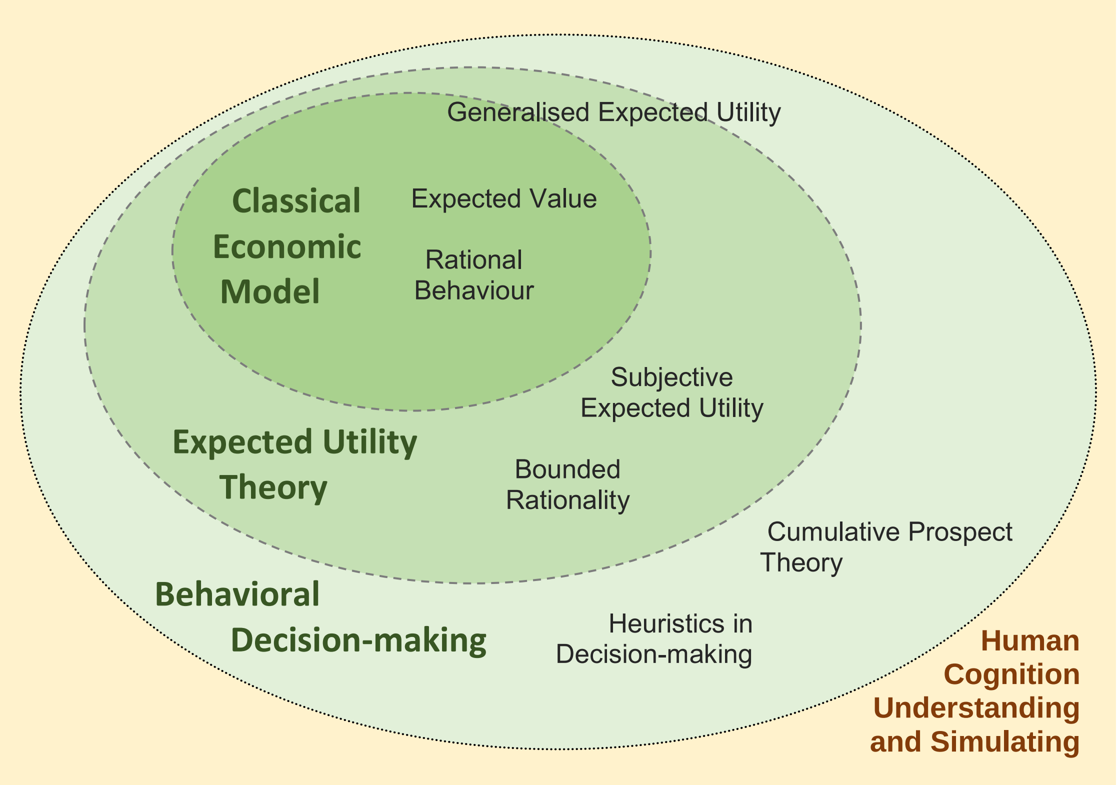

Generalised Expected Utility
Classical Economic Model
Expected Value
Rational Behaviour
Subjective Expected Utility
Expected Utility Theory
Bounded Rationality
Cumulative Prospect Theory
Behavioral Decision-making
Heuristics in Decision-making
Human Cognition Understanding and Simulating

Fig. 1. The map of commonly used approached to modelling decision-making

As demonstrated in Acquisti et al. (2005) and, later, further corroborated in Acquisti et al. (2016), people's decision-making regarding privacy diverges from what would be expected, should we base our assumptions on basic principles of value maximizing decision-making.

Privacy-related decisions take place in a certain context, whether it is a matter of the state of the mind of individual or properties of the environment. Mental fatigue, stress, attention span limitations, level of personal importance etc. on the one hand, and the social and physical environment can influence an individual's decision-making process. Most economic models of privacy decision-making ignore these situational factors. However, it is important to understand how situational variables can affect people's attitudes towards privacy.

Although, this is an extremely challenging task, certain advances have been made by cognitive scientists in their attempts to create a comprehensive framework of human cognitive processes, including perception and decision-making. Such frameworks – coined as cognitive architectures – may be capable of modelling the influence of various factors of the environment, momentary conditions and individual characteristics of decision-makers. One of the most flexible and complete of the cognitive architectures is ACT-R, proposed and being developed by a group of scholars in cognitive science and information theory.

3 State of the art

Privacy as a concept possesses multiple dimensions (Calo, 2011). We, however, will not attempt to understand privacy issues through all available lenses, but rather try to focus on how decision-making has been studied in terms of privacy attitudes.

Personal information disclosure is an intrinsic propensity inherent in humans. As demonstrated by Tamir et al. (2011) disclosing information about oneself is linked to self-rewarding as it causes excitation of dopaminergic pathway in the brain, that is, generates activation in the mesolimbic dopamine system which is associated with reward-related learning and perception of pleasure.

Privacy-related disclosures, however, seem to rely deeply on personal characteristics and context. Acquisti et al. (2015) discuss such factors as uncertainty associated with the consequences of privacy-related decisions, the context and the extent to which privacy concerns can be shaped by policy-makers and data holders. The authors emphasize among other things that transparency does not provide protection as people tend not to pay attention to legalism of privacy policies. Moreover, if general population was exercising due diligence by either reading or skimming privacy policies, the opportunity costs would arise in the national economy. And the amount of aggregate opportunity costs would exceed the total estimated value of online advertising at least by one order of magnitude (McDonald et al., 2008). Additionally, the perceived level control over privacy may play an inverse role for proneness to privacy harms, contradictory to what might be intuitively anticipated: a higher perceived level of control stipulates an actual decrease in privacy concerns, leading to lower watchfulness in exercising one's own privacy behaviour.

The economic approach to the study and modelling of privacy decisions is justified, as long as the value of privacy can be estimated, and the human's role in defining it is established. Acquisti et al. (2016) discuss how privacy has been regarded as an economic good and provide an explanation on how individuals' informed decisions about their privacy are being hindered, because of the possible asymmetry of the information available to people when they make privacy-related decisions.

Cumulative Prospect Theory can be applied for the purposes of modelling human decisions 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) authors first attempt to measure privacy concerns and estimate dependencies between factors and privacy constructs (“concerns of information finding” and “concerns of information abuse”), while later, in Dinev and Hart (2006), researchers provide more ground for the use of an extended privacy calculus, showing that – at least with the example of E-Commerce – Internet trust and person-al interest can outweigh privacy concerns 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.

Li et al. (2011) found that decisions regarding personal information disclosure depend on impressions that users internalize during first interaction with a website that prompts the users for said decisions to be made.

Attempts have been made to create a comprehensive integrated theory to approach modelling of the recognition heuristics and judgments (Marewski et al., 2011). Here authors address issues of an “ecological model of decision-making”, pointing out how scarce the research is on real-world decisions with utilizing “sense of prior encounter”.

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.).

In order to include various effects of internal and external factors influencing decision-making, we can try a broader model of cognition – one that simulates dynamic cognitive processes as functions in a system, consisting of input and data acquisition, memory, attention, decision making, and output generation. A widely used way to construct such a model is ACT-R.

ACT-R is one of the most detailed frameworks for modelling perception, procedural-al cognition and decision processes (Anderson, et al., 2004). It may provide major advantages for the modelling of privacy-related choices. As argued by Gonzalez and Lebiere (2005), there are numerous benefits to the modelling of economic decision making by using cognitive architectures, where ACT-R outcompetes its rivals, being in possession of a “more realistic characterization of the flexibility and adaptability of human behaviour”.

Thomson et al. (2015) argue that modelling paradigms (Taatgen et al., 2006) enabled in ACT-R, namely instance-based learning, can be applicable to modelling intuitive decision making. Authors manage to show that by using this cognitive architecture it is possible to implement risk aversion in learned (not forced) strategy choice. Veksler et al. (2013) demonstrate that the ACT-R framework can be used to implement human decision making arising from “associative learning”, not involving an a priori notion of rewards and punishments. Additionally, ACT-R is capable of modelling long-term (both declarative and procedural) and working memory functioning, perception and logic processes and, as shown by Peebles and Banks (2010) is suitable for dynamic decision-making, even though with certain shortcomings. As Taatgen and Anderson (2010) point out, the biggest challenge to overcome when it comes to modelling in cognitive architecture terms “is that it takes a substantial intellectual commitment to learn to understand models of a particular architecture and to learn to construct models”.

4 Proposed approach

In order to investigate how people consider information privacy implications, and perceive and internalise privacy-related information, we propose to develop a model of users’ decision-making process when it comes to make an explicit or implicit action (or abstain from one) to share or allow (re-)use of their personal information. The proposed model is expected to be based in Economics and Information and Cognitive Science advancements. Descriptive and predictive properties of the model shall be determined by perceived gains and losses, availability of information and impact of externalities at the moment of making a decision.

Decision-making, in accordance with the research rationale, is expected to be probed and simulated as a function of:

- the properties of the information that is to be disclosed,
- the perceived identity of who will have access to the information,
- the perceived identity of who requests the information,
- the context in which the information is to be provided,
- the users' individual characteristics,
- and the features of the indications from the system (e.g., warnings) pointing to the possible privacy implications of a user action.

The conceptual model will be based on existing research on user privacy preferences and decisions, as well as on existing research on user responses to alerts occurring during interaction with complex system. Fig. 2 shows a schematic depiction of factors that impact operator's response to system warnings (Meyer, 2004). This framework is useful for understanding the general picture of what can influence decision-making process regarding responses to indications. For the purposes of the project it seems appropriate to scope the factors of decision-making on Internet privacy preferences, using said framework.

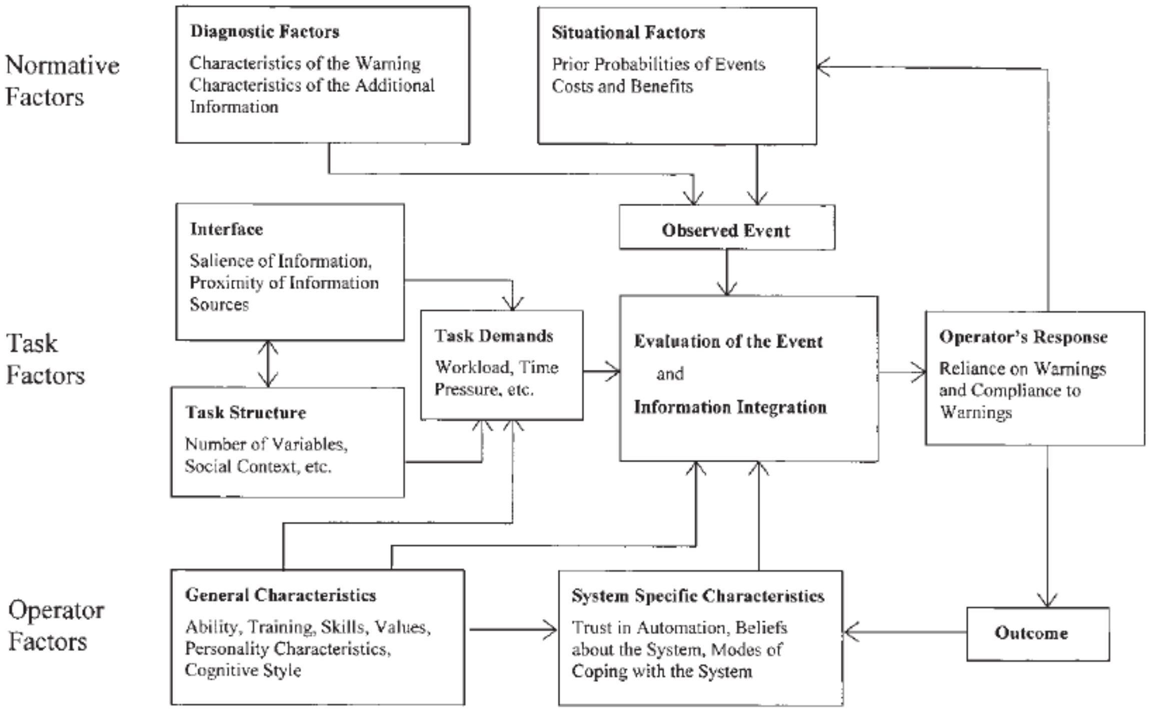

Normative Factors
Diagnostic Factors
Characteristics of the Warning
Characteristics of the Additional Information
Situational Factors
Prior Probabilities of Events
Costs and Benefits
Observed Event
Task Factors
Interface
Salience of Information, Proximity of Information Sources
Task Demands
Workload, Time Pressure, etc.
Task Structure
Number of Variables, Social Context, etc.
Evaluation of the Event
and
Information Integration
Operator's Response
Reliance on Warnings and Compliance to Warnings
Operator Factors
General Characteristics
Ability, Training, Skills, Values, Personality Characteristics, Cognitive Style
System Specific Characteristics
Trust in Automation, Beliefs about the System, Modes of Coping with the System
Outcome

Fig. 2. Schematic depiction of the categories of factors that affect responses to a warning (Meyer, 2004)

Disclosed information may vary in the level of technicality and detail. The identities of who accesses and who requests the personal information may be different and may be perceived erroneously, that is to be assumed as being different from factual objective identities. The context, in which the decision takes place, is one the main challenges to be modelled and tested, and is represented by the Task Structure and Task Demands in the Fig. 2. Users' individual characteristics (correspond to the Operator Factors) are those psychological traits, experience and mental features that may greatly impact the outcome of perception, evaluation and decision-making activities. The indications properties themselves (Interface) may vary in a way of how the information is conveyed to the users, in the way it is structured, and in the way how it requires the users to react (if at all).

In-depth analysis of relevant literature on privacy, warnings and behaviour is the starting point of current research project. Adequate background review should allow for devising of a broader conceptual model of decision-making in response to privacy-related indications. Once a conceptual model is formulated, the scope of the probing field shall be defined and an actual comprehensive model can be built, which later should enable construction of specific models to examine specific issues and test the predictive capabilities of proposed comprehensive model thereby checking its validity.

5 Research methodology

The research commences with comprehensive literature review, including but not limited to the part provide in Section 3: ”State of the Art” of this document and further investigation of the current state of the research on Internet privacy, privacy economics, human-computer interactions and system warning, human cognition, behaviour and decision-making, and advanced topics on modelling methods in information science. The literature review shall lead to narrowing down the domain of Internet privacy and defining the relations, which shall be modelled. Thus, it enables the formulation of the modelling approach and validation of the proposed research approach in detail.

Conceptual model inspired by the literature review will be followed up by a comprehensive model of Internet privacy decision-making. The latter model will be adjusted for testing for specific issues of people’s privacy attitudes. Ensuing analyses of test results will enable to adjust the model and improve its predictive capabilities. The experiments, which will be designed to validate the integrity and predictions of the models, will involve observing people’s behaviour when faced with privacy-related indications while interacting with information system. Improvement of the model is deemed as an iterative process of testing, date retrieval, data analysis and model adjustment.

Our general approach to the research in title justifies the use of quantitative approaches to the research project and at least the study of qualitative research products in the fields of privacy, warnings and behaviour.

One of the expected outputs of the modelling process of this research is industry and (or) policy-making guidelines that should offer recommendations on how to better formulate and convey privacy-related messages to data subjects.

The research shall be conducted according to Research Executive Agency regulations and in compliance to any and all applicable laws of the European Union and the State of Israel, including the instances of the international law.

6 Work plan

General outline of the work plan for the project is demonstrated in Fig. 3. The plan is subject to revision and adjustment.

Year	2017										2018												2019										
Calendar month	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov
Project month	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
Planned work / result	*The research period presented here is established in the corresponding Addendum to Researcher Agreement*																																
Literature review	🟩	🟩	🟩	🟩	🟩	🟩	▒	▒	▒	▒	░	░	░	░	░																		
Conceptual model							🟩	🟩	🟩	🟩																							
Comprehensive model											🟩	🟩	🟩	🟩	🟩																		
Model improvement and validation															🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩				
Guidelines																													🟩	🟩	🟩		
Secondment: GUF							🟩	🟩																									
Secondment: ATEA											🟩	🟩	🟩	🟩	🟩	🟩																	
Secondment: KAU																							🟩	🟩									
IFIP Summer School 2017					V		V																										
WP3: D3.1			V																														
WP4: D4.1			V																														
WP6: D6.7			V																														
WP3: D3.2									V																								
WP4: D4.2									V																								
WP3: D3.3																					V												
WP4: D4.3																					V												
WP3: D3.4																													V				
WP4: D4.4																													V				
Networking Session: WU, Vienna				V																													
Networking Session: TAU, Tel Aviv									V																								
Networking Session: UCL, London																V																	
Networking Session: GUF, Frankfurt																						V											
Networking Session: EWT, Milan																														V			
Dissertation Submission																																	V

Fig. 3. The work plan of the research project

References

1. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509-514.
2. Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. IEEE Security & Privacy, 3(1), 26-33.
3. Acquisti, A., Taylor, C., & Wagman, L. (2016). The Economics of privacy. *Journal of Economic Literature 54*(2), 442-492.
4. Anderson, J. R., Bothell, D., Byrne, M. D., Douglass, S., Lebiere, C., & Qin, Y. (2004). An integrated theory of the mind. *Psychological Review, 111*(4), 1036–1060.
5. Barberis, N. C. (2013). Thirty years of prospect theory in Economics. *The journal of economic perspectives, 27*(1), 173-195.
6. Calo, M. R. (2011). The boundaries of privacy harm. *Indiana Law Journal, 86*(3), 1131.
7. Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour & Information Technology, 23*(6), 413-422.
8. Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61-80.
9. 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.
10. Egelman, S., & Peer, E. (2015). Predicting privacy and security attitudes. *ACM SIGCAS Computers and Society, 45*(1), 22-28.
11. 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.
12. Gonzalez, C., & Lebiere, C. (2005). Instance-Based Cognitive Models of Decision-Making. *Transfer of knowledge in economic decision making*. New York: Palgrave McMillan.
13. 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.
14. 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.
15. 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.
16. Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: why we disclose. *Journal of Information Technology, 25*(2), 109-125.
17. 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.
18. 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.
19. Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems, 54*(1), 471-481.
20. McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *ISJLP*, *4*, 543-568.
21. Mahmood, S., & Desmedt, Y. (2013). Two new economic models for privacy. *ACM SIGMETRICS Performance Evaluation Review, 40*(4), 84-89.

22. 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.
23. Marewski, J. N., Pohl, R. F., & Vitouch, O. (2011). Recognition-Based Judgments and Decisions: What We Have Learned (So Far). *Judgment and Decision Making, 6*(5), 359-380.
24. Meyer, J. (2004). Conceptual issues in the study of dynamic hazard warnings. *Human Factors*, *46*(2), 196-204.
25. Peebles, D., & Banks, A. (2010). Modelling dynamic decision making with the ACT-R cognitive architecture. *Journal of Artificial General Intelligence, 2*(2), 52-68.
26. Taatgen, N. A., Lebiere, C., & Anderson, J. R. (2006). Modeling paradigms in ACT-R. *Cognition and Multi-Agent Interaction: From Cognitive Modeling to Social Simulation*, 29-52.
27. Taatgen, N., & Anderson, J. R. (2010). The past, present, and future of cognitive architectures. *Topics in Cognitive Science, 2*(4), 693-704.
28. Tamir, D. I., & Mitchell, J. P. (2012). Disclosing information about the self is intrinsically rewarding. *Proceedings of the National Academy of Sciences*, *109*(21), 8038-8043.
29. Thomson, R., Lebiere Ch., Anderson, J. R., & Staszewski, J. (2015). A general instance-based learning framework for studying intuitive decision-making in a cognitive architecture *Journal of Applied Research in Memory and Cognition, 4*(3), 180-190.
30. Veksler, V. D., Gray, W. D., & Shoelles, M. (2013). Goal-Proximity Decision-Making. *Cognitive Science: A Multidisciplinary Journal, 37*(4), 757-774.
31. 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.

Yefim Shulman (ESR08), Tel Aviv University (TAU)

I. Personal and Organizational Information

ESR´s Personal Information			
Name:	**EFIM SHULMAN**	**ID number**:	
Office Address:	Tel Aviv University, Tel Aviv 6997801, Wolfson Engineering Building, Room 003	**Phone**:	+972 3 640 9631
Mobile:	+972 58 799 2350	**E-Mail:**	efimshulman@mail.tau.ac.il

ESR´s Host Organization Information			
Name:	**Tel Aviv University**	**Phone**:	+972 3 640 8111
Address:	Tel Aviv University, Tel Aviv 6997801, Israel		
***If enrolled organization is different from host organization, please specify:**			
Name:	**-**	**Phone:**	**-**
Office Address:	**-**		

II. Supervision

Supervision			
Supervisor´s Name:	**Joachim Meyer**	**Title**:	Professor
Place of Employment:	Tel Aviv University	**Phone**:	+972 3 640 5994
Responsibility Distr.:	*To be defined*	**E-Mail:**	jmeyer@tau.ac.il
Co-Supervision			
Co-Supervisor´s Name:	*To be defined*	**Title**:	
Place of Employment:		**Phone**:	
Responsibility Distr.:	*To be defined*	**E-Mail:**	

Conduct of Supervision (per activity describe form of supervision and estimated supervision hours)**:**

Supervisor:

- **Regular meetings** – 1 hour per week. Days of the week re-scheduled each semester. Subject to change in case of emergency, holidays, one-time events interfering with the schedule.
- **Additional meetings** – depend on the workload and emerging questions, can be arranged upon request of the ESR. Timeslot should be defined and is subject to change in each particular case.
- **General guidance** – advice, criticism and suggestions obtained via email conversations.

Co-supervisor:
To be defined

III. Secondment

ESR´s Secondment			
Supervisor's Name:	**Kai Rannenberg**	**Position**:	Prof. Dr.
Organization´s Name:	**Goethe University Frankfurt**	**Phone**:	+49 69 798 34701
Address:	Goethe University Frankfurt, Theodor-W.-Adorno-Platz 4, Office 2.256, RuW Building, 60629 Frankfurt/Main, Germany	**E-mail:**	Kai.Rannenberg@m-chair.de

IV. Research Project

ESR´s Project			
Title:	**Modelling Responses to Privacy-related Indications**	**Ref. No:**	ESR8

Overview and background

Privacy iis a matter of growing concern for several actors. For the domain of information privacy these interested parties include: the data subjects (i.e., the users or the people, and the private entities), the regulators and controllers (i.e., governing bodies, associations in the public or private sector), the data holders (i.e., businesses and non-profit organisations, and state agencies). Currently, the data subjects' interactions with technology is unavoidably accompanied by multiple acts of personal information disclosure of varying extent and justification. If done explicitly as a choice to disclose in response to prompt dialogues requesting (lack of) actions, these actions are conscious decisions that can be modelled. Modelling this decision-making process will contribute to better understanding of people's perception of privacy, their sense-making of information system dialogues' content and their internalisation of the disclosure implications. Modelling outcomes of this decision-making process will have predictive capabilities, what will provide guidance for the data holders' on how to construct better ways of communicating privacy messages and privacy implications to the data subjects.

The research is expected to result in the development of a model of the users' decision-making regarding the performance of actions that may impact privacy as a function of: (A) the disclosed information, (B) the identity of who will have access to the information, (C) the context in which the information is provided, (D) the user's individual characteristics, (E) and indications from the system (e.g., warnings) pointing to the possible privacy implications of a user action.

The model is expected to be based and later validated on a combination of existing research on user privacy preferences and decisions, dedicated web surveys on users' privacy decisions, and laboratory experiments, assessing the effects of different variables on user decisions. The model is expected to be a combination of methods from Economics and Cognitive Science, aiming to predict user decisions based on the perceived costs and benefits and available information at a given moment.

Outputs expected to be produced over the course of the research project:

- Survey of relevant literature on privacy-related decisions.
- Initial model for predicting privacy-related decisions.
- Survey for collecting information on responses to privacy-related indications.
- Experimental platform for conducting experiments on privacy-decisions.
- Collection of empirical data on decisions based on privacy-related information.
- Validated model for predicting privacy-related decisions.
- Model-based guidelines for providing privacy-related indications.
- Papers in international conferences (no less than 4).
- Journal articles in connection with the research (3 or more).

V. Long-Term Career Objectives

Long-Term Career Objectives (over five years)

General Assumption:
the Ph.D. is awarded within the scope of the Privacy&Us project.

Goal 0:
Successfully finish a post-doctorate research project within 3 years after being awarded the Ph.D.

Objectives

1. Research interests definition: Human Intelligence / Artificial Intelligence, Data Science in Privacy Research, Privacy domains / disciplines.
2. Obtaining or improving skills and qualifications.
3. Professional Networking
4. Research location definition: Academia opportunities survey, Business Laboratories opportunities survey
5. Potential personal gains and losses evaluation.

Goal 1:
Receive a Major Research or Executive Position in the Industry by the end of the post-doctorate research project.

Objectives

1. Identify industry demands: Positions of Interest, Areas of Research, Areas of Business, Future Prospects.
2. Obtaining or improving skills and qualifications.
3. Resume: Professional Networking, Self-presentation and Application.

Goal A, *conditional*:
Receive a Research Position in the Industry immediately after the successful completion of the Ph.D. project.
*Condition: having **Goal 0** failed or become obsolete.*

Objectives

1. Understanding the reasons behind abandoning **Goal 0**.
2. Proceeding by applying situational adjustments to **Goal 1**.

Objectives [2, 3] for **Goals 0 and 1,** which are also implied under **Goal A,** will be partly met within the **Privacy&Us** project, and will be dealt with through the courses, training and workshops taken alongside those envisaged on the Grant Agreement. Main areas of improvement include privacy awareness, usability and human cognition and decision-making; formal analysis and modelling methods; analysis and modelling tools, and model implementation methods. The listed areas are examined through the fields of Behavioural Economics, Data Science and Cognitive Psychology.

VI. Short-Term Career Objectives

A. Project Research Results

Project Research Results

Presented according to the Privacy & Us project Plan.

Milestones	Expected Results
Survey of relevant literature on privacy-related decisions	Understanding the state of the art in privacy decision-making
Participation in international conferences	Papers
Research Proposal	Researcher Declaration and Career Development Plan

Development of an initial model for predicting privacy-related decisions	Initial model predicting privacy decision-making

Deliverables

WP3 – D3.1: The Initial Models [18]
WP4 – D4.1: User Interface Requirements [18]
WP6 – D6.7: Researcher Declarations and Career Development [18]

Anticipated Publications

Anticipated Conference/Workshop Attendance & Courses/Seminar Presentations

1 Privacy-by-Design Workshop: Can Engineers and Organisations Do It? (University of Haifa and Hewlett Packard Enterprise, Israel) – **Attended**

2 IFIP Summer School 2017 on Privacy and Identity Management – the Smart World Revolution (Joint Research Centre, Ispra, Italy)

B. Training

Research and Technical Training

Secondment Plan

First Secondments: Goethe University Frankfurt, August 25 – October 25, 2017, work with Prof. Rannenberg's group.

Interdisciplinary Training	
1	Privacy's wider context: Values in IT
2	Economics of privacy
3	Introduction to Privacy and PETs

Professional Training	
1	Increasing impact of research results
2	Peer Reviewing – Editor's view
3	Self-management

Other Training Activities

C. *Networking Activities*

1	**Privacy-by-Design Workshop: Can Engineers and Organisations Do It? (University of Haifa and Hewlett Packard Enterprise, Israel)**
2	**IFIP Summer School 2017 on Privacy and Identity Management – the Smart World Revolution (Joint Research Centre, Ispra, Italy)**

D. Research Management

E. Other activities

Other Activities (professional relevant)

Make-up course I: Quantitative Models of Human Performance
Make-up course II: Statistical Analysis of Data

VII. Signatures

Date & Signature of fellow

Date & Signature of supervisor

Luiza Rezende (ESR09), Tel Aviv University (TAU)

Research Proposal

for Privacy & Us (EU Horizon 2020 Marie Sklodowska-Curie Innovative Training Network) and as part of the degree of Ph.D. in Law at Tel Aviv University

May 2017

Reframing Informed Consent in Information Privacy Law Through Behavioral Economics and the Paternalism-Libertarianism Spectrum

Candidate:
Luiza Rezende

Supervisors:
Prof. Michael Birnhack (Law) &
Dr. Eran Toch (Industrial Engineering)

Buchmann Faculty of Law - Zvi Meitar Center for Advanced Legal Studies
Tel Aviv University

Abstract

Informed consent, in the context of information privacy law, is the requirement to obtain the data subject’s consent before collecting his or her personal data. Both in the American and European Union's legal systems, despite their structural differences, informed consent is central. In the last years, however, authors from different fields have shown concerns regarding the validity and effectivity of the informed consent requirement, raising multiple shortcomings. In the present work, I will first analyze these shortcomings through three concepts from behavioral economics - cognitive limitation, information asymmetry and time constraint - understanding how these behavioral characteristics generate issues in the information privacy context. In the next phase, I will explore suitable tools available to remedy or mitigate those shortcomings, focusing on their paternalistic or libertarian background. I will describe cases in other industries - such as the automobile, tobacco, food and environmental - where analogous behavioral issues were remedied using more paternalistic or more libertarian strategies, and will inquire how these learnings can be used in the context of reframing informed consent in information privacy. My methodology will involve legal theory, concepts from behavioral economics and political economy, and comparative analysis with other fields.

Table of Contents

1. Introduction

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.[1] The strictness and detailing of the consent requirement vary among legislations, however, both in the European Union and in the United States,[2] which differ significantly in their structure and content regarding privacy protection,[3] informed consent is central. In Europe, the new General Data Protection Regulation (GDPR),[4] defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[5] In the United States, the Federal Trade Commission's (FTC) Reports to Congress from 1998 and from 2012 speak about consent. The 1998 Report states that "the most fundamental principle is notice. Consumers should be given notice of an entity's information practices before any personal information is collected from them" and "choice means giving consumers options as to how any personal information collected from them may be used."[6] The 2012 Report states that "companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes."[7]

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 I classify as issues involving cognitive limitations,

[1] Information privacy or data privacy are used as synonyms in the present proposal. According to Greenleaf's study, "a 'data privacy law' is a national law which provides a set of basic data privacy principles, to a standard at least approximating the minimum provided for by the OECD Guidelines or Council of Europe Convention 108, plus some methods of officially-backed enforcement (i.e. not only self- regulation). A general constitutional protection for privacy, or a civil action (tort) of infringement of privacy is not sufficient, and nor is a voluntary code of conduct." See Graham Greenleaf, *Global Data Privacy Laws: 89 Countries, and Accelerating*, 115 PRIVACY LAWS & BUS. INTERN'L REP. 2 (2012).

[2] The legal systems of these two places will be the focus of the proposed thesis.

[3] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 YALE L.J. 1151 (2004) (comparing the underlying approaches of the American and European privacy regimes).

[4] 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. The Regulation was issued in 2016 and it is going to be enforced from April 2018.

[5] *Id*. art. 4(11).

[6] Martha K. Landesberg, Toby Milgrom Levin, Caroline G. Curtin, Ori Lev, *Privacy Online: A Report to Congress*, FTC 7-8 (1998).

[7] FTC Report, Protecting Consumer Privacy in an Era of Rapid Change, viii (2012).

information asymmetry, or time constraints.[8] Other authors have proposed solutions to these shortcomings, which I identify and organize in terms of their paternalistic or libertarian character.[9]

My argument in the proposed thesis is that through these three concepts from behavioral economics (cognitive limitation, information asymmetry and time constraint) and through the philosophical-political ideas of paternalism and libertarianism, it is possible to reach a deeper understanding regarding the shortcomings of informed consent and the most suitable tools available to mitigate or remedy them. To develop my argument, I will first characterize informed consent in privacy in the context of the two legal systems that will be in focus (American and the European Union's) and present the most relevant privacy theories and frameworks that will guide the analysis. The next step will be to explain the relevance of behavioral economics to the present context and apply behavioral concepts to the shortcomings of informed consent, identifying them as a cognitive limitation, information asymmetry or time constraint issue. With this broad conceptual background in hand, I will discuss available tools and strategies to overcome the shortcomings of informed consent, taking into consideration both their paternalistic or libertarian character, applicable privacy theories and the limitations of the legal systems in focus.

My 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 proposed thesis will be organized in the following way: *Part I* will be dedicated to the exposition of relevant privacy theories, the European and American information legal privacy regimes and the role of informed consent in each of them. *Part II* will deal with the shortcomings of informed consent in privacy, their characterization as a cognitive limitation, information asymmetry or a time constraint issue, and the solutions offered by authors from different fields, focusing on their libertarian and paternalistic characteristics. *Part III* will be dedicated to the explanation of the methodology: I will present the relevance of behavioral economics to the present context, including, in a more detailed form, the concepts of cognitive limitation, information asymmetry and time constraint and also the political-philosophical conceptions of paternalism and libertarianism, explaining why I chose these parameters to elucidate new understandings to informed consent. In *Part IV* I will discuss what tools can mitigate or overcome the shortcomings of informed consent in privacy

[8] They will be further explained in Section 2. For a table with the identified shortcomings of informed consent, see Annex I.

[9] These terms will be further explained in Section 2. For a visual representation of the paternalism-libertarianism spectrum, see Annex II.

focusing the analysis on the paternalistic or libertarian character of these solutions. In this last section, I will use examples from other fields – in which a more paternalistic or libertarian tool was used to overcome a shortcoming analogous to one of those in informed consent - and also explore the theoretical background, understanding how different conceptions of privacy might help me assess these solutions.

2. Literature review

2.1. Consent in the European Union and in the United States

Informed consent is a central element in both the American and the European legal systems. In the American system, as Thomas Norton explains,[10] since 1973 in the Ware Report,[11] and in the following year, in the Privacy Act of 1974,[12] we can already identify the principles behind notice and choice. After successive implementations of the notice and choice approach in policymaking efforts during the 1990s,[13] in 1998, the FTC asserted that notice is "the most fundamental principle" in online privacy protection.[14] In the 1998 FTC report to Congress,[15] the Fair Information Practice Principles (FIPPs) were consolidated,[16] and notice and choice were mentioned separately and had different requirements: notice was said to be the most fundamental principle, with the addition that "consumers should be given notice of an entity's information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information."[17] Regarding choice, the second principle, the report mentioned that "choice means giving consumers options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information — i.e., uses beyond those necessary to complete the contemplated transaction."[18]

[10] Thomas B. Norton, *The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model*, 27 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 181, 196-198 (2016).

[11] U.S. Dep't of Health, Educ. & Welfare, Records, Computers and the Rights of Citizens (1973).

[12] 5 U.S.C. § 552a (2012).

[13] Norton, *supra* note 10, at 197.

[14] *Id.*

[15] Landesberg et al., *supra* note 6.

[16] According to Paul Schwarz, "fair information practices are the building blocks of modern information privacy law. They are centered around four key principles: (1) defined obligations that limit the use of personal data; (2) transparent processing systems; (3) limited procedural and substantive rights; and (4) external oversight." See Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1614 (1999).

[17] Landesberg et al., *supra* note 6, at 7.

[18] Landesberg et al., *supra* note 6, at 8.

In the European system, informed consent is a central element in the GDPR; it is mentioned multiple times in the recitals and in different articles. The definition provided by Article 4(11) is that "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[19] The basic rule is that consent is required for the lawfulness of the processing of personal data whenever the situation does not fit any of the cases foreseen in Article 6(1). Obtaining the data subject's consent, however, is not enough, as the GDPR specifies conditions of validity for consent (Article 7), bringing significant new challenges for companies that collect data. The GDPR was approved on 27 April 2016 and will take effect as of May 2018. It is entirely binding and directly applicable to all member states, not being necessary a previous conversion into national law.

Despite the qualitative and structural differences between the systems,[20] in both of them, informed consent is central. I will now briefly discuss the theoretical background that will be relevant for the proposed thesis.

2.2. Privacy Theories and Relevant Approaches

The first relevant theory for the proposed thesis is privacy as control. Alan Westin defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[21] Julie Cohen, on the same note, advocated that if one values the individual as an agent of self-determination and community-building, he or she should "take seriously a conception of data privacy that returns control over much personal data to the individual."[22] James Whitman added that continental privacy protections are based on control of sorts of information disclosed about oneself, what the Germans call "information self-determination."[23] Authors have also presented a critical evaluation of this view. Ruth Gavison, for example, stated that it is not enough that someone has control over his or her information, as others can have access to this information by other means (invading his or her privacy, however without interrupting his or her control); or a person might have lost the control over his or her data and not have lost privacy, as nobody has accessed this data.[24] Lilian Edwards and Ian Brown pointed out that the deployment

[19] GDPR, *supra* note 4, art. 4(11).

[20] For a deeper discussion on the differences between the American and the European privacy systems, see Whitman, *supra* note 3.

[21] ALAN WESTIN, PRIVACY AND FREEDOM, 7 (1967).

[22] Julie Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1377 (2000).

[23] Whitman, *supra* note 3, at 1161.

[24] Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 427 (1980).

of social networks – and the unceasing voluntary self-exposure that occurs in that environment – represent a new challenge for the conception of privacy as control, as “consumers’ desire for data security and control conflict with their desire to self-disclose.”[25]

The second theory is privacy as access. Gavison says that “our interest in privacy … is related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others’ attention.”[26] Similarly, Moore sees the privacy right as “an access control right over oneself and to information about oneself” and when explaining the breadth of this conception, he says that “controlling access to ourselves affords individuals the space to develop themselves as they see fit. Such control yields room to grow personally while maintaining autonomy over the course and direction of one’s life.”[27] Daniel Solove criticized this theory, stating that “without a notion of what matters are private, limited-access conceptions do not tell us the substantive matters for which access would implicate privacy” and added that “the theory provides no understanding of the degree of access necessary to constitute a privacy violation.”[28]

The third theory is privacy as human dignity. Edward Bloustein built an innovative work arguing against William Prosser’s view of four types of privacy torts[29] and aligned with Warren and Brandeis’ unitary view of privacy.[30] Bloustein believes that there is one thing that unites all four privacy torts, which is an affront to human dignity.[31] It is not to say that he was in absolute agreement with Warren and Brandeis’ view of privacy as a “right to be let alone,” as he thought that “Warren and Brandeis went very little beyond thus giving ‘their right’ and ‘their interest’ a name and distinguishing it from other rights or interests.”[32] However, after thoroughly analyzing Prosser’s four torts, Bloustein concluded that “the tort cases involving privacy are of one

[25] Lilian Edwards & Ian Brown, *Data Control and Social Networking: Irreconcilable Ideas? in* HARBORING DATA: INFORMATION SECURITY, LAW AND THE CORPORATION, 1 (Andrea M. Matwyshyn ed., 2009).

[26] Gavison, *supra* note 24, at 423.

[27] Adam Moore, *Defining Privacy*, 39 J. SOC. PHIL. 411, 414 (2008).

[28] Daniel Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1104 (2002).

[29] Prosser analyzed over 300 cases involving privacy and identified four privacy torts, namely: “a) intrusion upon the plaintiff's seclusion or solitude, or into his private affairs; b) public disclosure of embarrassing private facts about the plaintiff; c) publicity which places the plaintiff in a false light in the public eye; d) appropriation, for the defendant's advantage, of the plaintiff's name or likeness” in William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

[30] Unitary in the sense that there would be only one privacy tort. The famous definition of privacy by Warren & Brandeis is “the right to be let alone”, in Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[31] Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962 (1964).

[32] *Id.* at 970.

piece and involve a single tort,"[33] and defined it as an infringement to human dignity. Solove criticizes Bloustein's conception of privacy, saying that "theories of privacy as personhood, however, fail to elucidate what privacy is because the theories often do not articulate an adequate definition of personhood"[34] and by arguing that those conceptions are too broad as "our personalities are not purely private; indeed, there is much that is unique to the self that we readily display and express in public."[35] Gavison, in the same sense, stated that "we may well be concerned with invasions of privacy, at least in part, because they are violations of dignity … But there are ways to offend dignity and personality that have nothing to do with privacy."[36]

Besides these three major theories, there are two other approaches that have special relevance to information privacy. The first is Solove's taxonomy of privacy.[37] As a reaction to the lack of preciseness in the meaning of privacy in the legal context and as an attempt to amplify Prosser's view of privacy law as subsumed to four privacy torts, Solove mapped and described four categories with multiple subcategories containing different types of privacy violations, thus providing us with a rich new tool to analyze privacy challenges that emerge from new technologies. The second one is Helen Nissembaum's Contextual Integrity framework.[38] One of its central ideas is that "there are no arenas of life not governed by norms of information flow, no information or spheres of life for which 'anything goes'. Almost everything - things that we do, events that occur, transactions that take place—happens in a context not only of place but of politics, convention, and cultural expectation."[39] She argues that by observing the dynamics of people's lives we see that individuals move between one context and another and for each context there is a different set of norms.[40] Nissembaum advocates that "contextual integrity is maintained when both types of norms [norms of appropriateness and norms of flow or distribution] are upheld, and it is violated when either of the norms is violated."[41]

The theories and frameworks above will help me assess and contextualize the shortcomings of informed consent and the proposed solutions, as I will explain in the methodology. In the next section I will characterize these

[33] *Id*. at 1000.

[34] Solove, *supra* note 28, at 1118.

[35] *Id*. at 1118.

[36] Gavison, *supra* note 24, at 438.

[37] See DANIEL SOLOVE, UNDERSTANDING PRIVACY (2008); Daniel Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

[38] See HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010); Helen Nissembaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 137 (2004).

[39] *Id*. (2004) at 137.

[40] *Id*.

[41] *Id*. at 138.

shortcomings.

2.3. The Shortcomings of Informed Consent

Authors from different fields have been pinpointing informed consent's shortcomings. Here, I group and name these shortcomings according to their characteristics, which are also visually represented in Annex I. They are ordered according to insights from behavioral economics, which I will discuss later:

a) *complexity*: the length and legalistic language of the privacy notices make it hard for the 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;[42]

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.[43] 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);

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.[44] 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;

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.[45] This is an illustration of how improbable,

[42] Stuart Moran, Ewa Luger, Tom Rodden, *Literatin: Beyond Awareness of Readability in Terms and Conditions*, PROCEEDINGS OF THE 2014 ACM INTERNATIONAL JOINT CONFERENCE ON PERVASIVE AND UBIQUITOUS COMPUTING ADJUNCT PUBLICATION - UBICOMP '14 ADJUNCT (2014).

[43] "When considering trade-offs between two future moments, present-biased preferences give strong relative weight to the earlier moment as it gets closer." Ted O'Donoghue & Matthew Rabin, *Doing it now or later*, 89(1) AM. ECON. REV., 103 (1999).

[44] See Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 999 (2014). See also Omri Ben-Shahar & Carl E. Shneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 649, 700 (2011).

[45] Alexis Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC (March 1st 2012), at http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851, based on Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy*

undesirable, economically inefficient and maybe impossible would be to promote all this reading;

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;[46]

f) *continual collection*: some wearables and other IoT (Internet of Things) devices[47] are constantly collecting data, therefore there is the challenge of knowing how many times should consent be required and how not to overwhelm the data subject with thousands of consent requests a day.[48]

g) lack of awareness: information privacy and its existing risks and concerns are subjects not yet broadly diffused and understood by the general public.[49] Besides that, important figures in the industry[50] and new technologic trends[51] 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

Policies, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 540 (2008).

[46] See Daniel Le Métayer & Shara Monteleone, *Computer Assisted Consent for Personal Data Processing*, 3D LSPI CONFERENCE ON LEGAL, SECURITY AND PRIVACY ISSUES IN IT (2008) ("Imposing that the user of pervasive systems gives his consent before each communication of personal data would largely defeat the purpose of providing these systems in the first place"). For another examination of this challenge, see Ewa Luger & Tom Rodden, *An Informed View on Consent for UbiComp*, PROCEEDINGS OF THE 2013 ACM INTERNATIONAL JOINT CONFERENCE ON PERVASIVE AND UBIQUITOUS COMPUTING - UBICOMP '13, 537 (2013).

[47] Internet of Things (IoT) generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention. There is, however, no single, universal definition". Karen Rose, Scott Eldridge, Lyman Chapin, *The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World*, INTERNET SOCIETY (2015), http://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151221-en.pdf.

[48] For other privacy concerns involving wearable technologies, see Vivian Genaro Motti & Kelly Caine, *Users' Privacy Concerns about Wearables*, FINANCIAL CRYPTOGRAPHY AND DATA SECURITY LECTURE NOTES IN COMPUTER SCIENCE 231 (2015).

[49] See for example Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, PEW RESEARCH CENTER (2014), at http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is. "Only 26% [of internet users] read privacy policies during a recent study and readership outside of laboratory conditions is believed to be far lower. Free market mechanisms based in consumer choice will fail to protect privacy if consumers do not understand the choices available to them" in Aleecia M. McDonald, Robert W. Reeder, Patrick Kelley, Lorrie Faith Cranor, *A Comparative Study of Online Privacy Policies and Formats*, at 2 (2009), at http://www.robreeder.com/pubs/PETS2009.pdf

[50] For example when Mark Zuckerberg, Facebook's CEO, said at the Crunchie awards in San Francisco in 2010 that privacy was no longer a social norm. Bobbie Johnson, *Privacy no longer a social norm, says Facebook founder*, THE GUARDIAN (11 January 2010), at https://www.theguardian.com/technology/2010/jan/11/facebook-privacy; or when Erich Schmidt, Google's former CEO (and current executive chairman at Alphabet), during an interview for CNBC in 2009 answered the question "whether users should be sharing information with Google as if it were a 'trusted friend'" with the statement "if you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place." Richard Esguerra, *Google CEO Eric Schmidt Dismisses the Importance of Privacy*, ELECTRONIC FRONTIER FOUNDATION, December 10th 2009, at https://www.eff.org/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy.

[51] Social networks and wearables, for example, require a constant flow of data from the data subject to the data collector/processor and this fact does not seem to be an obstacle to the massive adoption of those technologies.

want to be informed and do not read privacy notices, their consent cannot be deemed informed;

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 inevitably incomplete, preventing the consent to be deemed informed (as the data subject was not informed of future uses of his or her data);[52]

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;[53]

j) *lack of interface*: in the case of surveillance systems, such as CCTVs, some biometrics and 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;[54]

2.4. Analyzing the Shortcomings of Informed Consent Through Behavioral Economics

Now that we have a detailed list of the shortcomings of informed consent in information privacy, I will use the framework of behavioral economics to analyze and classify them. I chose this framework, as I will explain in this section, 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 me 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 state that “behavioral economics is the combination of psychology and

[52] Omer Tene & Jules Polonetsky, *Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP 239 (2013). Also, currently there are discussions on what would be considered personal data, there might be cases where a certain data in the beginning is not considered personal (therefore possibly no informed consent required) but afterwards it is discovered to be personal, thus creating problems for consent, see for example: Paul M. Schwarz & Daniel Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814 (2011).

[53] Luger & Rodden suggested that people should be able to review and withdraw their consent and their data during or after the interaction with the system, thus helping them understand how their data is being used and enabling a more detailed choice, *in* Ewa Luger & Tom Rodden, *An Informed View on Consent for UbiComp*, PROCEEDINGS OF THE 2013 ACM INTERNATIONAL JOINT CONFERENCE ON PERVASIVE AND UBIQUITOUS COMPUTING - UBICOMP'13 (2013). In another work, they proposed ethically grounded guidelines based on consent-sensitive systems that support user agency and autonomy. See Ewa Luger & Tom Rodden, *Sustaining Consent Through Agency*, PROCEEDINGS OF THE 2014 ACM INTERNATIONAL JOINT CONFERENCE ON PERVASIVE AND UBIQUITOUS COMPUTING ADJUNCT PUBLICATION - UBICOMP '14 ADJUNCT (2014). For a critical view on the lack of further control, see Fred H. Cate, *The Failure of Fair Information Practice Principles, in* CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY 341 (2006).

[54] See for example Michael Birnhack & Niv Ahituv, *Privacy Implications of Emerging and Future Technologies*, PRACTIS, 36 (2013), available at https://ssrn.com/abstract=2364396.

economics that investigates what happens in markets in which some of the agents display human limitations and complications."[55] 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."[56] The assumptions above define the *Homo economicus*, or the *Econ*. Behavioral economics replaces Econs with *Homo sapiens*,[57] 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.

Regarding the shortcomings of informed consent that were previously presented in section 2.3, if we apply to them the framework of behavioral economics, items "a", "b" and "c" are cognitive limitation issues;[58] items "d", "e" and "f" are time constraint issues,[59] and items "g", "h", "i" and "j" are information asymmetry issues.[60] These labels and their choice as a methodological background to analyze informed consent will be explained in the proposed thesis; through them it will be possible to identify analogous shortcomings in other fields and design comparisons with the information privacy field.

As I will advocate in the proposed thesis, behavioral economics is a useful tool to design regulatory models, and different authors have suggested ways to perform this task. Acquisti et al., for example, account for data

[55] Sendhil Mullainathan & Richard Thaler, *Behavioral Economics*, NBER WORKING PAPER NO. W7948 (October 2000).

[56] Richard Thaler, *Behavioral Economics: Past, Present, and Future*, 106 AM. ECON. REV. 1577, 1579 (2016).

[57] *Id.* at 1579.

[58] "Despite numerous examples of people with prodigious abilities that we might otherwise have thought impossible, much of cognitive psychology rests on the premise that human information-processing capacity is rather severely bounded" Ralph Hertwig & Peter M. Todd, *More Is Not Always Better: The Benefits of Cognitive Limits, in* THINKING: PSYCHOLOGICAL PERSPECTIVES ON REASONING, JUDGMENT AND DECISION MAKING, 213 (2003). For an explanation on cognitive ease and cognitive strain, which are connected with cognitive limitation, see DANIEL KAHNEMAN, THINKING FAST AND SLOW, 59-70, (2011).

[59] Time constraint is one of the elements of bounded rationality. "Bounded rationality is a concept proposed by Herbert Simon that challenges the notion of human rationality as implied by the concept of *homo economicus*. Rationality is bounded because there are limits to our thinking capacity, available information, and time (Simon, 1982)", available at https://www.behavioraleconomics.com/mini-encyclopedia-of-be/bounded-rationality.

[60] "[t]hat fact that different people know different things: workers know more about their ability than does the firm; the person buying insurance knows more about his health, whether he smokes and drinks immoderately, than the insurance firm; the owner of a car knows more about the car than potential buyers; the owner of a firm knows more about the firm that a potential investor; the borrower knows more about his risk and risk taking than the lender" in Joseph E. Stiglitz, *Information and the Change in the Paradigm in Economics, Prize Lecture in Columbia Business School, Columbia University*, 482, December 8th 2001, available at http://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/2001/stiglitz-lecture.pdf.

subjects' vulnerabilities in the privacy realm and propose that policy decisions take that into consideration.[61] 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.[62] In the same line, Thaler & Sunstein 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.[63] 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, 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.[64]

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 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;[65] he also adds that behavioral economics offers a useful framework to deal with this challenge.[66] In a similar sense, Gregory Conti states 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."[67] He also offers 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."[68] As Calo and Conti make it clear, data subjects, who are already impacted by information asymmetry in relation to companies, are made even more

[61] Alessandro Acquisti, Laura Brandimarte, George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 (6221) SCIENCE 509 (2015).

[62] *Id.*

[63] RICHARD THALER AND CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2009).

[64] Cass R. Sunstein, *Empirically Informed Regulation*, 78 U. CHI. L. REV. 1349 (2011).

[65] Calo, *supra* note 44, at 999.

[66] *Id.* at 999.

[67] Gregory Conti & Edward Sobiesk, *Malicious Interface Design: Exploiting the User*, INTERNATIONAL WORLD WIDE WEB CONFERENCE COMMITTEE, 278 (2010).

[68] *Id*. at 278.

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.

Some of the solutions offered – as they will be discussed below - also take into consideration behavioral economics ideas and apply them to law. Lauren Willis describes a very promising model of performance-based consumer law, in which rules have their assumptions and consequences systematically tested on inquiries and experiments.[69] William McGeveran, on the other hand, presents different views on how legislation can provide incentives for companies to comply with rules, specifically supporting the "responsive regulation" model.[70] In his own words "collaboration, flexibility, and the carefully graduated penalties of the regulatory pyramid work well for enforcement of privacy and data protection law."[71]

As a reaction to the shortcomings previously presented, authors from multiple fields offered different types of solutions, leading us to the normative section of the proposed thesis. In the next paragraphs, I will discuss these solutions, classifying them according to their paternalistic or libertarian character.

2.5. Consent Solutions and the Paternalism-Libertarianism Spectrum

The proposed solutions to the shortcomings of informed consent might be classified within a spectrum that goes from the most intense form of paternalism to the most extreme form of libertarianism. Before explaining the solutions themselves, it is important to clarify these concepts, which will serve as a methodological baseline to assess and compare different forms of policy tools and strategies.

Paternalism “is the interference of a state or an individual with another person, against their will, and defended or motivated by a claim that the person interfered with will be better off or protected from harm.”[72] In the legal context, it means a state intervention in the form of law or any regulatory measure, designed to protect individuals from harm or to generate welfare. A traffic rule indicating that the use of seat belt is mandatory is an example of a paternalistic legal measure, as the law wants to protect the individuals from hurting themselves. In the case of information privacy law, a paternalistic view has an underlying assumption that the data subjects, in general, are not able to choose about privacy matters by themselves and if they do that, they might cause harm or end up in a less favorable position. The result is that the law will impose upon all the option that is believed

[69] See Lauren Willis, *Performance-Based Consumer Law*, 82 U. CHI. L. REV. 1309 (2015).

[70] William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959 (2016).

[71] *Id.* at 1025.

[72] Gerald Dworkin, *Paternalism*, THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY, at: https://plato.stanford.edu/entries/paternalism.

to generate the most welfare, to the detriment of individual autonomy and freedom.

Libertarianism, on the other hand, "is a political philosophy that affirms the rights of individuals to liberty, to acquire, keep, and exchange their holdings, and considers the protection of individual rights the primary role for the state."[73] In the legal sense, the purpose of the law would be to protect rights such as the right to life, liberty, private property, freedom of speech and association, freedom of worship, government by consent, equality under the law, moral autonomy and other individual rights. "In general liberals have contended that government power should be limited to that which is necessary to accomplish this task. Libertarians are classical liberals who strongly emphasize the individual right to liberty."[74]

Taking the specific case of informed consent in information privacy law, a libertarian approach would attribute extreme focus to freedom of choice and autonomy, supporting a tool that poses the most freedom possible in the hands of the data subjects, even if it might mean, in many occasions, leaving them worse off.

On some point in this paternalism-libertarianism spectrum lies libertarian paternalism, a term coined by Richard Thaler and Cass Sunstein in 2003.[75] They advocate that "the libertarian aspect of our strategies lies in the straightforward insistence that, in general, people should be free to do what they like - and to opt out of undesirable arrangements if they want to do so" and "the paternalistic aspect lies in the claim that it is legitimate for choice architects to try to influence people's behavior in order to make their lives longer, healthier, and better."[76] They state that nudges should be designed in a way that can positively influence people's welfare, however, individuals that are not happy with the choice of the choice architect can opt out (differently from a pure paternalistic perspective, where the rule is mandatory).

Besides libertarian paternalism, there are other points on the scale that ranges from paternalism to libertarianism. Having in mind a spectrum that goes from one extreme to another,[77] in the next lines I will show where each of the proposed solutions to the shortcomings of informed consent is located. The solutions vary in terms of who is the central agent (lawmakers, regulatory agencies, companies, developers etc.), what tool is used (legal, technological, regulatory, design, market etc.) and their general effect (fostering paternalism,

[73] Peter Vallentyne & Bas van der Vossen, *Libertarianism*, THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY, at https://plato.stanford.edu/archives/fall2014/entries/libertarianism.

[74] David Boaz, *Libertarianism*, ENCYCLOPEDIA BRITANNICA (last updated 30 January 2009), at https://www.britannica.com/topic/libertarianism-politics.

[75] Richard Thaler & Cass Sunstein, *Libertarian Paternalism*, 93 Am. Econ. Rev 175 (2003).

[76] In THALER & SUNSTEIN, *supra* note 63, at 5

[77] As shown in Annex II.

libertarianism or any point in the middle). They are named according to their main characteristic and located in a gradual scale that takes into consideration their general effect.

The first point on the spectrum, the most paternalistic option, is *interventionist paternalism*, which includes the *legal* and the *technological* variations. The *legal* variation suggests that more specific laws on information privacy should be issued and they should deal with all decisions regarding data collection and processing, not leaving much or any space for individual choice.[78] The *technological* variation implies that we should increase the responsibility of developers in designing systems with an already high level of privacy embedded in it, exempting the data subject from choosing (to consent or not) or drastically reducing his or her role.[79]

The second point is *objective paternalism*, which includes *performance based regulation*,[80] in which a rule, after issued, is followed up by continuous tests or inquiries in order to validate its efficacy. In the case of informed consent, it means that any norm regulating informed consent would have to have its practical consequences tested and validated also *ex post*.

The third point is *libertarian paternalism*,[81] including *nudges*,[82] which are interventions made by choice

[78] Solove proposes measures to reform privacy self-management as it is today, for example through the creation of different tools to help people manage their privacy globally and the enactment of more substantive privacy rules that would regulate different types of data use, in Daniel Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013). Similarly, Mantelero proposes that more decision power is given to data protection authorities and recommends rigorous multiple impact assessment of data processing and a more general adoption of the opt out model. See Alessandro Mantelero, *The Future of Consumer Data Protection in the E.U. Re-thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics,* 30 COMP. L. & SEC. REV. 643 (2014).

[79] Javier Bustos-Jiménez, *Do We Really Need an Online Informed Consent? Discussion from a Technocratic Point of View*, PROCEEDINGS OF THE 2014 ACM INTERNATIONAL JOINT CONFERENCE ON PERVASIVE AND UBIQUITOUS COMPUTING ADJUNCT PUBLICATION – UBICOMP '14 ADJUNCT (2014). Friedman et al. decoupled informed consent in six elements (disclosure, comprehension, voluntariness, competence, agreement and minimal distraction) and assessed how information systems could support informed consent in terms of design and compatibility with the underlying technology; see Batya Friedman, Peyina Pinn, Jessica K. Miller, *Informed Consent by Design, in* SECURITY AND USABILITY, 495 (Lorrie Cranor & Simson Garfinkel eds., 2005); see also Batya Friedman, Edward Felten, Lynette I. Millett, *Informed Consent Online: A Conceptual Model and Design Principles*, CSE TECHNICAL REPORT - SEATTLE: UNIVERSITY OF WASHINGTON (2000).

[80] See Willis, *supra* note 69.

[81] I use libertarian paternalism in the sense coined by Cass Sunstein & Richard Thaler. In their words:

> "The libertarian aspect of our strategies lies in the straightforward insistence that, in general, people should be free to do what they like—and to opt out of undesirable arrangements if they want to do so" and regarding paternalism, "the paternalistic aspect lies in the claim that it is legitimate for choice architects to try to influence people's behavior in order to make their lives longer, healthier, and better. In other words, we argue for self-conscious efforts, by institutions in the private sector and also by government, to steer people's choices in directions that will improve their lives."

See THALER & SUNSTEIN, *supra* note 63, at 5; see also Thaler & Sunstein, *supra* note 75.

[82] "A nudge, as we will use the term, is any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention

architects[83] that help data subjects choose options that are more beneficial to them (according to the choice architect opinion). An example of nudges are defaults, which are pre-set options with the objective to direct the data subject's choice in a desired way. In the context of informed consent, the system would provide a default option (such as sharing certain data or not sharing anything), which ideally would reflect the most beneficial choice for the data subject. If the data subject does not like it, he or she can opt out.

The fourth point is *paternalistic libertarianism*. It includes *improved design*: many authors have been studying other possible designs for privacy notices, using symbols, labels or simpler language,[84] with the goal of facilitating data subjects' comprehension of the content; also *improved format*: notices that are more visceral or, in other words, that present the information in a more interactive or intrusive way, with the aim of calling the data subject's attention.[85] It is libertarian because the final choice stays with the data subject, but it is a paternalistic type of libertarianism because the improvements to design or format – and what information will be highlighted to help the data subjects in each case - are decided by a choice architect.

The fifth point is *technological libertarianism*, including *electronic agents*, which are tools that facilitate the decision and control process for data subjects,[86] and *continuous control mechanisms*, which are stronger control options to the data subjects, so that they can see, edit or delete all the information that was collected about them when they want.[87]

The sixth and last point, the most libertarian option, is *market libertarianism*, which includes market oriented views such as the *data as a tradable good* approach, in which consent is turned into a decision of selling or not selling a piece of data and where the data subject has the maximum control over his or her data.[88] In this type of

must be easy and cheap to avoid. Nudges are not mandates. Putting the fruit at eye level counts as a nudge. Banning junk food does not." See THALER & SUNSTEIN, *supra* note 63, at 6.

[83] Thaler & Sunstein explain that "A choice architect has the responsibility for organizing the context in which people make decisions" and "there are many parallels between choice architecture and more traditional forms of architecture. A crucial parallel is that there is no such thing as a 'neutral' design" in THALER & SUNSTEIN, *id.*, at 3.

[84] See Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, Lorrie Faith Cranor, *Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach*, PROCEEDINGS OF THE 28TH INTERNATIONAL CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS - CHI '10 (2010); McDonald, *supra* note 54.

[85] See for example Ryan Calo, *Against Notice Skepticism in Privacy (And Elsewhere)*, 87 NOTRE DAME L. REV. 1027 (2012).

[86] For multiple suggestions on how to improve informed consent in the context of the Internet of Things and specifically on forms of "pre-consent," see Lilian Edwards, *Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective*, EU. DATA PROTECTION L. REV., 32 (2016).

[87] On the idea that privacy is an integral part of relationship building between data subjects and companies and on integrating privacy with offline CRM processes, see Lizzie Coles-Kemp & Elahe Kani-Zabihi, *On-line Privacy and Consent: A Dialogue not a Monologue*, PROCEEDINGS OF THE 2010 WORKSHOP ON NEW SECURITY PARADIGMS - NSPW '10 (2010).

[88] Larry Downes, *A Rational Response to the Privacy 'Crisis'*, 716 CATO INSTITUTE POLICY ANALYSIS, 31 (2013).

solution the data subject is the exclusive responsible to value and trade his personal data, and the government would only interfere to avoid abuses.

2.6. Reframing Informed Consent in Information Privacy

As shown above, the proposed thesis will have two methodological backgrounds, which confer the original character of the present work: first, the analysis of the shortcomings of informed consent in terms of behavioral economic issues (cognitive limitation, information asymmetry and time constraint) and second, the use of the concepts of paternalism and libertarianism (and the spectrum between them) to characterize and discuss possible solutions to the shortcomings of informed consent.

By detailing, organizing and characterizing the shortcomings of informed consent in terms of behavioral economics issues, I will create a path for interdisciplinarity, as comparisons with challenges from other industries (which show the same behavioral character) will be possible, allowing a new depth of understanding of current challenges within the information privacy field.

The discussion of possible solutions to informed consent in privacy in terms of their paternalistic or libertarian character is another important point. First, for the interdisciplinarity, as I will be able to compare policy choices in the information privacy industry with those adopted in other fields. Second, because when discussing the paternalistic or libertarian characteristic of available solutions I will obtain a new layer of understanding, which will help me assess better the suitability or not of a certain tool in the context of informed consent in information privacy.

3. Research Questions

In the proposed thesis my research questions will be: 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?

In the proposed thesis I will be mostly interested in: a) unveiling the multiple shortcomings of informed consent in privacy and analyzing them in terms of their behavioral characteristics, 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.

4. Methodology

I intend to utilize legal theory and analytical method. First, I will analyze the relevant privacy theories and the selected legal systems, setting the theoretical and normative stage for the discussions that will follow. Second, I will present the shortcomings of informed consent in privacy and assess them in terms of behavioral economics' concepts, namely cognitive limitation, information asymmetry and time constraint. Third, I will present the concepts of paternalism and libertarianism and will apply the methodology of the paternalism-libertarianism spectrum to the solutions to the challenges of informed consent in information privacy. At this point I will turn to a comparative analysis and stablish analogies between informed consent in privacy and other fields that have or had similar behavioral shortcomings, such as tobacco, automobile, food and environmental. The intention is to better understand what was the policy tool used to overcome or mitigate these shortcomings and how paternalistic or libertarian this solution was. Lastly, benefiting from the theoretical and normative background built through the thesis, I will return to the information privacy context and discuss solutions to the shortcomings of informed consent in light of their paternalistic or libertarian character.

5. Main Arguments

Despite the differences between the legal systems, informed consent is a central requirement to collect and process personal data both in the European Union and in the United States, which are the two legal systems in focus in the proposed thesis. However, in recent years, researchers from different fields have pinpointed numerous shortcomings related to it, highlighting that it might not be the best tool to promote privacy protection, mainly in the context of information privacy, where new technologies bring even more challenges to the proper implementation of informed consent.

The shortcomings stem from multiple fields and have different characteristics. I have positioned them in ten different categories and described them in terms of their behavioral character, namely if they are an issue of cognitive limitation, information asymmetry of time constraint. The classification in terms of behavioral economics issues will allow me to compare them with cases in other fields that share analogous behavioral shortcomings, broadening my scope of analysis.

The use of behavioral economics concepts to discuss normative and policy issues has also other advantages. Authors such as Calo and Conti have shown that behavioral economics 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.[89] It is also a useful tool to design regulatory models, as Aquisti et al and Thaler & Sunstein have advocated[90] and as a last example, it is also possible to apply behavioral strategies directly to law, as Willis and McGeveran have done.[91]

After discussing the shortcomings, I will focus on the solutions, both the ones already presented by multiple authors, as well as those I wish to offer. These solutions vary significantly on the level of paternalism or libertarianism they foster, therefore I have created the paternalism-libertarianism spectrum and classified the possible solutions within this spectrum.[92] The use of the political-philosophical concepts of paternalism and libertarianism will foster interdisciplinary, as they will allow me to compare and analyze policy tools offered in other fields with those proposed for the information privacy field. They will also broaden the scope of analysis, adding a new theoretical layer to the discussion of possible improvements and alternatives to informed consent in information privacy.

The privacy theories and selected legal systems will also be central to the proposed analysis. The privacy theories will help me consider points of view that informed consent in information privacy can incorporate, broadening the discussion to include approaches that currently might not be the most popular, but which can help me reframe informed consent in information privacy. The selected legal systems – the American and the European Union's – will give me a more concrete overview of existing limits and requirements to informed consent, and will possibly also invoke existing opportunities that are not being explored yet.

6. Reference List

Books

HOOFNAGLE, CHRIS JAY (2016) FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY.

KAHNEMAN, DANIEL (2011) THINKING FAST AND SLOW.

NISSENBAUM, HELEN, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010).

SOLOVE, DANIEL (2008) UNDERSTANDING PRIVACY.

THALER, RICHARD H. & CASS R. SUNSTEIN (2009) NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH,

[89] See Calo, *supra* note 44 and Conti, *supra* note 67.

[90] See Acquisti et al, *supra* note 61, Thaler & Sunstein, *supra* note 63.

[91] See Willis, *supra* note 69 and McGeveran, *supra* note 70.

[92] The Spectrum is visually represented *infra*, on Annex II.

AND HAPPINESS.

WESTIN, ALAN (1967) PRIVACY AND FREEDOM.

Articles

Acquisti, Alessandro, Laura Brandimarte, George Loewenstein (2015) *Privacy and Human Behavior in the Age of Information*, 347 (6221) SCIENCE 509.

Avineri, Erel (2014) *Nudging Safer Road Behaviors*, RAN NAOR FOUNDATION FOR THE PROMOTION OF RESEARCH IN ROAD SAFETY, at http://www.rannaorf.org.il/webfiles/files/Nudge_in_Road_Safety_final.pdf

Omri Ben-Shahar & Carl E. Shneider (2011) *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 649.

Bickel, Warren K. & Gregory J. Madden (1998) *The Behavioral Economics of Smoking*, NBER WORKING PAPER NO. 6444.

Birnhack, Michael & Niv Ahituv (2013) *Privacy Implications of Emerging and Future Technologies*, PRACTIS, at https://ssrn.com/abstract=2364396.

Bloustein, Edward J. (1964) *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962.

Bustos-Jiménez, Javier (2014) *Do We Really Need an Online Informed Consent? Discussion from a Technocratic Point of View*, PROCEEDINGS OF THE 2014 ACM INTERNATIONAL JOINT CONFERENCE OF PERVASIVE AND UBIQUITOUS COMPUTING ADJUNCT PUBLICATION – UBICOMP'14 ADJUNCT.

Calo, Ryan (2012) *Against Notice Skepticism in Privacy (And Elsewhere)*, 87 NOTRE DAME L. REV. 1027.

_________ (2014) *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995.

Carlsson, Fredrik & Olof Johansson-Stenman (2012) *Behavioral Economics and Environmental Policy*, ANNU. REV. RESOUR. ECON. 75.

Cate, Fred H. (2006) *The Failure of Fair Information Practice Principles, in* CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY 341.

Cohen, Julie (2000) *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373.

Coles-Kemp, Lizzie & Elahe Kani-Zabihi (2010) *On-line Privacy and Consent: A Dialogue not a Monologue*, PROCEEDINGS OF THE 2010 WORKSHOP ON NEW SECURITY PARADIGMS - NSPW '10.

Conti, Gregory & Edward Sobiesk (2010) *Malicious Interface Design: Exploiting the User*, INTERNATIONAL WORLD WIDE WEB CONFERENCE COMMITTEE.

Downes, Larry (2013) *A Rational Response to the Privacy 'Crisis'*, 716 CATO INSTITUTE POLICY ANALYSIS 31.

Edwards, Lilian & Ian Brown (2009) *Data Control and Social Networking: Irreconcilable Ideas? in* HARBORING DATA: INFORMATION SECURITY, LAW AND THE CORPORATION, (Andrea Matwyshyn ed).

Edwards, Lilian (2016) *Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective*, EUROPEAN DATA PROTECTION LAW REVIEW 32.

Friedman, Batya, Peyina Pinn and Jessica K. Miller (2005) *Informed Consent by Design*, in SECURITY AND USABILITY, *495-521* (Lorrie Cranor & Simson Garfinkel eds.).

Friedman, Batya, Edward Felten and Lynette I. Millett (2000) *Informed Consent Online: A Conceptual Model and Design Principles*, CSE TECHNICAL REPORT - SEATTLE: UNIVERSITY OF WASHINGTON.

Gavison, Ruth (1980) *Privacy and the Limits of Law*, 89 YALE L.J. 421.

Greenleaf, Graham (2012) *Global Data Privacy Laws: 89 Countries, and Accelerating*, 115 PRIVACY LAWS & BUSINESS INTERNATIONAL REPORT, SPECIAL SUPPLEMENT.

Hertwig & Todd (2003) *More Is Not Always Better: The Benefits of Cognitive Limits*, in THINKING: PSYCHOLOGICAL PERSPECTIVES ON REASONING, JUDGMENT AND DECISION MAKING.

Just, David R., Lisa Mancino, Brian Wansink (2007) *Could Behavioral Economics help improve Diet quality for Nutrition Assistance Program Participants?* UNITED STATES DEPARTMENT OF AGRICULTURE, 43 ECONOMIC RESEARCH REPORT, available at http://ben.cornell.edu/pdfs/USDA-BeEcon.pdf

Kelley, Patrick Gage, Lucian Cesca, Joanna Bresee, Lorrie Faith Cranor (2010) *Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach*, PROCEEDINGS OF THE 28TH INTERNATIONAL CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS - CHI '10.

Le Métayer, Daniel & Shara Monteleone (2008) *Computer Assisted Consent for Personal Data Processing*, 3D LSPI CONFERENCE ON LEGAL, SECURITY AND PRIVACY ISSUES IN IT.

Luger, Ewa & Tom Rodden (2013) *An Informed View on Consent for UbiComp*, PROCEEDINGS OF THE 2013 ACM INTERNATIONAL JOINT CONFERENCE ON PERVASIVE AND UBIQUITOUS COMPUTING - UBICOMP'13.

__________ (2013) *An Informed View on Consent for UbiComp*, PROCEEDINGS OF THE 2013 ACM INTERNATIONAL JOINT CONFERENCE ON PERVASIVE AND UBIQUITOUS COMPUTING - UBICOMP '13, at 537.

__________ (2014) *Sustaining Consent Through Agency*, PROCEEDINGS OF THE 2014 ACM INTERNATIONAL JOINT CONFERENCE ON PERVASIVE AND UBIQUITOUS COMPUTING ADJUNCT PUBLICATION - UBICOMP '14 ADJUNCT.

Mantelero, Alessandro (2014) *The Future of Consumer Data Protection in the E.U. Re-thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics*, 30 COMPUTER LAW & SECURITY REVIEW 643.

McDonald, Aleecia M. & Lorrie Faith Cranor (2008) *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 540.

McDonald, Aleecia M., Robert W. Reeder, Patrick Kelley, Lorrie Faith Cranor (2009) *A Comparative Study of Online Privacy Policies and Formats*, at 2, at http://www.robreeder.com/pubs/PETS2009.pdf.

McGeveran, William (2016) *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959.

Moore, Adam (2008) *Defining Privacy*, 39 J. SOC. PHILOS. 411.

Moran, Stuart, Ewa Luger, Tom Rodden (2014) *Literatin: Beyond Awareness of Readability in Terms and Conditions*, PROCEEDINGS OF THE 2014 ACM INTERNATIONAL JOINT CONFERENCE ON PERVASIVE AND UBIQUITOUS COMPUTING ADJUNCT PUBLICATION - UBICOMP '14 ADJUNCT.

Motti, Vivian G. & Kelly Caine (2015) *Users' Privacy Concerns About Wearables*, FINANCIAL CRYPTOGRAPHY AND DATA SECURITY LECTURE NOTES IN COMPUTER SCIENCE 231.

Mullainathan, Sendhil & Richard Thaler (2000) *Behavioral Economics*, NBER WORKING PAPER NO. W7948.

Nissembaum, Helen (2004) *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119.

Norton, Thomas B. (2016) *The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model*, 27 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 181.

O'Donoghue, Ted & Matthew Rabin (1999) *Doing it now or later*, 89(1) AM. ECON. REV., 103.

Ohm, Paul *(2010) Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701.

Schwartz, Paul M. (2011) *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999).

Schwarz, Paul M. & Daniel J. Solove (2011) *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814.

Rose, Karen, Scott Eldridge, Lyman Chapin (2015) *The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World*, THE INTERNET SOCIETY, http://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151221-en.pdf.

Prosser, William L. (1960) *Privacy*, 48 CAL. L. REV. 383.

Solove, Daniel (2002) *Conceptualizing Privacy*, 90 CAL. L. REV. 1087.

__________ (2006) *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477.

__________ (2013) *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880.

Stiglitz, Joseph E. (2001) *Information and the Change in the Paradigm in Economics, Prize Lecture in Columbia Business School, Columbia University*, December 8th 2001, http://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/2001/stiglitz-lecture.pdf

Sunstein, Cass R. (2011) *Empirically Informed Regulation*, 78 U. CHI. L. REV. 1349.

Thaler, Richard & Cass Sunstein (2003) *Libertarian Paternalism*, 93 AM. ECON. REV 175.

Thaler, Richard & Cass R. Sunstein (2003) *Libertarian Paternalism Is Not an Oxymoron*, 70 U. CHI. L. REV, 1159.

Thaler, Richard (2016) *Behavioral Economics: Past, Present, and Future*, 106 AM. ECON. REV. 1577.

Tene, Omer & Jules Polonetsky (2013) *Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP 239.

Warren, Samuel & Louis Brandeis (1890) *The Right to Privacy*, 4 HARV. L. REV. 193.

Whitman, James Q. (2004) *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 YALE L.J. 1151.

Willis, Lauren (2015) *Performance-Based Consumer Law*, 82 U. CHI. L. REV. 1309.

Laws and Regulations

U.S. Dep't of Health, Educ. & Welfare, Records, Computers and the Rights of Citizens (1973).

Privacy Act of 1974 - 5 U.S.C. § 552a (2012).

GDPR 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.

Reports

Landesberg, Martha K. Toby Milgrom Levin, Caroline G. Curtin, Ori Lev (1998) *Privacy Online: A Report to Congress*, FTC.

FTC Report (2012) Protecting Consumer Privacy in an Era of Rapid Change.

Other Sources

Boaz, David, *Libertarianism*, ENCYCLOPEDIA BRITANNICA at https://www.britannica.com/topic/libertarianism-politics.

Dworkin, Gerald, *Paternalism*, THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY, (Edward Zalta), at: https://plato.stanford.edu/entries/paternalism

Esguerra, Richard *Google CEO Eric Schmidt Dismisses the Importance of Privacy*, ELECTRONIC FRONTIER FOUNDATION, at https://www.eff.org/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy

Johnson, Bobbie, *Privacy no longer a social norm, says Facebook founder*, THE GUARDIAN, January 11th 2010, at https://www.theguardian.com/technology/2010/jan/11/facebook-privacy

Madrigal, Alexis (2012) *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC, at http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851.

Simon, Herbert A. (1982), *Models of bounded rationality* in “Bounded Rationality”, at https://www.behavioraleconomics.com/mini-encyclopedia-of-be/bounded-rationality/

Smith, Aaron (2014) *Half of Online Americans Don’t Know What a Privacy Policy Is*, PEW RESEARCH CENTER, at http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is.

Vallentyne, Peter & Bas van der Vossen, *Libertarianism*, THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Edward Zalta), at https://plato.stanford.edu/archives/fall2014/entries/libertarianism

Annex I

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 inevitably incomplete, preventing the consent to be deemed informed (as the data subject was not informed of future uses of his or her data);	Information Asymmetry
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

Annex II

Paternalism-Libertarianism Spectrum							
Name of category	Interventionist Paternalism (Legal and Technological)		Objective Paternalism	Libertarian Paternalism	Paternalistic Libertarianism	Technological Libertarianism	Market Libertarianism
Characteristic	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

Luiza Rezende (ESR09), Tel Aviv University (TAU)

1 Career Development Plan Year 1

I. Personal and Organizational Information

ESR´s Personal Information			
Name:	**Luiza Santiago Rezende**	**ID number**:	YC088413
Office Address:	Tel Aviv University, Zvi Meitar Center for Advanced Legal Studies, Faculty of Law, room 1	**Phone**:	
Mobile:	+972 542-444-640	**E-Mail:**	luizarezende@mail.tau.ac.il

ESR´s Host Organization Information			
Name:	**Tel Aviv University**	**Phone**:	
Address:	Tel Aviv University, P.O. Box 39040, Tel Aviv 6997801, Israel		
***If enrolled organization is different from host organization, please specify:**			
Name:		**Phone:**	
Office Address:			

II. Supervision

Supervision			
Supervisor´s Name:	**Dr. Eran Toch and Prof. Michael Birnhack**	**Title**:	
Place of Employment:	Tel Aviv University	**Phone**:	
Responsibility Distr.:	100%	**E-Mail:**	birnhack@post.tau.ac.il, erant@post.tau.ac.il
Co-Supervision			
Co-Supervisor´s Name:		**Title**:	
Place of Employment:		**Phone**:	
Responsibility Distr.:		**E-Mail:**	
Conduct of Supervision (per activity describe form of supervision and estimated supervision hours):			
- Detailed analysis and review of the thesis proposal and every chapter of the thesis by both supervisors. Multiple revisions, comments and feedbacks. - Constant communication via email and occasional meetings with both supervisors to ask doubts, request readings recommendations, suggestions etc. - Bi-weekly lab meeting with Dr. Eran in the Industrial Engineering building to present the last developments of the research and discuss it; 1h30 every 2 weeks.			

III. Secondment

ESR´s Secondment

Supervisor's Name:	Emiliano De Cristofaro	**Position**:	Senior Lecturer (Associate Professor)
Organization´s Name:	University College London, Department of Computer Science	**Phone**:	+44 20 7679 0349
Address:	Gower Street, London WC1E 6BT, United Kingdom	**E-mail:**	e.decristofaro@ucl.ac.uk

IV. Research Project

ESR´s Project			
Title:	Reframing Informed Consent in Information Privacy Law Through Behavioral Economics and the Paternalism-Libertarianism Spectrum	**Ref. No:**	

Overview and background

Informed consent, in the context of information privacy law, is the requirement to obtain the data subject's consent before collecting his or her personal data. Both in the American and European Union's legal systems, despite their structural differences, informed consent is central. In the last years, however, authors from different fields have shown concerns regarding the validity and effectivity of the informed consent requirement, raising multiple shortcomings. In the present work, I will first analyze these shortcomings through three concepts from behavioral economics - cognitive limitation, information asymmetry and time constraint - understanding how these behavioral characteristics generate issues in the information privacy context. In the next phase, I will explore suitable tools available to remedy or mitigate those shortcomings, focusing on their paternalistic or libertarian background. I will describe cases in other industries - such as the automobile, tobacco, food and environmental - where analogous behavioral issues were remedied using more paternalistic or more libertarian strategies, and will inquire how these learnings can be used in the context of reframing informed consent in information privacy. My methodology will involve legal theory, concepts from behavioral economics and political economy, and comparative analysis with other fields.

V. Long-Term Career Objectives

Long-Term Career Objectives (over five years)

After I finish my PhD, I hope to have acquired enough interdisciplinary skills in order to be able to work in a leadership position related to privacy in the high-tech industry. During the PhD, besides improving my legal knowledge, I hope to be learn from other fields such as computer science, human-computer interaction, behavioral economics and related others.

I believe that multidisciplinary skills and the ability to work in diverse environments are key factors for success in the high tech / information privacy industry, as technology is constantly changing and challenging old concepts of privacy. Also, I consider my legal knowledge and legal experience key assets in the privacy context, as technological advancements and structural changes have to be accompanied by the suitable legal provisions and concerns originated in the privacy field, which require a professional with legal background to implement.

Therefore, in the long run, I expect to have the necessary qualifications to work in such a dynamic and complex environment such as the information privacy field, being able to bridge the technical aspects with the legal framework that embraces them.

VI. Short-Term Career Objectives

A. Project Research Results

Project Research Results
Presented according to Privacy & Us project Plan.

Milestones	Expected Results
Writing Ph.D. proposal (M18)	Wrote a research proposal that will guide my research work.
Career development plan (M18)	Thought and developed a career development plan that covers the next 5 years after the Ph.D. studies and details my progress in the first year.
3.1: The Initial Models (M18)	Submitted a report with a detailed specification of the modeling approach that will be taken.
5.1: Privacy Principles (M20)	Submitted a detailed report that reflects on whether legal concerns further influence the privacy threats.

Deliverables
3.1: The Initial Models (M18) 5.1: Privacy Principles (M20) 6.7: Researcher Declarations and Career Development Plan (M18)

Anticipated Publications
- No anticipated publications so far.

Anticipated Conference/Workshop Attendance & Courses/Seminar Presentations
- Attended IFIP Summer School 2016 (22th-26th August 2016, Karlstad, Sweden); - Attended the first network wide event (25th-27th August 2016, Karlstad, Sweden); - Attended Computers Privacy & Data Protection (CPDP – Jan/2017) in Brussels – Belgium; - Will attend the second network wide event (29th – 2nd May / June, Vienna, Austria); - Will attend the Cyber Week at Tel Aviv University – 25th – 29th June; - Will attend the Conference on Behavioural Economics – 16th-17th July – Tel Aviv.

B. Training

Research and Technical Training
At Tel Aviv University, for the first year of my studies I have a requirement to attend 8 credits (4 courses of 26 teaching hours each) and write a thesis (first thesis) to be submitted by around October 2017. All the courses are in English and given by guest Professors from renown Universities. In the end of 2016 I attended Global IP and Sustainable Development, by Professor Margaret Chon (Seattle University of Law) and Global IT Law, by Professor Michael Geist (University of Ottawa). In May / June 2017 I will attend other two courses: Privacy in the Information State: Challenges and Critique, by Prof. Lisa Austin (University of Toronto Faculty of Law), and Law, Science and Expertise, by Prof. Sheila Jasanoff (Harvard Kenedy School). All the courses have either a take home exam or a final paper to be developed by the student, which in any case are graded and are pre-requisite for the successful completion of the PhD.

Secondment Plan

First secondment occurred between April and May 2017 in UCL (London). During the secondment, thanks to the guidance offered by Prof. Emiliano De Cristofaro, I was able to meet multiple PhD students conducting research in privacy at UCL's computer science department; we were able to discuss our research plans, current developments and theoretical / practical perspectives privacy. I also had the opportunity to meet with senior privacy researchers at UCL, namely Angela Sasse, Georges Danezis, Steven Murdoch and had conference calls with Richard Gomer (South Hampton University), Jane Kaye (Oxford). All the meetings and exchanges above were essential to the development of the ideas involved in my research and the advancement of my work. Also, the fact that I had the opportunity to interact intensely with computer science PhD students is also a valuable opportunity to have a more technical (and less legal) overview of my own research and conceptions of privacy.

Interdisciplinary Training

- Privacy of Personal Health Data, August 2016 (Karlstad, Sweden)
- General Data Protection Regulation – Next Step?, August 2016 (Karlstad, Sweden)
- Introduction to Usability, August 2016 (Karlstad, Sweden)
- Legal Privacy Workshop – Privacy by Design, August 2016 (Karlstad, Sweden)
- The Future of Privacy and Identity Management, August 2016 (Karlstad, Sweden)

Professional Training

- Scientific Paper Writing, August 2016 (Karlstad, Sweden)
- Professional Networking, August 2016 (Karlstad, Sweden)
- Self-Management training, April 2017 (online, offered by Hubert Jäger – Uniscon)

Other Training Activities

- Has monthly meetings with other PhD students researching privacy at Tel Aviv University with the goal of exchanging experiences research insights and new ideas;
- Scheduled one to one meetings with the other Privacy&Us' ESRs to understand their current stage in their respective research, exchange ideas and look for future collaborations.

C. *Networking Activities*

- IFIP Summer School 2016 (22th-26th August 2016, Karlstad, Sweden);
- First network wide event (25th-27th August 2016, Karlstad, Sweden);
- Computers Privacy & Data Protection (CPDP – Jan/2017) in Brussels – Belgium;
- Secondment in April / May 2017 at UCL – organized multiple meetings with UCL's PhD students and senior researchers;
- Second network wide event (29th – 2nd May / June, Vienna, Austria);
- Cyber Week at Tel Aviv University – 25th – 29th June;
- Conference on Behavioural Economics – 16th-17th July.

D. Research Management

- Supervisors are constantly providing guidance on how to conduct research and achieve the desired results.

E. Other activities

Other Activities (professional relevant)
- Created and keeps a blog about privacy: http://www.privacyobserver.com - Keeps a Twitter account related to privacy: https://twitter.com/PrivacyChannel

VII. Signatures

Date & Signature of fellow

Date & Signature of supervisor

Other Activities (professional relevant)
- Created and keeps a blog about privacy: http://www.privacyobserver.com - Keeps a Twitter account related to privacy: https://twitter.com/PrivacyChannel

VII. *Signatures*

Date & Signature of fellow

Date & Signature of supervisor

Privacy preserving cloud service for smart applications

Lamya Abdullah (ESR10), UNISCON (UNI)

Abstract. Smart environments may have an enormous impact on society, sustainability, and the quality of life. It's applications can leverage the advantages of the services provided by cloud computing. However, collected massive amounts of personal and contextual data which are being stored and processed by a third party is becoming one of the main concerns regarding the new trends. Both sectors, smart environment and cloud computing, have great potentials and advantages which make them growing fast and attracting service providers in several domains. Hence, this research focuses on studying privacy threats in such applications and understanding the requirement for an abstract model to provide data privacy.

1 Introduction

The vast potential of smart services and data management, that come under different names such as ubiquitous computing, smart environment or Internet of Things, is becoming increasingly feasible. For the last decades several technologies such as wireless communication, sensing technology, higher storage capacities, processing power and cloud computing, have been developed and advanced to solve various challenges to build smart applications towards the next generation of technological services. However, as theses technologies rapidly advance, users data privacy challenges increase as well *. This document describes research motivation, objectives, methodology and approach and the work time line of the study. Then an overview of studied related work is presented.

1.1 Motivation

In a general smart environment architecture, various sensor equipments are deployed to collect data and monitor an environment of interest. The sensing layer provides large amounts of heterogeneous data, which is later processed, shared and stored for different purposes, such as health-care services, smart-homes, energy consumption, systems risk analysis. Therefore a massive amount of data is produced with the growing exploitation of such applications for which traditional storage and processing trends might not be efficient anymore. Thus the trend is to utilize the power of cloud computing which is expected to play a significant role in the smart environment paradigm [15]. Smart environment applications can leverage the platforms and/or infrastructure services provided by clouds as storage and processing platform [21]. Fig. 1 shows a general architecture for smart environments in which the cloud service hosts the analysis processes and the storage system for the collected data by different types of devices. The stakeholders of the data can be application service providers, cloud service providers — considered as third party— and the application end-users (either data sources or consumers).

Several research and commercial projects have been proposed and developed for smart environment applications on top of cloud infrastructure such as: mobile cloud computing for a health-care system [23], management system for sensing resources [22] and air quality monitoring [14]. The examples, which will be visited again in the related work section, entail application domains where collected data could be very private details, systems design and infrastructure secrets or even general environmental values however the contextual data could reveal personal location and hence movements, habits, activities and behavior of individuals at home, work or in a public spaces. None of the three presented or discussed privacy issues nonetheless the applications heavily depend on the collected users-data. Usually service providers focus on the functionality and challenges of providing the smart and intelligent services, but less are discussing the exact user privacy challenges.

The main concern and perhaps the major challenge in the massive collection of data is security and hence privacy especially as it is being processed, stored, hosted by third parties not only by the application service providers. In order to minimize privacy concerns in such environments several privacy enhancing technologies have been proposed and studied. In this

[*] The author attempts to study these issues within the context of Uniscon GmbH, a company focusing on providing privacy preserving services; such as sealed cloud [29] to its customers

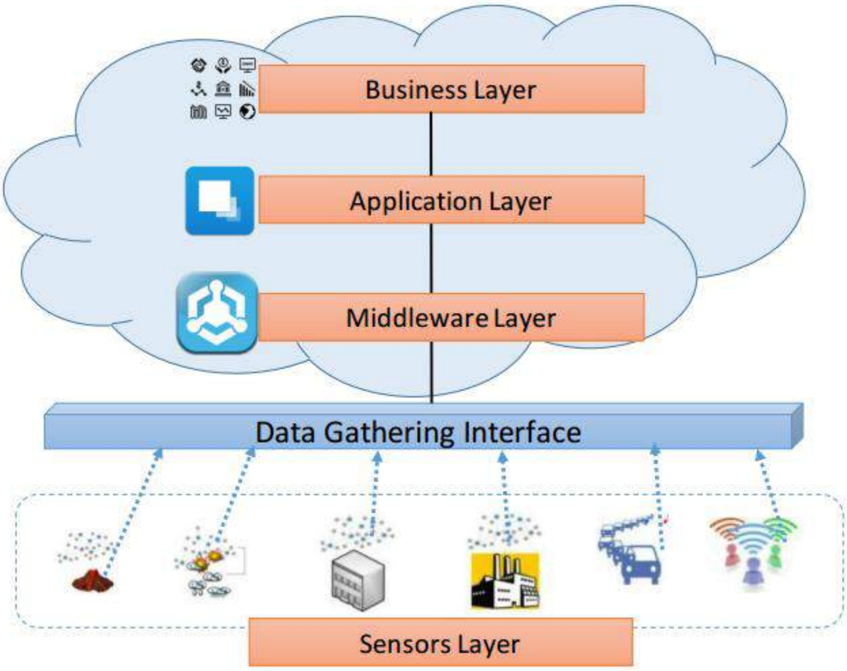


Figure 1: Cloud Services for Smart Environment

research we focus on reducing privacy concerns and studying the threats and the requirements of running smart environment applications using cloud computing platforms.

1.2 Research Objectives

Smart environment applications provide services that heavily depend on collected data that is a potential privacy threat. This research targets to develop understanding of privacy threats related to smart environment applications. The objectives of this research can be summarized by the following questions:

1. How can the privacy problem in smart environment be formally defined?
2. What are the requirements for an abstract model that provide privacy in smart environments?
3. What could be a general model for providing privacy enhancing technology in smart environment application?
4. How could an abstract model be instantiated to a real world application scenario, from a context of a cloud provider company like Uniscon GmbH?
5. What are the design choices for adaptive methods of privacy protection in a given application scenario?

6. How can different designs be evaluated?
7. What are the practical trade-offs of devising adaptive methods in real-life applications?

1.3 Research Approach

To fulfill the main objectives of the study, we first want to understand the theoretical part via analyzing and formalizing requirements and related concepts to be able to communicate about them. Then we aim to design a model that provides data privacy and build a concrete a prototype using sealed cloud [29] to better understand the practical design problems such as efficiency, security and data privacy. The research will be conducted in three main phases, as illustrated below.

1.3.1 Understanding Theoretical concepts

During the first phase of the study, we investigate the concept of sealing and design a formal model to understand sealing as mentioned in the literature and as implemented in practice. Sealing is defined as the ability to limit access to data and computation and to bind processing to a particular authorized hardware environment. During this stage, the Secure Multi-party Computation (SMC) problem is studied in the context of protocol designing, as SMC is a problem for which data privacy is a crucial requirement. The design process aims in understanding the properties provided by the sealing concept and how it can be integrated into a model that achieves possible solution for the SMC problem.

1.3.2 Requirement Analysis

Requirement analysis phase is based on the findings in the privacy protection in smart environment literature. Basic requirements shall be gathered based on a critical analysis for previous work and also based on the understanding of practical concepts. For example, Langheinrich in 2002 suggested general requirements for privacy awareness ubiquitous computing [31] and recently Bettini et al. [7] presented privacy threats and requirements for different domains in a smart environment. Moreover, the analysis shall consider the properties defined in the previous phase. Furthermore, an application scenario will be studied or concrete requirements analysis. A candidate application is “connected cars”, in which cars are equipped with different sensors. Data is collected and sent to the cloud to be stored, processed and analyzed, Fig 2. The result is then shared with corresponding stakeholder. Application scenarios could be: user-behavior evaluation for insurance companies, car maintenance, road maintenance. The result of this phase will present the main blueprint for designing a prototype to instantiate an abstract privacy preserving model.

1.3.3 Design, implementation and Evaluation of a Prototype

To design a prototype based on the requirements set, a general model shall be devised first by interpreting the requirements into implementable practical properties. Then we are planing to implement the prototype to evaluate the designed model for practical efficiency and applicability.

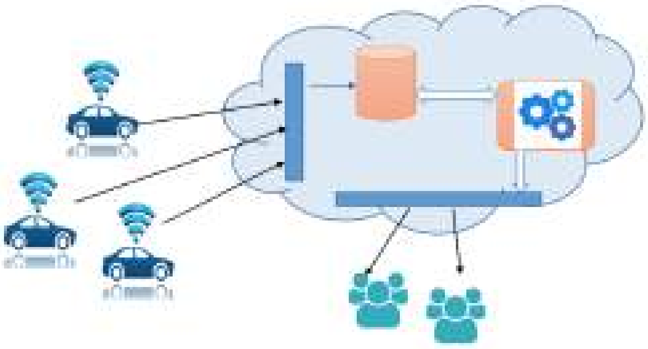


Figure 2: Connected cars application

The evaluation will include an empirical and quantitative study based on experiments to be run on the implemented prototype.

1.4 Work Plan

The proposed doctoral study time line is demonstrated in Fig.3. It starts by conducting a literature review, broken into three categories: the state of art, understanding the theoretical and practical concepts, respectively. This will enable better identification of the technical requirements to design and implement the potential prototype. The literature review will remain as a continuous task that goes in parallel during the entire time of the study. Furthermore, some tasks such as requirements analysis and design can be iterative and inter-related. So is the evaluation phase, which includes an experimental/empirical and quantitative study for the prototype, it will overlap with implementation and might be in an iterative mode as well. The writing process shall be going on in parallel during the time line, for both the final thesis submission and possible disseminations as demonstrated in the figure by “X”.

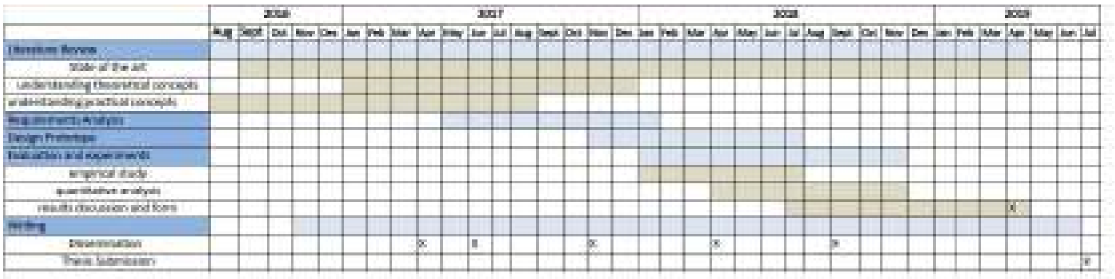


Figure 3: The PhD study Time Plan

2 Related Work

The body of work that studies privacy preserving solutions in smart environment applications and/or cloud computing is expanding as the demand for both the service and data security and privacy increases. A number of projects have been already proposed and deployed on top of cloud infrastructures such as mobile cloud computing for a health-care system [23] in which biomedical signals are collected from multiple locations via mobile devices as a monitoring terminal. Furthermore, a personalized health-assistant is installed to provide health summaries. Collected data is synchronized into the dedicated health-care cloud computing service. Hence, the service is seamlessly anytime and anywhere available under network connection. Another example is a management system for sensing resources. Fazio and Puliafito [22] present a cloud framework that enables users to choose the type of cloud service they need. The framework combines data-centric and device-centric models and it was designed based on the specifications of Sensor Web Enablement standard. Chen et al. presented a real system deployed to monitor indoor air quality inside offices of Microsoft in China and to collect outdoor air quality [14]. The system analyzes air quality data collected over a long period and can provide employees information to guide their decision making. Furthermore, the system was designed to offer actionable and energy-efficient suggestions to “heating, ventilation and air conditioning” systems. The common feature among the three example is that they rely on the cloud to provide the service.

In order to understand the privacy risks in such environments, we need to understand cloud computing at first, the following subsection illustrates a general background of cloud computing. Then the next subsections illustrate the related work which has been studied so far for the sake of developing good understanding of the theoretical and practical foundations for the study.

2.1 General Background of Cloud Computing

Cloud computing is the service of providing on-demand resources from applications to data centers and computing resources. It is evolving and growing fast as many new players are getting into the service environment (marketplace) [25]. A strict cloud computing definition has not been an easy task in IT industry. Several organizations came up with concrete definitions, such as IBM, ENISA (European Network and Information Security Agency) [20] and NIST(National Institute of Standards and Technology) [36]. Cloud computing is defined in the ISO/IEC 17788 as:*“paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand”*, where resources include storage, software, applications, networks, operating systems and servers [27]. Cloud consumers (business owners, organizations who provide application services, end users) are able to provision certain level of cloud services from cloud providers. It is the result of various computing disciplines interaction [1] and thus it inherits general distributed information systems characteristics in addition to it’s own characteristics.

The definition of the cloud model is composed of essential characteristics that cloud consumers should expect from cloud providers, three service models and four deployment models, in both ISO/IEC and NIST definitions [27, 36].

Essential characteristics of the cloud

Cloud computing in general has a number of identified characteristics: scalability of infrastructure, location independence, reliability, flexibility and elasticity of resources provisioning [46]. By utilizing a well designed visualization of storage and computing power, cloud can provide elastic, dynamic, scalable and shared resources. That yields availability, one of the unique characteristics of cloud [1]. Detailed characteristics as been presented by the standards could be summarized as:

- *On-demand self-service*: cloud consumers can provision capabilities as needed automatically without or with minimum interaction with the provider.
- *Resource pooling*: cloud providers' physical or virtual resources are pooled and aggregated to serve more than one consumer with resources assigned and reassigned to consumers dynamically. This directly ensures the Multi-tenancy feature.
- *Multi-tenancy:* resources are assigned and allocated in a way that can serve multiple consumers while keep their data and computations inaccessible to and isolated from each other.
- *Broad network access:* resources are available over network and can be accessed via heterogeneous thin or thick client platforms.
- *Measured service:* a metered delivery of the service to provide transparency for both provider and consumers, where resource usage can be monitored controlled and reported.
- *Rapid elasticity and scalability:* to consumers, capabilities available for provisioning appear to be unlimited due to resource elastic provision and release capabilities.

Service models of the cloud

- *Infrastructure as a Service* (IaaS): a cloud consumer is provided a controlled access to the virtual infrastructure and is able to deploy and run software (operating systems and applications). The consumer is provided to provision processing, storage, network and fundamental computing resources.
- *Platform as a Service* (PaaS): cloud consumer is provided to provision platform-related tools and operating system so consumers can deploy or acquire applications created by tools provided by the cloud provider.
- *Software as a Service* (SaaS): a consumer is using the providers application running on the cloud which accessed from various client interfaces. The consumer does not manage the underlying infrastructure including operating systems and applications configuration with possible exceptions for user-specific application settings.

Further service models include Communications as a Service (CaaS), Compute as a Service (CompaaS),Data Storage as a Service (DsaaS). Recently, with the rapid growth of service provisioning, the term XaaS X as a Service has emerged to describe anything as a Service.

Deployment models of cloud

Clouds can be deployed following four deployment models: public, private, hybrid and community. The public cloud is the most common deployment model in which the physical infrastructure is shared by multiple cloud clients. The architecture and infrastructure security are the responsibility of the service provider in this model. While in the private cloud, a single organization or its multiple business units use the cloud service. This type of cloud can be hosted on organization premises or somewhere else, moreover, it can be owned and managed by the cloud service provider, the organization itself, or both. Hybrid cloud and community cloud are less popular, yet. In the community model, a specific community of clients or organizations that share some interests use the deployed cloud which could be owned by one or more of the organizations in the community. Finally, the hybrid model is the mix of two or more cloud models deployed together to enable data and application portability [1].

Data security, privacy and trust are the most important factors that could block or allow consumers to migrate their data, application and/or business and base their valuable data on the cloud while they might feel as they are loosing control over their data and computations. In the current trend, security is managed through policies and Service Level Agreements (SLA) that is the foundation of services between consumers and providers [12]. Cloud security standards such ISO/IEC 27017 provides a code of practice of information security for cloud computing based on the ISO 27001 and 27002 information security standards. ISO 27017 suggests additional security controls which are specific for the cloud those are not covered in information security standards ISO/IEC 27001 and 27002. These are shared roles and responsibilities within a cloud computing environment, removal of cloud service customer assets, segregation in virtual computing environments, virtual machine hardening, administrators operational security, cloud services monitoring. Additional standard —ISO/IEC 27018— focuses more on the cloud providers who are processing *Personal Identified Information* (PII). So cloud companies with lots of PII probably shall consider the three standards 27001, 27017 and 27018.

2.2 Trusted computing

The term of trusted computing is taken from the field of trusted systems. In trusted computing, the machine behaves in expected ways consistently, those behaviors are enforced by computer hardware and software [37]. The field of trusted computing was studied to understand other proposed solutions for cloud security and/or secure multi party computation which were based on properties provided by Hardware Security Modules (HSMs). HSMs are physical computing devices that mainly manage and protect digital keys and provide tamper-proof property. Additional key concept in trusted computing is “secure boot” which allows only signed and verified code and drivers to be loaded during boot process.

Among concepts of trusted computing, we focused on both remote attestation and sealed storage, due to their usage to provide data security in distributed systems. In the *Trusted Platform Module* (TPM), England and Peinado [19] introduced an abstraction called *sealed storage*, a possibility of “programs to store long lived secrets” [18]. The abstraction encrypts data for the program, but key handling is done within the abstraction, i.e., the program does not get to see the key, and decryption (i.e., unsealing) is performed by the abstraction only for the program that initiated the original sealing operation. The abstraction provided by the TCG group are used as a platform for security and software attestation— one example is [39] which will be illustrated in the discussion of work related to trust in cloud computing, later.

2.3 Privacy metrics and Data privacy in smart environment

Many studies have been trying to address privacy issues in different domains in information technology in general and in smart environment applications in particular. This subsection illustrates examples of such studies presented over the past years. Recently, Bertino [6] discussed general security and privacy concepts and research directions for Big Data as sub-domain of smart environments. Before that, Bettini et al. [7], presented a state of the art of privacy threats and requirements in several application domains for ubiquitous computing. In their survey they classified privacy preserving approaches for smart environment applications and categorized them under five categories: Access-control, Obfuscation, Anonymity, Cryptography and Privacy-preserving Data mining. Furthermore, adversaries and third parties were identified for applications categories. Another survey was conducted in 2015 by Wagner and Eckhoff [44] and presented six domains of privacy studies: Databases, Communication Systems, Communication Systems, Smart Metering, Genome Privacy and Social Networks. The result of this survey is a taxonomy of over eighty privacy metrics. The presented metrics are helpful to measure the degree of privacy enjoyed by users in a system depending on the application domain.

Furthermore, number of studies discussed privacy for specific applications such as location-service [5], smart home automation systems [28] and smart calenders [40]. Langheinrich [31] introduced a privacy-aware system that allows data collectors to announce and implement data usage policies. Although the implemented system cannot guarantee the privacy, the author argues that it can create a sense of accountability. Finally, it is worthy to mention a recent work by Alohaly and Takabi [2] which focused on analyzing applications policy text to quantify data collection practice by locating the text segments that are relevant to collection practices. The main goal of the study was to provide the applications users an indicator of the amount of collected data and privacy.

2.4 Security, privacy and trust in cloud computing

One major challenge for smart environment applications is to utilize the cloud capabilities is the user data privacy due to number of challenges related to data security, privacy and trust in the field of cloud computing. Several studies have been proposed to provide secure solutions and hence ensure data privacy in the cloud via providing data confidentiality, access control and increasing trust in the service provider. Recently, large amounts of diffident kinds of surveys were published as the number of work discussing cloud issues increased; such as Takabi et al. [42], Hashizume et al. [26] and Singh et al. [41]. Additionally, Lorunser et al. [33] presented the EU Project Prismacloud which aims to address security and privacy issues in cloud and to provide technologies based on cryptography means to deploy a privacy enabled cloud service.

A great focus is shown on *trust* in cloud computing as it is one of the major requirement for consumers to move their data to the cloud. Trust was described as the facilitator in cloud computing [25]. Moreover, Brown and Chase [10] showed how users can gain trust into service applications. They addressed the issue of how to build support for trustworthy services in the cloud within the context of a larger trust management framework. The applications of such kind of work could be extended furthermore if the provided platform was proven to be trusted. One remarkable study was presented by Santos et al. [39] who extended the primitives provided by trusted computing to be adopted in a cloud service by adding seal and unseal primitives. The primitive of sealing uses policy attributes to ensure that the unsealing operation will only take place on a cloud node whose attributes matches the sealing policy. Basic target was to provide the cloud customers/consumers the trust that their data is only accessible in correct nodes.

One of the practical solutions is Sealed Cloud [29] developed in Uniscon GmbH. It aims to prevent cloud administrators and operators from accessing users' data either privileged or unprivileged. The basic mechanisms to achieve this goal are the so-called *data clean-up*, the *purely volatile keeping of keys*, and a *full chain of trust*[29]. Sealed cloud will be the platform on top of which the model in this study will be created and instantiated.

2.5 Secure Multi-party Computation

The problem of Secure Multi-party Computation (SMC) [45] is generally defined as follows a set of parties wishes to correctly compute some common function F of their local inputs. Unfortunately, the parties do not trust each other, nor the channels by which they communicate, but they want to keep their local data as private as possible. If there exists a single third party that is mutually trusted by all other parties, then the problem is easy to solve. However, solving SMC becomes challenging as this assumption is not applicable. We can distinguish proposed solutions and studies for SMC into two categories: cryptography-based and non-cryptography based solutions.

The publication of the first protocols for SMC that do not rely on a trusted third party [13] spawned a substantial body of work, starting from investigations of synchronous computation models. Much progress has been made since, especially regarding practical and efficient SMC protocols for two parties such as in [34, 35, 32, 30]. All these can be considered purely cryptography-based solutions.

On the other hand, non-cryptography based solutions have been proposed. Avoine and Vaudenay [4] examined the approach of jointly simulating a Trusted Third Party (TTP) using hardware security modules. This approach was later extended by Avoine et al. [3] who show that in a system with security modules, the problem of fair exchange can be reduced to a special form of consensus. Then the TrustedPals system [24] extended this idea to the general problem of SMC and it was shown that the use of security modules could not improve the resilience of SMC. A correct majority of parties was still needed. Cortiñas et al. [16] extended TrustedPals with a very weak synchrony assumption to reduce SMC to the problem of uniform consensus.

Over the years, several studies have been presenting solutions for SMC for some specific scenarios or problems. Du and Atallah [17] developed a framework to identify the set of computation problems domains where SMC has been used. Those domains include privacy-preserving intrusion detection, geometric computations, database query, statistical analysis, and data mining. Later, Orlandi [38] presented the advancement of the generic SMC practical solutions till the year of the study. However, SMC was not just discussed in the generic mode in the recent years, e.g. Titze et al. [43] extended the SEPIA, a practical implementation library of SMC [11], to anonymize the originator of an arbitrary input data; and Bogdanov et al. [9] deployed a framework for data collection and analysis system on top of Sharemind [8]. Sharemind is a distributed virtual machine for performing privacy-preserving computations (SMC) on integer and boolean inputs.

The problem of SMC, will be used in the context of formal modeling the smart environment applications scenario.

References

[1] Mohammed M. Alani. *Elements of Cloud Computing Security*. 2016.

[2] Manar Alohaly and Hassan Takabi. Better privacy indicators: A new approach to quantification of privacy policies. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, Denver, CO, 2016. USENIX Association.

[3] Gildas Avoine, Felix C. Gärtner, Rachid Guerraoui, and Marko Vukolic. Gracefully degrading fair exchange with security modules. In *Dependable Computing - EDCC-5, 5th European Dependable Computing Conference, Budapest, Hungary, April 20-22, 2005, Proceedings*, pages 55–71, 2005.

[4] Gildas Avoine and Serge Vaudenay. Optimal fair exchange with guardian angels. In *Information Security Applications, 4th International Workshop, WISA 2003, Jeju Island, Korea, August 25-27, 2003, Revised Papers*, pages 188–202, 2003.

[5] Alastair R. Beresford and Frank Stajano. Mix zones: User privacy in location-aware services. In *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, PERCOMW '04, pages 127–, Washington, DC, USA, 2004. IEEE Computer Society.

[6] Elisa Bertino. Data security and privacy: Concepts, approaches, and research directions. In *Computer Software and Applications Conference (COMPSAC), 2016 IEEE 40th Annual*, volume 1, pages 400–407. IEEE, 2016.

[7] Claudio Bettini and Daniele Riboni. Privacy protection in pervasive systems: State of the art and technical challenges. *Pervasive and Mobile Computing*, 17:159–174, 2015.

[8] Dan Bogdanov, Sven Laur, and Jan Willemson. *Sharemind: A Framework for Fast Privacy-Preserving Computations*, pages 192–206. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.

[9] Dan Bogdanov, Riivo Talviste, and Jan Willemson. *Deploying Secure Multi-Party Computation for Financial Data Analysis*, pages 57–64. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.

[10] Andrew Brown and Jeffrey S. Chase. Trusted platform-as-a-service: A foundation for trustworthy cloud-hosted applications. In *Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop*, CCSW '11, pages 15–20, New York, NY, USA, 2011. ACM.

[11] Martin Burkhart, Mario Strasser, Dilip Many, and Xenofontas Dimitropoulos. Sepia: Privacy-preserving aggregation of multi-domain network events and statistics. In *Proceedings of the 19th USENIX Conference on Security*, USENIX Security'10, pages 15–15, Berkeley, CA, USA, 2010. USENIX Association.

[12] Victor Chang, Yen-Hung Kuo, and Muthu Ramachandran. Cloud Computing Adoption Frameworka security framework for business clouds. *Future Generation Computer Systems*, 57:24–41, 2015.

[13] David Chaum, Ivan Damgård, and Jeroen van de Graaf. Multiparty computations ensuring privacy of each party's input and correctness of the result. In *Advances in Cryptology - CRYPTO '87, A Conference on the Theory and Applications of Cryptographic Techniques, Santa Barbara, California, USA, August 16-20, 1987, Proceedings*, pages 87–119, 1987.

[14] Xuxu Chen, Yu Zheng, Yubiao Chen, Qiwei Jin, Weiwei Sun, Eric Chang, and Wei-Ying Ma. Indoor air quality monitoring system for smart buildings. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '14, pages 471–475, New York, NY, USA, 2014. ACM.

[15] V. Coroama, J. Bohn, and F. Mattern. Living in a smart environment - implications for the coming ubiquitous information society. In *2004 IEEE International Conference on Systems, Man and Cybernetics (IEEE Cat. No.04CH37583)*, volume 6, pages 5633–5638 vol.6, Oct 2004.

[16] Roberto Cortiñas, Felix C. Freiling, Marjan Ghajar-Azadanlou, Alberto Lafuente, Mikel Larrea, Lucia Draque Penso, and Iratxe Soraluze Arriola. Secure failure detection and consensus in trustedpals. *IEEE Trans. Dependable Sec. Comput.*, 9(4):610–625, 2012.

[17] Wenliang Du and Mikhail J. Atallah. Secure multi-party computation problems and their applications: A review and open problems. In *Proceedings of the 2001 Workshop on New Security Paradigms*, NSPW '01, pages 13–22, New York, NY, USA, 2001. ACM.

[18] Paul England and Marcus Peinado. Authenticated operation of open computing devices. In *Information Security and Privacy, 7th Australian Conference, ACISP 2002, Melbourne, Australia, July 3-5, 2002, Proceedings*, pages 346–361, 2002.

[19] Paul England and Talha Tariq. Towards a programmable TPM. In *Trusted Computing, Second International Conference, Trust 2009, Oxford, UK, April 6-8, 2009, Proceedings*, pages 1–13, 2009.

[20] European Network ENISA and Information Security Agency. Cloud Computing - Benefits, Risks and Recommendations for Information Security. Technical Report 1, 2012.

[21] M. Fazio, A. Celesti, A. Puliafito, and M. Villari. Big data storage in the cloud for smart environment monitoring. *Procedia Computer Science*, 52:500 – 506, 2015.

[22] M. Fazio and A. Puliafito. Cloud4sens: a cloud-based architecture for sensor controlling and monitoring. *IEEE Communications Magazine*, 53(3):41–47, March 2015.

[23] Ee-May Fong and Wan-Young Chung. Mobile cloud-computing-based healthcare service by noncontact ecg monitoring. *Sensors*, 13(12):16451–16473, 2013.

[24] Milan Fort, Felix C. Freiling, Lucia Draque Penso, Zinaida Benenson, and Dogan Kesdogan. Trustedpals: Secure multiparty computation implemented with smart cards. In *Computer Security - ESORICS 2006, 11th European Symposium on Research in Computer Security, Hamburg, Germany, September 18-20, 2006, Proceedings*, pages 34–48, 2006.

[25] Sheikh Mahbub Habib, Sascha Hauke, Sebastian Ries, and Max Mühlhäuser. Trust as a facilitator in cloud computing: a survey. *Journal of Cloud Computing: Advances, Systems and Applications*, 1(1):19, 2012.

[26] Keiko Hashizume, David G. Rosado, Eduardo Fernández-Medina, and Eduardo B. Fernandez. An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4(1):5, 2013.

[27] Recommendation ITU-T. ISO/IEC 17788 - Information technology - Cloud computing - Overview and vocabulary. (Y.3500):1–16, 2014.

[28] A. Jacobsson, M. Boldt, and B. Carlsson. On the risk exposure of smart home automation systems. In *2014 International Conference on Future Internet of Things and Cloud*, pages 183–190, Aug 2014.

[29] Hubert A Jäger, Arnold Monitzer, Ralf Rieken, Edmund Ernst, and Khiem Dau. Sealed cloud–a novel approach to safeguard against insider attacks. pages 15–34, 2014.

[30] Vladimir Kolesnikov. Gate evaluation secret sharing and secure one-round two-party computation. In *Advances in Cryptology - ASIACRYPT 2005, 11th International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, December 4-8, 2005, Proceedings*, pages 136–155, 2005.

[31] Marc Langheinrich. A privacy awareness system for ubiquitous computing environments. In *UbiComp 2002: Ubiquitous Computing, 4th International Conference, Göteborg, Sweden, September 29 - October 1, 2002, Proceedings*, pages 237–245, 2002.

[32] Yehuda Lindell and Benny Pinkas. An efficient protocol for secure two-party computation in the presence of malicious adversaries. *J. Cryptology*, 28(2):312–350, 2015.

[33] Thomas Lorünser, Charles Bastos Rodriguez, Denise Demirel, Simone Fischer-Hübner, Thomas Groß, Thomas Länger, Mathieu des Noes, Henrich C. Pöhls, Boris Rozenberg, and Daniel Slamanig. *Towards a New Paradigm for Privacy andSecurity in Cloud Services*, pages 14–25. Springer International Publishing, Cham, 2015.

[34] Philip D. MacKenzie, Alina Oprea, and Michael K. Reiter. Automatic generation of two-party computations. In *Proceedings of the 10th ACM Conference on Computer and Communications Security, CCS 2003, Washington, DC, USA, October 27-30, 2003*, pages 210–219, 2003.

[35] Dahlia Malkhi, Noam Nisan, Benny Pinkas, and Yaron Sella. Fairplay - secure two-party computation system. In *Proceedings of the 13th USENIX Security Symposium, August 9-13, 2004, San Diego, CA, USA*, pages 287–302, 2004.

[36] Peter Mell and Timothy Grance. NIST definition of cloud computing. Technical report, 2011.

[37] C. Mitchell and Institution of Electrical Engineers. *Trusted Computing*. Computing and Networks Series. Institution of Engineering and Technology, 2005.

[38] C. Orlandi. Is multiparty computation any good in practice? In *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 5848–5851, May 2011.

[39] Nuno Santos, Rodrigo Rodrigues, Krishna P. Gummadi, and Stefan Saroiu. Policy-sealed data: A new abstraction for building trusted cloud services. In *Proceedings of the 21st USENIX Conference on Security Symposium*, Security'12, pages 10–10, Berkeley, CA, USA, 2012. USENIX Association.

[40] F. Schaub, B. Knings, and M. Weber. Context-adaptive privacy: Leveraging context awareness to support privacy decision making. *IEEE Pervasive Computing*, 14(1):34–43, Jan 2015.

[41] Saurabh Singh, Young-Sik Jeong, and Jong Hyuk Park. A survey on cloud computing security: Issues, threats, and solutions. *Journal of Network and Computer Applications*, 75:200 – 222, 2016.

[42] H. Takabi, J. B. D. Joshi, and G. J. Ahn. Security and privacy challenges in cloud computing environments. *IEEE Security Privacy*, 8(6):24–31, Nov 2010.

[43] D. Titze, H. Hofinger, and P. Schoo. Using secure multiparty computation for collaborative information exchange. In *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pages 1717–1722, July 2013.

[44] Isabel Wagner and David Eckhoff. Technical privacy metrics: a systematic survey. *CoRR*, abs/1512.00327, 2015.

[45] Andrew Chi-Chih Yao. Protocols for secure computations (extended abstract). In *23rd Annual Symposium on Foundations of Computer Science, Chicago, Illinois, USA, 3-5 November 1982*, pages 160–164, 1982.

[46] Dimitrios Zissis and Dimitrios Lekkas. Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3):583–592, 2012.

Lamya Abdullah (ESR10), UNISCON (UNI)

Career Development Plan Year 1

I. *Personal and Organizational Information*

ESR´s Personal Information			
Name:	**Lamya Abdullah**	**ID number**:	
Office Address:	Uniscon GmbH, Agnes-Pockels-Bogen 1, 80992 München, Germany	**Phone**:	+49 89 41615987
Mobile:	+49 17629209386	**E-Mail:**	Lamya.abdullah@uniscon.de

ESR´s Host Organization Information			
Name:	**Uniscon Universal Identity Control GmbH**	**Phone**:	+49 89 41615987
Address:	Agnes-Pockels-Bogen 1, 80992 München, Germany		

II. Supervision

Supervision			
Supervisor´s Name:	**Felix C.Freiling**	**Title**:	Prof.Dr.-Ing
Place of Employment:	Friedrich-Alexander-University Erlangen	**Phone**:	+49 9131 85 69901
Responsibility Distr.:	%	**E-Mail:**	felix.freiling@cs.fau.de
Co-Supervision			
Co-Supervisor´s Name:	**Hubert Jäger**	**Title**:	Dr.
Place of Employment:	Uniscon Universal Identity Control GmbH	**Phone**:	+49 89 41615987
Responsibility Distr.:	%	**E-Mail:**	
Co-Supervision **Co-Supervision**			
Co-Supervisor´s Name:	**Claudio Bettini**	**Title**:	Prof.
Place of Employment:	EveryWare Technologies *University of Milan*, *Italy*	**Phone**:	+39 02 503 16281
Responsibility Distr.:	%	**E-Mail:**	claudio.bettini@unimi.it
Conduct of Supervision (per activity describe form of supervision and estimated supervision hours)**:**			

- supervision by supervisor:

- Regular supervision meetings are held weekly, the duration in average 1.5 H, less or more based on task and required organization.
- Cooperative brainstorming, writing, training and research related orientation.
- Scientfic discussions.

- supervision by co-supervisor 1:

- practical requirement understanding and discussions and organizational tips (frequent meetings and according to needed discussion)
-

- supervision by co-supervisor 2:

- scientific discussion and feedback (every month and a half in average), for the next stage more frequent discussions shall be held.

III. Secondment

ESR´s Secondment			
Supervisor’s Name:	**Simone Fischer-Hübner**	**Title**:	Prof.Dr.
Organization´s Name:	Karlstad University	**Phone**:	+46 54 700-1723
Address:	Universitetsgatan 2, 651 88 Karlstad	**E-mail:**	simone.fischer-huebner@kau.se

IV. Research Project

ESR´s Project			
Title:	**Adaptive data privacy for smart environments**	**Ref. No:**	10
Overview and background			

Smart environments may have an enormous impact on society, sustainability, and the quality of life. It's applications can leverage the advantages of the services provided by cloud computing. However, collected massive amount of personal and contextual data which being stored and processed by a third party is becoming one of the main concerns regarding the new trends. Both sectors, smart environment and cloud computing, have great potentials and advantages which make them growing fast and attracting service providers in several domains. Hence, this research focuses on studying privacy threats in such applications

V. Long-Term Career Objectives

Long-Term Career Objectives (over five years)
Completing PhD study, my primary long term objective is to find a research position, either in the form of post-doctoral only research and/teaching in an academic institution. I would prefer to do some teaching so that I can share the experience and knowledge I am developing during my training time. Idealy I would prefer to research in the field of data analysis and privacy challenge, and preserving approches to participate in the trend of protecting users of the ongoing developing technology. To develope more knowledge in the field of the data analysis, I will seek training in the recent trends for the data analytics, together with technical experience I have, to enhance understanding so that to integrate privacy protection tenchique within the process.

For the career after finishing the doctoral degree, not only scientific skills or technical skills are needed. I believe the training program in Privacy&US is providing me wide range of skills which broden interdiciplinary- aspects to broden my knowledge and view of researchproblems and challenges. In addition to dessemination skills as well as interpersonal and communication skills I need to practice communicating results, findings and ideas.

VI. Short-Term Career Objectives

A. Project Research Results

Project Research Results
Presented according to Privacy & Us project Plan.

Milestones	Expected Results
Literature undersatnding (M20)	Develop undersatnding of the requirements in literature
Writing research plan (M18)	Proposing novel approaches to address the gaps identified in the literature
Career development plan (M18)	Development initial plan toward career after the doctoral studies
Privacy requirement analysis (M18)	Analysing the privacy requirements and privacy principles which are essential for smart environment applications as part of deliverable report.
User interface requirement analysis (M18)	Analysing the user interface and usability requirements which are essential for smart environment applications as part of deliverable report.

Deliverables
D2.1: Requirements Analysis (M18) D4.1: User Interface Requirements (M18) D5.1: Privacy Principles (M20) D6.7: Researcher Declarations and Career Development Plan (M18)

Anticipated Publications
- 22nd symposium of ESORICS 2017, Oslo, Norway on September 11-13 2017 **Submission**: “*Implementing Secure Multiparty Computation using Sealing”* *-A work -in-progress: a SOK of privacy preserving studies for cloud computing – how is privacy addressed and/or implemented in cloud computing.*

Anticipated Conference/Workshop Attendance & Courses/Seminar Presentations
- COINS/SWITS Ph.D. student seminar 2017 (Oslo) 7-9 June 2017, - 12th IFIP Summer School on Privacy and Identity Management - the Smart World Revolution, Ispra, Italy, 3-8 September 2017

B. Training

Research and Technical Training

- Introduction to PETs, August 2016 (Karlstad, Sweden)
- Privacy Enhancing Technologies, January 2017 (Online Module)

Secondment Plan

Please see Appndix -1

Interdisciplinary Training

- Privacy of Personal Health Data, August 2016 (Karlstad, Sweden)
- General Data Protection Regulation – Next Step?, August 2016 (Karlstad, Sweden)
- Introduction to Usability, August 2016 (Karlstad, Sweden)
- Legal Privacy Workshop – Privacy by Design, August 2016 (Karlstad, Sweden)
- The Future of Privacy and Identity Management, August 2016 (Karlstad, Sweden)

Professional Training

- Scientific Paper Writing, August 2016 (Karlstad, Sweden)
- Professional Networking, August 2016 (Karlstad, Sweden)

Other Training Activities

- Participated in paper review- for conference ESORICS2017

C. *Networking Activities*

- First network wide event (25th-27th August 2016, Karlstad, Sweden)
- Secondment in Karlstad (May 2017 – June 2017).
- Privacy&Us-Training Events (August 2016 in Karlstad; June 2017 in Vienna).
- Cooperation with fellow ESRs.

D. Research Management

Online corse - Self management (April 2017)

E. Other activities

Other Activities (professional relevant)

Risk analysis evaluation, a study to quantify data confidentiality in SaaS cloud service.

VII. Signatures

Date & Signature of fellow

Date & Signature of supervisor

Appendix-1:
Secondment Research Plan – Briefly
discussing and working with you and the team on enhancement for a paper that we are submitting. Kindly find the attached file, please.

- Discussion /sharing /feedback for research questions and research ideas and findings.
In addition to discussion for implementation of Privacy technologies on clouds involving user's preferences.
- Continue preparing research proposal/cdp and presentation.

- Discussing and working on further enhancement for the paper "Solving Secure Multiparty Computation using Sealing"- The paper presents a system model on which the Secure Multiparty Computation (SMC) problem can be solved, the system model is based on sealing concept.
One of the possible next steps (further enhancement) will be adjusting the presented protocol to achieve the privacy property of the SMC.
Referring to the paper, Lemma 4 (the privacy Lemma), It would be much stronger proved if a privacy-preserving implementation for the communication protocol - the Uniform Reliable Broadcast (URB). So we can ensure that the final protocol is information-leakage resilient, thus achieving anonymity of both (senders and receivers) and to provide unobservability of the exchanged values to fulfill the property described in Lemma 4.
Maybe we can think about some generic approach that relays on an unobservability layer which could perform message piggybacking, or we could think about a specific design approach that makes the communication protocol more resilient with higher efficiency.

Privacy-Preserving Personal Genomic Testing

Alexandros Mittos (ESR11), University College London (UCL)

Abstract. Advances in biomedical research with genomic data have improved the quality of medical services, whilst in parallel created significant privacy concerns for people whose data has been collected [1]. To date, there are works in the literature that provide technical and legal solutions to these concerns, but without focusing on the needs of the end-user. This documents serves as the research proposal the early stage researcher (ESR) intends to conduct during his scholarship of Privacy&Us, a project funded by the European Union's Horizon 2020 research and innovation program within the Marie Skłodowska-Curie Innovative Training Networks (ITN-ETN) framework. This research will focus on the field of genomic privacy from a user perspective; identify users' perceptions to genomics, with the end-goal of informing the design of a user-centric secure personal genome testing infrastructure. A mixed methods approach will be used in order to identify the users' needs, by conducting quantitative and qualitative studies. At the end of these studies, we hope our research will enable users to benefit from the advances in genomics testing services whilst protecting their privacy.

1 Introduction

The reduced costs of human genome sequencing, advances in the biomedical community, and the tendency to create and store hundreds of thousands of sequenced genomes (a) will have an impact on the quality of services available to users worldwide for the better and (b) has the potential to become a privacy liability to the DNA donors and their relatives [1].

Genomic Privacy is the research field that tries to provide to researchers ways of using the advances biomedical research has achieved, whilst protecting the privacy of its users. So far, there are works in the literature that provide both technical and legal solutions to these problems, but very few of these works focus on the user's concerns, attitudes, and perceptions in regards to genomics and privacy.

In order to address this we aim to focus our research in genomic privacy from a user-centered perspective. We plan to identify the users' concerns and perceptions, using quantitative and qualitative methods, with the goal to design a user-centered secure personal genome testing infrastructure with an effective, meaningful, and usable user interface which will enable users to control and access genomic data.

2 Background

During the last 15 years the world witnessed the rapid drop of genome sequencing costs. The first human genome was sequenced in 2003, by the Human Genome Project which lasted 13 years and cost \$3B [2, 3]. In 2017, a complete sequence of human genome costs less than \$1,000 [4]. One of the results of this massive drop in price was the transition from traditional medicine to personalized medicine. This promising new way of medicine allows physicians to better assess the disease susceptibility of their patients, understand better how these diseases will affect them, and allows the physicians to evaluate the optimal therapy for each patient, by examining the unique characteristics of ones genome.

In 2006, a company called 23andMe was founded, offering direct-to-consumer (DTC) genetic testing and providing ancestry and health reports to its consumers. These health reports contain the disease susceptibility of the individual to certain diseases (i.e., Alzheimer's disease), a carrier status report (i.e, if the donor caries the variant of beta thalassemia), and wellness reports (i.e., how efficiently the individual metabolizes caffeine). Ancestry reports exist for recreational reasons and allow the individual to know their genetic heritage.

Shortly after, dozens of similar companies surfaced all around the world, providing similar or more specialized services. This tendency affected governments as well, and as a result, in the last five years we witnessed the birth of many governmental genomic projects. These projects aim to build biorepositories containing the sequenced genomes of hundreds of thousands of patients in the hopes of providing better healthcare for their patients. Genomics England, a Department of Health project funded by the UK government, aims to sequence 100,000 genomes of NHS patients by the year 2017 [5], while on the other side of the Atlantic ocean, the US government in 2015 announced the Precision Medicine Initiative [6].

As promising as it is though, sequencing genomic data can lead to a series of privacy threats which arise from the unique aspects DNA consists of. The most important factor to threatening privacy is the fact that DNA is unique and it is proven very difficult to anonymize [7]. On top of that, one's DNA contains sensitive information about her, such as the disease susceptibility to various physical and mental diseases. Hence, baring specific circumstances, the patient might become the victim of genetic discrimination. The problem is greatly enhanced by the fact that DNA remains mostly unchanged over the years. This means that even in the span of decades a potential breach might affect one's privacy. Lastly but not least, one's DNA does not reveal information only about her, but it reveals information about her relatives and potential offspring as well. This fact complicates the problem since it raises the question of whether one has the right to donate or publish her genome to the public.

We know explain some acronyms which are going to be used throughout this proposal:

Single Nucleotide Polymorphisms (SNP). SNPs are a type of genetic variation among humans. They express the difference in a certain DNA position between two individuals. For instance, a certain individual, instead of having the nucleotide thymine (T) in position POS, they might have the nucleotide cytosine (C) [8].

Genome-Wide Association Studies (GWAS). GWAS enable researchers to conduct a genome-wide an examination of genetic variants in a group of individuals to see if a variant is associated with a trait [9].

3 State of the Art

We review the state of the art of privacy-enhancing technologies for genomic data processing/sharing and computational genetic testing. The literature regarding genomic privacy spans several communities, including science and engineering as well as law, policy, ethics, social science, and anthropology. We focus our research on the science and engineering works. We group the works into five categories: *Access and Storage Control*, *Genetic Relatedness*, *Clinical Applications*, *Outsourcing of Genomic Data*, and *Statistical Research*. We note that the legal perspective of genomic privacy is out of the scope of this proposal.

3.1 Genetic Relatedness Testing

A number of efforts investigate privacy-preserving methods for genealogy and ancestry testing 2, as well as genetic relatedness. These tests aim to determine whether two individuals are related (e.g., they are father and child) or to what degree (e.g., they are n-th cousins). Whereas, ancestry testing attempts to estimate an individual's "genetic pool", e.g., where their ancestors might come from. Several popular DTC genomic companies operate in this market, including 23andMe and AncestryDNA.

Privacy research in this context aims to support privacy-friendly versions of some of the existing genealogy and ancestry tests. Baldi et al. [10] show how two individuals, each holding a copy of their genome, can use private set intersection protocols [11] to simulate in-vitro paternity tests based on Restriction Fragment Length Polymorphisms (RFLP), and in such a way that they do not have to disclose their genomes to each other or two third-parties.

He et al. [12] let individuals privately discover their genetic relatives by comparing their genome to others stored, encrypted, in the same bio-repository. They rely on fuzzy encryption [13] (i.e., unlike traditional encryption schemes, where the encryption and decryption keys are identical, with fuzzy encryption, the keys must be similar but do not have to be identical) as well as on so-called secure genome sketch (SGS), which allows individuals to encrypt their genome using a key derived from their own genome. The corresponding ciphertext does not reveal sensitive information about the individual's genome, thus can be published to a third party and distributed to other individuals, who can detect relatedness (up to 3rd cousins) by trying to decrypt other ciphertexts.

Naveed et al. [14] use Controlled Functional Encryption (C-FE), which enables a client to learn only certain functions of encrypted data using keys which obtained from an authority. As discussed later, this can be used for patient similarity, e.g., allowing a physician to search for other patients with similar symptoms, perform disease susceptibility testing, as well as paternity and kinship applications. While [10] expects the user to store his genome in a personal device, and their protocol requires access to his fully sequenced genome, C-FE allows genealogy testing using SNP profiles that a user can get from a company like 23andMe.

3.2 Clinical Applications

Another line of work focuses on genetic and genomic tests for *personalized* medicine applications, e.g. assessing individuals' risk or predisposition to certain diseases, targeted screening and preemptive intervention [15], adjusting drug dosage, or determining the best course of treatment. These tests typically consist in checking for the presence of a few genetic mutations/SNPs.

In this context, there are two main models – in both cases a medical test unit performs some test against an individual's genome, however, (1) in one model, individuals keep a copy of their sequenced genome and consent to tests so that only the outcome is disclosed, while (2) another involves a semi-trusted party (defined in [16] as Storage and Processing Unit, or SPU) to store an encrypted copy of the patient's genetic information.

Baldi et al. [10] operate in model (1) and support privacy-preserving SNP testing using as examples testing of mutations in *hla-b* and *tpmt* genes (relevant, resp., in HIV and leukemia patients). The protocol, which relies on a private set intersection variant [17]: (i) pushes most of the pre-computation offline so that protocol interaction incurs complexity depending only on the number of SNPs to be tested, (ii) ensures that SNPs that are tested are kept private (as this is often a company's intellectual property), while (iii) guaranteeing that the test is authorized by a trusted party such as the FDA.

Djatmiko et al. [18] support personalized medicine tests such as adjusting Warfarin dosage [19] via private linear combination of SNPs. They assume patients to retain control of their genomic data, and aim to hide both the test's specifics and the patient's genome. They let a testing facility privately select data to be evaluated (using private information retrieval [20]), and process it while encrypted. The patient securely computes the linear combination of the test coefficients (using additive homomorphic encryption [21]) and shows the results to their physician.

Ayday et al. [16] introduce model (2) and focus on disease susceptibility testing, whereby a Medical Center (MC) performs disease susceptibility tests by privately analyzing the patient's SNPs, specifically, computing a weighted average of risk factors and SNP expressions. Patients get their genome sequenced, once, through a Certified Institution (CI), which encrypts the patient's SNPs and their positions and uploads them to a Storage and Processing Unit (SPU). Then, either MC computes the disease susceptibility using homomorphic encryption and proxy re-encryption, or the SPU provides the relevant SNPs to the MC. Ultimately their model allows the MC to process the patient's genomic data in a private manner.

Also relying on semi-trusted parties is the system proposed by Naveed et al. [14]: the sequencing institution encrypts a patient's genome using controlled-functional encryption (C-FE) under a public key issued by a central authority, and publishes the ciphertext. Medical units can then run personalized medicine-type tests using a one-time function key, obtained by the authority, which corresponds to one specific test and can only be used for that.

Wang et al. [22] focus on the problem of finding similar patients, using edit distance (ED), which is useful, e.g., to physicians inquiring about how similar patients respond to certain therapies. ED is used as a biological similarity indicator [23], described as the minimum number of edits required to change a string into another. Using optimized garbled circuits, authors support a genome-wide, privacy-preserving similar patient query system. In order for the scheme to work, each party (e.g., hospitals) has to agree on a public reference genome and independently compress their local genomes using that reference genome, creating a Variation Call Format (VCF) file. Then, the ED of two genomes can be calculated by securely comparing the two VCF files.

3.3 Access and Storage Control

Due to its significant and long-term sensitivity, it is obviously crucial to guarantee secure access to and storage of genomic information. Karvelas et al. [24] propose to store data in a special randomized data structure using Oblivious RAM (ORAM) [25], achieving access pattern privacy, by relying on two servers ("cloud" and "proxy") to cooperatively operate the ORAM. Clients can then query data using a third entity ("investigator"), which retrieves encrypted data from the ORAM and instructs the cloud and the proxy to jointly and privately compute functions using secure computation [26].

Ayday et al. [27] present a framework which can privately store, retrieve, and process SAM files. Sequence Alignment Map (SAM) is a text-based format to store nucleotide sequences. In their scheme, a certified institution sequences and encrypts the patient's genome, creating the SAM files which are being stored in a biorepository. Then, a medical unit, using order-preserving encryption (OPE) [28], can retrieve the data and conduct a genetic test. The cryptographic keys of the patients are being stored in a masking and key manager, which could be a governmental entity or a company.

Huang et al. [29] focus on long-term security, introducing GenoGuard, a tool protecting encrypted genomic data against an adversary who tries to exhaustively guess the decryption key. This is possible thanks to Honey Encryption (HE) [30], so that any decryption attempt using an incorrect key yields a random, yet plausible genome sequence.

Genomic data is stored using two standard formats: (i) BAM, a binary format version of the previously mentioned SAM format, and (ii) CRAM, which is compatible with BAM but allows for lossless compression. However, when applying standard symmetric encryption methods to these formats, they might become susceptible to information leakage when a client is querying specific genomic regions, by overlapping reads with each retrieval. Therefore, Huang et al. [31]

develop a tool called SECRAM, which enables compression, encryption, and selective retrieval of genomic data while protecting the data from information leakage using (OPE). It consumes less storage than BAM, and maintains CRAM's efficient compression and downstream data processing.

3.4 Outsourcing of Genomic Data

In order to conduct large-scale biomedical analysis (such as genome-wide association studies, or GWAS), researchers need access to genomic data held by different entities. However, sharing genomic information faces several obstacles – e.g., researchers may be prevented by regulatory or ethical bodies from releasing data, or might only have patients' consent to use their data in a specific study at a specific institution. Therefore, research has proposed a number of privacy-enhancing methods to address these issues, primarily, by securely outsourcing data to a semi-trusted cloud so that two or more entities can collectively use it.

Kamm et al. [32] propose a data collection system where genomic data are being distributed in several entities using secret sharing. They use secure multiparty computation (MPC) to conduct computations on the secret-shared data without leaking any information. Using these tools they support secure GWAS between independent entities, such as hospitals and biobanks.

Xie et al. [33] introduce the SecureMA framework which allows secure meta-analysis of genome-wide association studies. Meta-analysis is technique in statistics to synthesize information from multiple independent studies [34]. Their framework (a) generates and distributes encryption/decryption keys to the participating entities, and encrypts the association statistics of each study locally, and (b) securely computes the meta-analysis results using the encrypted data.

Humbert et al. [35] consider the case where individuals want to donate their genome to research, but are concerned about their privacy and that of their relatives. To address this, they first quantify the genomic privacy of an individual by calculating the "global privacy weight" of every SNP, and then they provide an obfuscation mechanism which enables the users to publish their data for research purposes, while protecting their privacy. Their obfuscation technique is based on SNP hiding. The choose which SNPs to hide based on the "global privacy weight" of every SNP and its linkage disequilibrium (LD) correlation. LD is a non-random association, or correlation, between SNPs, which among other things, is being used to form the basis for mapping complex diseases association by association. In their protocol, the SNPs with the highest weight are the ones for which the LD correlations cause the highest decrease in genomic privacy. Their obfuscation technique removes those SNPs, allowing the individuals to publish their genomic data while protecting their privacy.

Xu et al. [36] focus on the process of read-mapping, which is used for finding patterns in long DNA sequences, for SNP discovery and genotyping. They propose a solution which can securely outsource read-mapping to the cloud, using the MapReduce [37] framework and field programmable gate arrays (FPGAs) [38].

Stade et al. [39] study the case of Next Generation Sequencing (NGS) [40]. NGS data can enable researchers identify causative or predisposing mutations. However, sharing this kind of data is most of the times forbidden due to privacy regulations. The authors create a tool, called GrabBlur, which aggregates NGS data and shares them in a public database, while making sure the individual samples are unidentifiable. Their tool aggregates single nucleotide variants (SNVs) which are linked to a specific trait or phenotype. They ensure anonymity by deleting important information from the individual's exome or genome. When a researcher finds an interesting SNV, she can get in contact with the submitter to exchange further information about the carrier.

Zhang et al. [41] propose a framework, called FORESEE, that provides chi-square statistics by outsourcing computations to the cloud. In their scheme, a data owner encrypts its data and uploads it to a public cloud. FORESEE enables secure divisions over the encrypted data and access to the results by authorized users.

Constable et al. [42] develop a framework that enables two entities to use a distributed system to conduct secure GWAS computations. Their framework allows the calculation of minor allele frequencies (MAFs) and χ^2-statistics using MPC.

Aziz et al. [43] consider the problem of large-scale biomedical research where different entities want to combine their genomic data for cohort analysis. They propose a secure sharing and computation architecture which uses the Paillier cryptosystem [21] and Order-preserving encryption [44]. In their scheme, when a researcher submits a query, the participating data owners execute it on their data and send the results to a central server, encrypted. The central server adds all the values together and sends them to the crypto service provider for decryption. The results are then submitted to the researcher. Their architecture supports the count query and the ranked query algorithms.

Ghasemi et al. [45] present a model which outsources genomic data to the cloud, available for the execution of count and top-k queries. Their scheme guarantees the privacy of the users by permuting and adding fake genomic sequences to the raw data. At first, the dataset is being preprocessed by and stored in the cloud. Then, the cloud can execute the count and top-k queries on the database and send the results to the researcher.

Chen et al. [46] propose a framework, called PRINCESS, which can conduct private computation over encrypted data using data distributed by institutes in different continents. Instead of using heavyweight cryptographic techniques such as homomorphic encryption, they utilize the SGX computing architecture (Software Guard Extensions) [47] which provides a way of isolating sensitive data in a protected enclave and then securely computing the results. The authors test the performance of their framework by conducting the Kawasaki Disease (KD) [48] test using data distributed in three different continents. They show that their framework computes the results over $40,000$ faster in comparison to similar solutions based on homomorphic encryption and garbled circuits.

3.5 Statistical Research

This category includes works which use Differential Privacy (DP) as the main mechanism for preserving privacy. In general terms, DP is a tool aimed for statistical databases, which tries to provide as accurate query results as possible while minimizing the chances for an adversary to identify the database contents [49]. The way DP works is by taking the contents of a database and creating another one by adding some noise to it, using some probability distribution like the Laplace mechanism.

The problem is that standard DP techniques cannot be used in GWAS. This is because in GWAS the number of outputs, which in our case is the correlations between SNPs, is far greater than the number of the patients [50]. But since the purpose of GWAS is to pinpoint to the statistics with the highest importance, that is, those which reveal a correlation between certain SNPs and a disease, it is possible to design DP in way which results in a small number of outputs with higher accuracy [51, 52].

The drawback of [51, 52] is the fact that they require the researcher to know beforehand what to ask (such as the top-k most significant SNPs) while in a typical GWAS, finding the k most significant SNPs is the goal, not the requirement. Johnson and Shmatikov [50] propose a way of privacy-preserving GWAS where the researchers are not required to know beforehand which questions to ask (exploratory data analysis). Their work allows the researchers to compute the number and location of the most significant SNPs to a disease, the p-values of a statistical test between a SNP and a disease, any correlation between two SNPs, and the block structure of correlated SNPs, in a differentially private way.

In answer to Homer's attack [53], Uhlerop et al. [54], using differential privacy, introduce ways of releasing aggregate GWAS data in a privacy preserving manner. More specifically, their work allows the computation of ϵ-differentially private χ^2-statistics and ρ-values and the release of these statistics regarding the most relevant SNPs. Later, Yu et al. [55] extend the work of [54] by managing to allow an arbitrary number of controls and cases for differentially-private χ^2-statistics.

Li et al. [56] propose a privacy framework based on DP, called Membership Privacy. More specifically, they introduce the notion of Positive Membership Privacy (PMP), where an adversary cannot significantly infer the information that an entity exists in a dataset, and the notion of Negative Membership Privacy (NMP), where an adversary cannot significantly infer the information that an entity does not exist in a dataset. Tramèr et al. [57] use PMP along with a relaxation of DP, and they show that for various privacy budgets and adversarial settings the tradeoff between privacy and utility changes.

4 Proposed Approach & Methodology

Our research will be conducted in four discrete phases.

4.1 Understanding the Research Landscape

We conduct a comparative technical analysis of the state of the art by examining the literature from a critical point of view and by systematizing the current knowledge. We group our observations into categories providing a holistic overview of the works proposed. A special focus is being given to usability. We discuss with a series of expert in the biomedical community in order to determine whether the current works are solving the problems that the biomedical community faces. The ultimate goal of this phase is to determine if the genomic privacy community has been solving the "right" problems – meaning problems that the biomedical community currently faces, and to derive open problems, if any.

In order to achieve this we aim to produce a Systemization of Knowledge (SoK) paper where the state of the art will be explained and assessed based on a series of categories. First we group the literature into five categories: *Access and Storage Control*, *Genetic Relatedness*, *Clinical Applications*, *Outsourcing of Genomic Data*, and *Statistical Research*. Then we assess each paper using four discrete criteria categories, more specifically: *Architecture*, *biology*, *privacy mechanisms*, and *utility*.

4.2 Quantitative Analysis

This phase aims to analyze twitter data using a number of keywords related to direct-to-consumer (DTC) genomics companies and genomics in general (i.e. personalized medicine, precision medicine). The goal of the study is to compare the perceptions of the public in regards to genomics. What is the overall sentiment (positive or negative) around personalized medicine and DTC genomics companies, what is the emotion of the users (i.e. happy, angry, scared etc.), what is the content of these tweets, as well as who is tweeting about genomics (user-profile analysis).

This phase will be conducted in steps:

(a) Crawling the twitter data. The Twitter API does not include the option of fetching older tweets, therefore, a manual crawler will have to be used. We will crawl tweets that contain words which are related to DTC companies and genomics in general.

(b) Detection of emotion. Using published algorithms we will analyze the dataset in order to find out the emotion per category (i.e. angry, scared, happy etc.)

(c) Hashtag analysis. This step will analyze the hashtags of the tweets. i.e. Which hashtags are the most popular.

(d) Latent Dirichlet Allocation (LDA). LDA is a method to extract topics from a given text. Using LDA we will be able to find interesting topics among our dataset.

(e) Sentiment Analysis. Using published algorithms we will analyze the sentiment per category in order to find out if it is positive or negative.

(f) URL Characterization. This step will analyze the URLs of the dataset. i.e. How many tweets contain URLs, how many of these URLs are popular.

(g) User analysis. This step will analyze the profile of the users. In order to achieve this we will crawl the latest $1,000$ tweets of a random percentage of the users in order to find out who is interested in genomics and what do they tweet about in general.

At this point, we note that twitter represents only a subset of the available social networks. We do not claim that the results of this phase are representative of the 100% of the DTC-GC users. However, we argue that they represent certain trends, if they are examined under the correct context.

4.3 Qualitative Analysis

Phase 3 will use a qualitative research method in the form of semi-structured interviews with users of DTC genomics companies and/or users of personalized medicine techniques. The study will be investigative in nature, starting from recounts of overall experiences with DTC companies, and aiming to elicit recurring concerns, fears, hopes – as perceived by the users. We will follow a scenario-based approach to stimulate conversations about secondary uses of data, e.g., data after death, impact on relatives.

We will do so to elicit views from scenarios representing potential discovery of sensitive, embarrassing, or life-changing results and to depict avenues for possible discrimination. Due to its qualitative nature, this set of user studies will put a strong emphasis on exploring the personal views of DTC users, rather than setting out to test hypotheses. By working with unstructured data, we will not be restricted to a closed set of categories and will investigate collected data by explicitly interpreting the meanings and functions of human decisions. The studies will provide insight on the "human side" of genomic testing, helping to uncover aspects related to privacy, security, trust, and ethics.

4.4 User-Centered Secure Personal Genome Testing Infrastructure

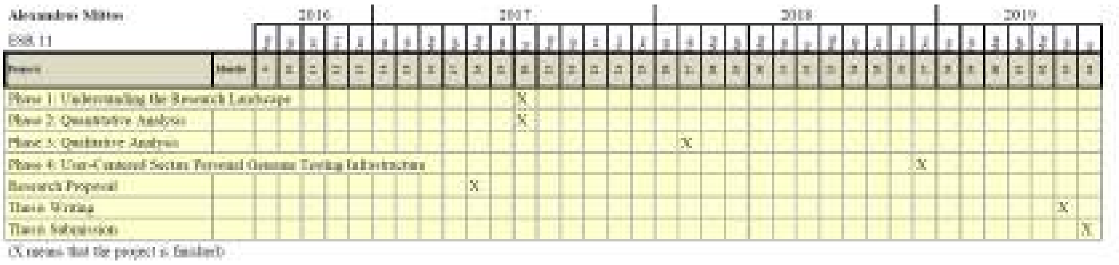
Phase 4 consists of the design of a user-centered secure personal genome testing infrastructure. In this context, we will help individuals get ahold of their genomic data from DTC companies. We plan to design an effective, meaningful, and usable user interface which will enable users to control and access genomic data.

We will follow standard methods for iterative user-centered design. We will explore two possible strategies: (1) Genomic data is stored (encrypted) on a personal device controlled by the user, and (2) Genomic data is encrypted and outsourced to a dedicated cloud server and can be queried only with the active consent of the genome's owner. We will implement and test prototypes that build on the early work by Dr. De Cristofaro [10, 58] for the first strategy, and on other recent proposals by EPFL researchers [16] for the second one. These two approaches will be analyzed in terms of their usability, allowing us to draw preliminary conclusions on what architecture should be preferred and why.

Working toward the user-centered design of a genome testing architecture for personal genomic applications requires us to compare the effects on both usability and security of the two different strategies. Usable prototypes should not only be intuitive and minimize the cognitive load on users, but also allow them to fully understand their interaction with the system and successfully address their privacy fears and concerns, which we will be able to do building on the results from phase 2 and 3.

In regards to building the system, we will work on realizing the underlying technical tools to enable privacy-preserving genomic testing. Regardless of whether encrypted genomes are outsourced to the cloud or kept on a personal device, secure genome applications should satisfy sound data safety and privacy requirements. Long-term security of genomic data requires not only preventing unauthorized parties from accessing genomic information, but also binding a genome to its owner.

To this end, we will rely on techniques based on hardware tokens and cryptographic tools



Alexandros Mittos		2016					2017												2018												2019						
ESR 11		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Project	Months	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Phase 1: Understanding the Research Landscape													X																								
Phase 2: Quantitative Analysis													X																								
Phase 3: Qualitative Analysis																				X																	
Phase 4: User-Centered Secure Personal Genome Testing Infrastructure																														X							
Research Proposal											X																										
Thesis Writing																																				X	
Thesis Submission																																					X

(X means that the project is finished)

Figure 1: Work Plan

and guarantee that testing is performed in a privacy-respecting way, i.e., in such a way that only the test outcome is disclosed (and not the entire genome of the individual undergoing the test). Specifically, we will work on efficient cryptographic protocols that support privacy-friendly screening for genetic traits and inherited diseases, testing partner compatibility for recessive disease prevention, disease predisposition and response to drugs and treatments, as well as ancestry and genealogy testing.

We will build on prior work [10, 58, 16], but will actually prototype a working system, building the back-end technical tools in such a way that they are soundly integrated with usable, meaningful user interfaces. In particular, we will focus our efforts on the users' involvement in secure testing, aiming to minimize cognitive effort, misaligned incentives, and primary task disruption, so that users are helped in making meaningful security decisions, without letting the security and privacy protection layer become a burden for the user.

5 Work Plan

Figure 1 shows the proposed time plan for the duration of 3 years. Phase 1, "Understanding the Research Landscape", is a systemization of knowledge paper (SoK) which examines the literature from a critical point of view. Phase 2 runs in parallel with phase 1, and it aims to compare the perceptions of the public in regards to DTC genomics companies. Phase 3 is a qualitative study in the form of semi-structured interviews with users of DTC genomics, in order to explore the personal views of DTC users. Phase 4 is the design of a user-centered secure personal genome testing infrastructure based on our findings from the previous phases. The final step is the writing and submission of the thesis.

References

[1] Erman Ayday, Emiliano De Cristofaro, Jean-Pierre Hubaux, and Gene Tsudik. The chills and thrills of whole genome sequencing. 2013.

[2] Samuel Levy, Granger Sutton, Pauline C Ng, Lars Feuk, Aaron L Halpern, Brian P Walenz, Nelson Axelrod, Jiaqi Huang, Ewen F Kirkness, Gennady Denisov, et al. The diploid genome sequence of an individual human. *PLoS Biol*, 5(10):e254, 2007.

[3] David A Wheeler, Maithreyan Srinivasan, Michael Egholm, Yufeng Shen, Lei Chen, Amy McGuire, Wen He, Yi-Ju Chen, Vinod Makhijani, G Thomas Roth, et al. The complete genome of an individual by massively parallel dna sequencing. *nature*, 452(7189):872–876, 2008.

[4] www.genome.gov. sequencingcosts, 2017.

[5] Genomics England. The 100,000 genomes project, 2015.

[6] Francis S Collins and Harold Varmus. A new initiative on precision medicine. *New England Journal of Medicine*, 372(9):793–795, 2015.

[7] Stuart Bradley. Realistic dna de-anonymization using phenotypic prediction. 2015.

[8] nature.com. Snp, 2016.

[9] www.genome.gov. genomewideassociationstudies, 2017.

[10] Pierre Baldi, Roberta Baronio, Emiliano De Cristofaro, Paolo Gasti, and Gene Tsudik. Countering gattaca: efficient and secure testing of fully-sequenced human genomes. In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 691–702. ACM, 2011.

[11] Emiliano De Cristofaro, Paolo Gasti, and Gene Tsudik. Fast and Private Computation of Cardinality of Set Intersection and Union. 2012.

[12] Dan He, Nicholas A Furlotte, Farhad Hormozdiari, Jong Wha J Joo, Akshay Wadia, Rafail Ostrovsky, Amit Sahai, and Eleazar Eskin. Identifying genetic relatives without compromising privacy. *Genome research*, 24(4):664–672, 2014.

[13] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In *International conference on the theory and applications of cryptographic techniques*, pages 523–540. Springer, 2004.

[14] Muhammad Naveed, Shashank Agrawal, Manoj Prabhakaran, XiaoFeng Wang, Erman Ayday, Jean-Pierre Hubaux, and Carl Gunter. Controlled functional encryption. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 1280–1291. ACM, 2014.

[15] S. Cass. Cheap DNA sequencing will drive a revolution in health care. http://www.technologyreview.com/biomedicine/24587/, 2010.

[16] Erman Ayday, Jean Louis Raisaro, Jean-Pierre Hubaux, and Jacques Rougemont. Protecting and evaluating genomic privacy in medical tests and personalized medicine. In *Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society*, pages 95–106. ACM, 2013.

[17] Emiliano De Cristofaro and Gene Tsudik. Practical private set intersection protocols with linear complexity. In *International Conference on Financial Cryptography and Data Security*, pages 143–159. Springer, 2010.

[18] Mentari Djatmiko, Arik Friedman, Roksana Boreli, Felix Lawrence, Brian Thorne, and Stephen Hardy. Secure evaluation protocol for personalized medicine. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society*, pages 159–162. ACM, 2014.

[19] International Warfarin Pharmacogenetics Consortium et al. Estimation of the warfarin dose with clinical and pharmacogenetic data. *N Engl J Med*, 2009(360):753–764, 2009.

[20] Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan. Private information retrieval. In *Foundations of Computer Science, 1995. Proceedings., 36th Annual Symposium on*, pages 41–50. IEEE, 1995.

[21] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 223–238. Springer, 1999.

[22] Xiao Shaun Wang, Yan Huang, Yongan Zhao, Haixu Tang, XiaoFeng Wang, and Diyue Bu. Efficient genome-wide, privacy-preserving similar patient query based on private edit distance. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 492–503. ACM, 2015.

[23] James G Taylor, Eun-Hwa Choi, Charles B Foster, and Stephen J Chanock. Using genetic variation to study human disease. *Trends in molecular medicine*, 7(11):507–512, 2001.

[24] Nikolaos Karvelas, Andreas Peter, Stefan Katzenbeisser, Erik Tews, and Kay Hamacher. Privacy-preserving whole genome sequence processing through proxy-aided oram. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society*, pages 1–10. ACM, 2014.

[25] Oded Goldreich and Rafail Ostrovsky. Software protection and simulation on oblivious rams. *Journal of the ACM (JACM)*, 43(3):431–473, 1996.

[26] Yehuda Lindell and Benny Pinkas. A proof of security of yao's protocol for two-party computation. *Journal of cryptology*, 22(2):161–188, 2009.

[27] Erman Ayday, Jean Louis Raisaro, Urs Hengartner, Adam Molyneaux, and Jean-Pierre Hubaux. Privacy-preserving processing of raw genomic data. In *Data Privacy Management and Autonomous Spontaneous Security*, pages 133–147. Springer, 2014.

[28] Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, and Yirong Xu. Order preserving encryption for numeric data. In *Proceedings of the 2004 ACM SIGMOD international conference on Management of data*, pages 563–574. ACM, 2004.

[29] Zhicong Huang, Erman Ayday, Jacques Fellay, Jean-Pierre Hubaux, and Ari Juels. Genoguard: Protecting genomic data against brute-force attacks. In *2015 IEEE Symposium on Security and Privacy*, pages 447–462. IEEE, 2015.

[30] Ari Juels and Thomas Ristenpart. Honey encryption: Security beyond the brute-force bound. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 293–310. Springer, 2014.

[31] Zhicong Huang, Erman Ayday, Huang Lin, Raeka S Aiyar, Adam Molyneaux, Zhenyu Xu, Jacques Fellay, Lars M Steinmetz, and Jean-Pierre Hubaux. A privacy-preserving solution for compressed storage and selective retrieval of genomic data. *Genome Research*, 26(12):1687–1696, 2016.

[32] Liina Kamm, Dan Bogdanov, Sven Laur, and Jaak Vilo. A new way to protect privacy in large-scale genome-wide association studies. *Bioinformatics*, 29(7):886–893, 2013.

[33] Wei Xie, Murat Kantarcioglu, William S Bush, Dana Crawford, Joshua C Denny, Raymond Heatherly, and Bradley A Malin. Securema: protecting participant privacy in genetic association meta-analysis. *Bioinformatics*, page btu561, 2014.

[34] Evangelos Evangelou and John PA Ioannidis. Meta-analysis methods for genome-wide association studies and beyond. *Nature Reviews Genetics*, 14(6):379–389, 2013.

[35] Mathias Humbert, Erman Ayday, Jean-Pierre Hubaux, and Amalio Telenti. Reconciling utility with privacy in genomics. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society*, pages 11–20. ACM, 2014.

[36] Lei Xu, Hanyee Kim, Xi Wang, Weidong Shi, and Taeweon Suh. Privacy preserving large scale dna read-mapping in mapreduce framework using fpgas. In *Field Programmable Logic and Applications (FPL), 2014 24th International Conference on*, pages 1–4. IEEE, 2014.

[37] Jeffrey Dean and Sanjay Ghemawat. Mapreduce: simplified data processing on large clusters. *Communications of the ACM*, 51(1):107–113, 2008.

[38] Lei Xu, Weidong Shi, and Taeweon Suh. Pfc: Privacy preserving fpga cloud-a case study of mapreduce. In *Cloud Computing (CLOUD), 2014 IEEE 7th International Conference on*, pages 280–287. IEEE, 2014.

[39] Björn Stade, Dominik Seelow, Ingo Thomsen, Michael Krawczak, and Andre Franke. Grabblur-a framework to facilitate the secure exchange of whole-exome and-genome snv data using vcf files. *BMC genomics*, 15(4):S8, 2014.

[40] Jacek Majewski, Jeremy Schwartzentruber, Emilie Lalonde, Alexandre Montpetit, and Nada Jabado. What can exome sequencing do for you? *Journal of medical genetics*, pages jmedgenet–2011, 2011.

[41] Yuchen Zhang, Wenrui Dai, Xiaoqian Jiang, Hongkai Xiong, and Shuang Wang. Foresee: Fully outsourced secure genome study based on homomorphic encryption. *BMC medical informatics and decision making*, 15(Suppl 5):S5, 2015.

[42] Scott D Constable, Yuzhe Tang, Shuang Wang, Xiaoqian Jiang, and Steve Chapin. Privacy-preserving gwas analysis on federated genomic datasets. *BMC medical informatics and decision making*, 15(5):1, 2015.

[43] Al Aziz, Md Momin, Mohammad Z Hasan, Noman Mohammed, and Dima Alhadidi. Secure and efficient multiparty computation on genomic data. In *Proceedings of the 20th International Database Engineering & Applications Symposium*, pages 278–283. ACM, 2016.

[44] Alexandra Boldyreva, Nathan Chenette, Younho Lee, and Adam O'neill. Order-preserving symmetric encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 224–241. Springer, 2009.

[45] Reza Ghasemi, Md Momin Al Aziz, Noman Mohammed, Massoud Hadian Dehkordi, and Xiaoqian Jiang. Private and efficient query processing on outsourced genomic databases. *IEEE Journal of Biomedical and Health Informatics*, 2016.

[46] Feng Chen, Shuang Wang, Xiaoqian Jiang, Sijie Ding, Yao Lu, Jihoon Kim, S Cenk Sahinalp, Chisato Shimizu, Jane C Burns, Victoria J Wright, et al. Princess: Privacy-protecting rare disease international network collaboration via encryption through software guard extensions. *Bioinformatics*, page btw758, 2017.

[47] Ittai Anati, Shay Gueron, Simon Johnson, and Vincent Scarlata. Innovative technology for cpu based attestation and sealing. In *Proceedings of the 2nd international workshop on hardware and architectural support for security and privacy*, volume 13, 2013.

[48] Chiea Chuen Khor, Sonia Davila, Willemijn B Breunis, Yi-Ching Lee, Chisato Shimizu, Victoria J Wright, Rae SM Yeung, Dennis EK Tan, Kar Seng Sim, Jie Jin Wang, et al. Genome-wide association study identifies fcgr2a as a susceptibility locus for kawasaki disease. *Nature genetics*, 43(12):1241–1246, 2011.

[49] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. In *Theory of Cryptography Conference*, pages 265–284. Springer, 2006.

[50] Aaron Johnson and Vitaly Shmatikov. Privacy-preserving data exploration in genome-wide association studies. In *Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 1079–1087. ACM, 2013.

[51] Raghav Bhaskar, Srivatsan Laxman, Adam Smith, and Abhradeep Thakurta. Discovering frequent patterns in sensitive data. In *Proceedings of the 16th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 503–512. ACM, 2010.

[52] Stephen E Fienberg, Aleksandra Slavkovic, and Caroline Uhler. Privacy preserving gwas data sharing. In *2011 IEEE 11th International Conference on Data Mining Workshops*, pages 628–635. IEEE, 2011.

[53] Nils Homer, Szabolcs Szelinger, Margot Redman, David Duggan, Waibhav Tembe, Jill Muehling, John V Pearson, Dietrich A Stephan, Stanley F Nelson, and David W Craig. Resolving individuals contributing trace amounts of DNA to highly complex mixtures using high-density SNP genotyping microarrays. *PLoS Genet*, 4(8), 2008.

[54] Caroline Uhlerop, Aleksandra Slavković, and Stephen E Fienberg. Privacy-preserving data sharing for genome-wide association studies. *The Journal of privacy and confidentiality*, 5(1):137, 2013.

[55] Fei Yu, Stephen E Fienberg, Aleksandra B Slavković, and Caroline Uhler. Scalable privacy-preserving data sharing methodology for genome-wide association studies. *Journal of biomedical informatics*, 50:133–141, 2014.

[56] Ninghui Li, Wahbeh Qardaji, Dong Su, Yi Wu, and Weining Yang. Membership privacy: a unifying framework for privacy definitions. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 889–900. ACM, 2013.

[57] Florian Tramèr, Zhicong Huang, Jean-Pierre Hubaux, and Erman Ayday. Differential privacy with bounded priors: reconciling utility and privacy in genome-wide association studies. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 1286–1297. ACM, 2015.

[58] Emiliano De Cristofaro, Sky Faber, and Gene Tsudik. Secure genomic testing with size- and position-hiding private substring matching. In *Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society*, pages 107–118. ACM, 2013.

Alexandros Mittos (ESR11), University College London (UCL)

Career Development Plan Year 1

I. *Personal and Organizational Information*

ESR´s Personal Information			
Name:	**Alexandros Mittos**	**ID number**:	(UCL SN) 16132298
Office Address:	UCL Computer Science Department Room 4.02 Malet Place Engineering Building Gower Street,, London WC1E 6BT UK	**Phone**:	+44 (0) 78014 57167
Mobile:	+44 (0) 78014 57167	**E-Mail:**	alexandros.mittos.16@ucl.ac.uk

ESR´s Host Organization Information			
Name:	**University College London**	**Phone**:	+44 20 7679 2000
Address:	Gower St, Bloomsbury, London WC1E 6BT, UK		

II. *Supervision*

Supervision			
Supervisor´s Name:	**Emiliano De Cristofaro**	**Title**:	Senior Lecturer (Associate Professor)
Place of Employment:	University College London	**Phone**:	+44 20 7679 0349
Responsibility Distr.:	%70	**E-Mail:**	e.decristofaro@ucl.ac.uk
Co-Supervision			
Co-Supervisor´s Name:	**Delphine Reinhardt**	**Title**:	Dr.
Place of Employment:	Universität Bonn	**Phone**:	+49 228 736 0551
Responsibility Distr.:	%30	**E-Mail:**	delphine.reinhardt@cs.uni-bonn.de

Conduct of Supervision (per activity describe form of supervision and estimated supervision hours)**:**

- Distribution of supervisor responsibility between the main supervisor and co-supervisor:

The majority of work is distributed towards Dr. Emiliano De Cristofaro. During the four-month secondment in Bonn, the majority of work is expected to be distributed towards Dr. Delphine Reinhardt.

- Conduct of supervision:

Weekly meetings with Dr. Emiliano De Cristofaro. The duration is 1 hour on average and additional discussions are commenced when appropriate and necessary. Expected regular meetings with Dr. Delphine Reinhardt during the four-month secondment in Bonn.

III. Secondment

ESR´s Secondment			
Supervisor's Name:	**Andreas Sachs**	**Positio n:**	Head of IT Security and Technical Aspects of Data Protection
Organization´s Name:	**Data Protection Authority of Bavaria for the Private Sector**	**Phone:**	0981/53-1304
Address:	Bayerisches Landesamt für Datenschutzaufsicht (BayLDA) Promenade 27 91522 Ansbach	**E-mail:**	Andreas.Sachs@lda.bayern.de

IV. Research Project

ESR´s Project			
Title:	**Privacy-Preserving Personal Genomic Testing**	**Ref. No:**	11

Overview and background

The advances of the biomedical field in regards to genomics have impacted the quality of medical services to users worldwide for the better, but in the same time they have the potential to breach their privacy. To date, the literature has focused on creating privacy-preserving methods which utilize these services but not with respect to the users' concerns and needs. This research focuses on the field of genomic privacy from user-centered perspective. It aims to identify the users' perceptions and design a user-centered secure personal genome testing infrastructure with an effective, meaningful, and usable user interface which will enable users to control and access genomic data. We first use quantitative and qualitative methods to identify the users' needs and then we use these results in order to design the previouslymentioned infrastructure. We believe that this will enable users to unveil the full potential of the genomics services while protecting their privacy.

V. Long-Term Career Objectives

Long-Term Career Objectives (over five years)

After completing my PhD, my long-term career objective is to seek a position in applied research. This can be achieved either by staying in academia and or aiming the industry. I wish to share my experience and knowledge with experts in the field of privacy.

Meanwhile I plan to expand my knowledge to broader subjects of security and privacy. More specifically I am interested in Secure Multiparty Computation (MPC) and Differential Privacy.

I also believe that a key component of producing useful research is interdisciplinarity, something Privacy & Us values. Therefore, I plan to broaden my knowledge on other fields like usability. The Privacy & Us network gives me the perfect opportunity to achieve this.

VI. Short-Term Career Objectives

A. Project Research Results

Project Research Results
Presented according to Privacy & Us project Plan.

Milestones	Expected Results
Literature Review (SoK) (M20)	Examination of the literature from a critical point to derive open problems, if any.
Research Proposal (M18)	Proposition of novel approaches to address the gaps identified in the literature
Career development plan (M18)	Preparation of CDP toward my career after my research studies
Quantitative Analysis (M20)	Analyze twitter data to compare the perceptions of the public in regards to genomics
User interface requirement analysis (M18)	Analysing the user interface and usability requirements which are essential for the user-centered secure personal genome testing infrastructure

Deliverables

2.1: Requirements Analysis (M18)
4.1: User Interface Requirements (M18)
5.1: Privacy Principles (M20)
6.7: Researcher Declarations and Career Development Plan (M18)

Anticipated Publications

- *18th Privacy Enhancing Technologies Symposium (PETS 2018)*, Barcelona, Spain
  Submission: SoK: Genomic Privacy -- Are We Going In The Right Direction?

- *CHI 2018: ACM CHI Conference on Human Factors in Computing Systems*, Montréal, Canada
  Submission: A Longitudinal Measurement Study of the Perceptions of Twitter Users on Direct to Consumer Genomics Companies

Anticipated Conference/Workshop Attendance & Courses/Seminar Presentations

- *3rd International Workshop on Genome Privacy and Security (GenoPri'16), Chicago, IL, USA (attended)*
- *IDASH Security and Privacy Workshop 2016, Chicago, IL, USA (attended)*

B. Training

Research and Technical Training

- Introduction to PETs, August 2016 (Karlstad, Sweden)
- Privacy Enhancing Technologies (UCL, London)

Secondment Plan

- The goal is to investigate how the General Data Protection Regulation (GDPR) treats health data (with emphasis on genomic data) and if genomics companies in Bayern (and Germany in general) use sufficient means of protection in regards to privacy.

Interdisciplinary Training

- Privacy of Personal Health Data, August 2016 (Karlstad, Sweden)
- General Data Protection Regulation – Next Step? August 2016 (Karlstad, Sweden)
- Introduction to Usability, August 2016 (Karlstad, Sweden)
- Legal Privacy Workshop – Privacy by Design, August 2016 (Karlstad, Sweden)
- The Future of Privacy and Identity Management, August 2016 (Karlstad, Sweden)

Professional Training

- Scientific Paper Writing, August 2016 (Karlstad, Sweden)
- Professional Networking, August 2016 (Karlstad, Sweden)

Other Training Activities

- Self-management Training, April – May, 2017

C. *Networking Activities*

- First network event (25th-27th August 2016, Karlstad, Sweden) (attended)
- Second network event (30th May – 2nd June, 2017, Vienna, Austria)
- 3rd International Workshop on Genome Privacy and Security (GenoPri'16), Chicago, IL, USA (attended)
- IDASH Security and Privacy Workshop 2016, Chicago, IL, USA (attended)

D. Research Management

- Nothing to report

E. Other activities

Other Activities (professional relevant)

- Contributed as sub-reviewer in the 3rd International Workshop on Genome Privacy and Security (GenoPri'16), Chicago, IL, USA

VII. Signatures

Date & Signature of fellow

Date & Signature of supervisor

PhD Research Proposal

Privacy preserving online identity management through self-disclosure and self-presentation when diagnosed with HIV

Mark Warner

Primary Supervisor: Professor Ann Blandford

Co-Supervisor: Professor Joachim Meyer

Submitted in partial fulfilment of the requirements for the degree of:

Doctor of Philosophy

June 2017

University College London, UCL Interaction Centre,
Department of Computer Science, Faculty of Engineering
University College London

Declaration

I, Mark Warner, confirm that the work presented in this proposal is my own. Where information has been derived from other sources, I confirm that this has been indicated in the proposal.

Table of Content

1 Abstract

When new technologies enter into society and challenge perceptions of privacy, it is often suggested that only those who have something to hide have something to fear (Solove, 2007). However, this idea is based on the premise that people only hide things for nefarious reasons, which this current research will show, is not the case. Controlling the disclosure of information about the self provides people with an instrument for presenting themselves to people in different ways, depending on the goals within a given context or interaction. When someone is diagnosed with a sensitive, stigmatising condition such as HIV, it can be challenging to integrate this new aspect of their self into their online lives. Privacy allows people to manage self-disclosure of information so they can develop and manage a plurality of contextually constructed, goal driven identities across different online environments, without fear of damaging the reputations of these identities. This research will conduct a series of qualitative studies to understand the factors that influence the effective management of people's online identities when diagnosed with HIV. Through these studies, a behavioural model will be developed and tested using quantitative methods. The model will provide a better understanding of how people diagnosed with HIV build conviction for the decisions they make when disclosing across different online environments. The model and the research findings from each study can be used to inform designers developing communication technologies intended for people managing HIV.

2 Introduction

When a person is diagnosed with Human Immunodeficiency Virus (HIV), the disclosure of their condition within their local social context has been shown to increase levels of social support, helping to reduce stress and anxiety (Kalichman, DiMarco, Austin, Luke, & DiFonzo, 2003) and improve treatment response (Stirratt et al., 2006; Strachan, Bennett, Russo, & Roy-Byrne, 2007; Trinh et al., 2016). Online environments like PatientsLikeMe encourage people to share their health data online, creating social health environments enabling people to engage with one another, increasing health awareness and supporting self-management (Frost & Massagli, 2008). Individuals may also decide to disclose their status in online dating application to meet other men with HIV; they may choose to disclose in online support forums to increase self-management or through online social networks to gain social support from friends and family.

Against these benefits, perceived costs to privacy have been identified as factors affecting non-disclosure (Derlega, Green, Serovich, & Elwood, 2002; Derlega & Barbee, 1998; Derlega et al., 2004; Emlet, 2008; Fesko, 2001; Greene, Derlega, Yep, & Petronio, 2003; Greene, Parrott, & Serovich, 1993; Serovich & Mosack, 2006; Winchester et al., 2013). Nevertheless, very little is understood about how privacy affects HIV disclosure in online interactions and the effects it has on managing online identities after diagnoses. In environments where the costs to a person's identity through ineffective privacy management can be significant, how is conviction developed around decisions to engage in technologies which require self-disclosure and self-presentation? When unintended online disclosures occur which affect the social desirability of the individual's identity, how does this impact on the individual's behaviour and their future decision-making under similar conditions?

The primary contribution of this research will be a better understanding of the interrelated role of privacy, self-disclosure, and self-presentation in the management of online identities of MSM when diagnosed with HIV. The research will contribute to the existing privacy literature through the development of a novel, narrative based approach to privacy information disclosure decision-making. In doing so, the research will look to understand online communication technologies from the perspective of MSM when diagnosed with HIV, exploring the central question of this research:

What factors influence the effective management of a person's online identity when diagnosed with HIV?

In exploring the different aspects of this question, the research will not only focus on interactions directly related to HIV. It will not for example, only explore the self-disclosure of an individual's HIV status, but will develop an understand of how a person's HIV status changes their perception of privacy and their online self-disclosure and self-presentation behaviour from a broader perspective.

3 Background

The methods used to communicate, socialise, and interact have changed significantly since the early 1980s when HIV was first recognised as a major problem. E-Mail, online social networks (OSNs) and e-commerce are just three technologies that have revolutionised our interactions. They have enabled people from around the world to connect with one-another, communicating to share: news, events, health and wellbeing data, multimedia, location, even providing live video broadcasting capabilities. Many of the technologies encourage users to build personal profiles, to disclose details of their offline lives and to establish social connections with one another. Many of these connections are known in the offline world, making online environments much less independent spaces (Baym, 2010). When using various platforms, people develop a plurality of contextually constructed, goal driven identities, with self-disclosure acting as a function of this behaviour (Schau & Gilly, 2003). These identities allow individuals to present different versions of their self to influence the way they are perceived, and to advance the goals pursued in the particular context (Chaudoir & Fisher, 2010; Chaudoir, Fisher, & Simoni, 2011; Derlega & Grzelak, 1979; Derlega, Metts, Petronio, & Margulis, 1993; Omarzu, 2000).

Privacy allows people to manage the way they present their self to others, feeling violated when others discover something about them they had not anticipated them knowing.

This is especially salient with sensitive information that has a discrediting or spoiling effect on an identity (Goffman, 1963). When diagnosed with HIV, individuals may experience their offline self going through a process of change, experiencing the feeling of a “new-self” at a time of considerable anxiety, paranoia and distress (Flowers, Davis, Larkin, Church, & Marriott, 2011, p.1381).

In the online world, the complexity of the environment can lead to concerns over unintended disclosures through organisational or social threats. These can include the sale of information to third parties (Dinev & Hart, 2006), analysis of the data to discover information the subject had never intended to be known (Kosinski, Stillwell, & Graepel, 2013; Malheiros, Preibusch, & Sasse, 2013), and the sharing of data between social contacts to spread rumours and gossip (Debatin, Lovejoy, Horn, & Hughes, 2009). Organisational threats to privacy have been shown to reduce the amount of information disclosed, whilst social threats create greater concern and awareness over the information being revealed (Krasnova, Günther, Spiekermann, & Koroleva, 2009), having a potentially negative impact on individuals’ health.

When self-disclosing sensitive information to others, uncertainty exist over how this information will be viewed, and how it will impact on the impression that is “given off” (Goffman, 1956). Self-disclosure allows people to reveal information about their self in the form of emotionally constructed, personalised narratives which adds contexts to the information. If this is missing then the information receiver may start to develop their own narrative, void of this emotion. This may increase the discrediting effect, inhibiting the individual’s ability to manage the presentation of their self, leading to discrepancies between how the individual perceives their self to be, and how others perceive them (Higgins, 1987).

The discrepancy between what Higgins (1987) refers to as the *actual* self and the *ought* or i*deal* self others have may lead to individuals taking action to maintain consistency between these different states. When diagnosed with HIV, individuals may change their behaviour to protect this new aspect of their identity from being revealed, in what Arkin (1981) describes as protective self-presentation. This protective approach is used to avoid disapproval through more modest, or neutral self-presentation and seeks to minimise the risk of the person's identity becoming spoilt through unintended disclosures. This protective behaviour in a complex online environment may lead to individuals placing greater weight on the short and long term disclosure cost. This may increase the cognitive load when acting to protect the self, resulting in load reducing acts to simplify their online lives, such as reduced self-disclosure, technology abandonment or anonymising communications.

4 State of the Art

This research starts from the premise that privacy allows people to choose the information they disclose, with self-disclosure acting as a functional aspect of how people present their self to others. This section will review the existing literature on privacy, relating it to identity management, self-presentation, and self-disclosure. The contextual nature of privacy and the social stigma of HIV creates a unique environment in which to study these concepts. To further our understanding of the contextually specific factors affecting HIV disclosure, previous HIV disclosure research in both offline and online interactions will be reviewed. Finally, research which proposes narratives as a way of understanding decision-making will be reviewed to support the narrative based approach of this current research.

4.1 Privacy in the management of the self

In a world without privacy, people would be ill equipped to manage how they develop and present different versions of their self in different online environments, a behaviour referred to here as identity management (Suler, 2002). The first part of this section presents an introduction to privacy from several different perspectives, and then introduces a model of privacy that will be used as part of this research. As this work relates to privacy's role in the management of online identities, this section will also explore the concept of self-disclosure and how it relates to the way people present their identities to others. Finally, this section will discuss the role privacy plays in allowing people to manage not just what they disclose to others, but how it is presented and used to support identity.

Privacy as a concept can be explored from several different perspectives, it crosses many disciplines and is inherently quite broad in its scope. Post (2000) described privacy as a complex value, with many dimensions in conflict or competing with one another. The term privacy is often replaced with the word secrecy, with Posner (1977) suggesting people's right to secrecy as a form of privacy; with control a way of limiting distribution of secrets. The idea that a person must have control for privacy to exist was disputed by Reiman (1995) who identified excretion as a situation which lacks control, but expects privacy. There are also conflicts when viewing privacy as a right to secrecy. As an example, people living with HIV may not always have control over whether they disclose their status, being unable to access HIV testing services, or receive treatment without disclosure. These types of conflicts create significant challenges for privacy when the states within which things can exists are fixed around rigid definitions.

In contrast to the earlier literature which framed privacy around dichotomies of public/private, control/no control, Nissenbaum's (2009) theory of privacy as a contextual integrity suggests a more nuanced, contextualised approach. To illustrate this from an OSN perspective, when someone posts a message containing information of low intimacy to their online network, they may consider the environment private, sharing only to a restricted group of people; perhaps their family, friends and acquaintances. When the intimacy of the content is increased, this same environment may be considered much less private. In this example, the context around the information being posted changed, and whilst the audience stayed the same, the expectations of privacy were higher as the sensitivity of the information increased. This example illustrates that absolute control over information is not possible or expected in the online world, and instead, norms around the appropriate flow of information is being used to manage privacy expectations (Nissenbaum, 2009). This type of online behaviour shows that people are willing to relinquish control over their data to increase usability, but they do not lose awareness or cease to care over what other people know about them. Gavison (1980) discussed this in terms of a privacy scale, taking a neutral, descriptive perspective to describe privacy as the level of access and awareness a person has over others, from both a physical and a relational perspective. She suggests different factors affect the scale of privacy, namely: knowledge, physical proximity, awareness and access to others.

In attempting to model privacy, researchers have typically focused on a specific element of privacy, such as understanding how concerns to privacy are formed (Krasnova et al., 2009; Smith, Milberg, & Burke, 1996; Xu, 2007; Xu, Dinev, Smith, & Hart, 2008), and how these privacy concerns impact on willingness to disclose information online (Dinev & Hart, 2006; Dinev & Hart, 2005; Dinev, Hart, & Mullen, 2008; Dwyer et al., 2007). The Adams and Sasse (2001) privacy model which will be used in this current research does not focus on how privacy concerns are formed, or include privacy as a factor in the disclosure process, instead modelling how users' perceptions of privacy are formed using a number of contextually specific emotional constructs.

The Adams and Sasse (2001) privacy model was originally developed around multimedia communications, but has much broader applicability. The model suggests that users evaluate privacy by judging the sensitivity of the information being disclosed, evaluating the trust in the person receiving the information and assessing the cost and benefits of disclosing the information for a perceived pay-off (Adams & Sasse, 2001). Each of these elements interrelate, for example, as the sensitivity of the information increases, so too does the required trust in the information receiver. The model provides an understanding of the privacy evaluation behaviour that users make before self-disclosing online, but does not explain how users decide to disclose on the outcome of their evaluations, how these evaluations and disclosures affect identity, and how a person’s experiences impact on the emotional constructs of this model. In understanding identity within the context of privacy, self-disclosure will first be examined, seeking to understand how it is used in the presentation of a person’s identity.

Self-disclosure is described as a functional goal driven behaviour, used to validate, express and present the self to others (Derlega & Grzelak, 1979; Schau & Gilly, 2003). Revealing information in a progressive behaviour by increasing the depth and breadth of information disclosed allows for more intimate relationships to develop (Altman & Taylor, 1973). Altman and Taylor's (1973) social penetration theory (SPT) proposed that when meeting for the first time, the goals of disclosure are to maximise social desirability, following norms of social appropriateness. This progressive and reciprocal nature of self-disclosure is suggested as a mechanisms for establishing interpersonal trust (Wheeless, 1978). Providing some evidence of this, Zea, Reisen, Poppen, Echeverry, & Bianchi's (2004) found that HIV positive MSM were more likely to disclose their status to a person they had had previous discussed intimate information with, such as their sexual orientation.

Similar to the reciprocal nature of relationships, the disclosure of information at a certain breadth and depth is often reciprocated with a similar level of personal information (Derlega et al., 1993; Joinson, 2001). This reciprocal exchange of intimate information may help to build trust in the relationship, with both parties feeling less exposed with the increased information symmetry that exists. However, the reason for reciprocal disclosures online may not be exclusively attributable to trust building. Joinson (2001) suggest speech pattern matching behaviour may be used when interacting online, with people disclosing more or less information, dependent on the word count or duration of other people's disclosures.

Extending SPT, Omarzu (2000) developed a three-stage disclosure decision model which incorporates the dimension of duration, measured as the amount of time spent, or the volume of information disclosed. In her model, she suggests that increased perceptions of utility leads to increases in the breadth and duration of disclosure, whilst the perceived costs of disclosing are associated with levels of intimacy (Omarzu, 2000). Discussing large amounts of information for long periods of time at a superficial level is unlikely to expose a person to high levels of risk, whilst disclosing intimate details of a person's HIV status will increases risk of social rejection, and the spoiling of their identity if privacy is violated. The consistent theme running through these theories of privacy and self-disclosure is that of identity, and the risk of intimate information becoming known to others resulting in the person's identity being perceived negatively by others.

In exploring the concepts of identity, and the way people present their self to others, Goffman (1956) used a dramaturgical approach, describing the world is a stage upon which people conduct the performances of their lives. He suggests that individuals present their self with the goal of being perceived positively by others, a mode of self-presenting described by Arkin (1981) as the acquisitive self. Arkin suggests two presentation strategies. The first is the default acquisitive self, used to gain approval from others, and the second, the protective self used to present a neutral image and intended to avoid disapproval. These two self-presentation modes can be used interchangeably, depending on the contextualised goals of the individual. For example, when a person is diagnosed with HIV, they may use online support forums to seek help and advice from others, not to seek approval but to minimise disapproval. As people present different versions of their self to different audiences, they carefully monitor and regulate the communication stimuli to ensure that their desired identity is being effectively presented (Brown, 2014). Goffman (1956) described this as the unintended impression that are “given-off”, as opposed to the impressions that individual’s intend to “give”, suggesting identity management as a form of control over how others perceive the self. Leary (1995) is more specific in relating control with self-presentation, describing it as “The process of controlling how one is perceived by other people” (p.2). If privacy is a form of control over information about our self (Fried, 1968; Froomkin, 2000; Joinson & Paine, 2012; Posner, 1977), then privacy becomes a fundamental requirement when performing effective self-presentation. If control over a person’s personal information is lost, it may inhibit their ability to manage how other people perceive them, creating discrepancy between how they perceive their self to be, and how other people perceive them to be (Higgins, 1987).

Higgins' (1987) self-discrepancy theory (SDT) proposes three states of the self, all of which can be viewed from both the perspective of the individual, or from the perceptive of other people. Our actual self is the way in which *we believe our self to be*, helping to create our self-concept; our ideal self is the self that *we would like to be*; and lastly our ought self, the self that *we believe society would like us to be*. People who have accepted their HIV status and possess an up-to-date understanding of the impact the condition has on their lives may perceive their self differently to how others perceive them. SDT proposes that we are driven by our desire to reduce discrepancy between our actual self (our self-concept), and the other states of self. Higgins (1987) postulates that increased discrepancy between two states results in an increase in various negative psychological conditions. As we interact, the expectations of audiences in different environments will change the level of discrepancy between our self states. It is not uncommon to hear people suggest that they “feel themselves” around certain groups when discrepancy between states is low. When people are in an environment where discrepancy is high, they may change the way they present to minimise discrepancy, to become more socially desirable. But it may not always be the individual who adjusts their self to their social setting. People may use self-disclosure and self-presentation strategies to exchange more intimate information with others; to build better relationships which help them to adapt the expectations of people within that environment. As an example, in a family setting a person with HIV may disclose personal information related to their status to help build a positive narrative around their condition. Disclosing this information, and updating and educating those around them may lead to a change in people's perceptions, and help to reducing discrepancies between self states that may have existed.

The process of self-presenting provides a mechanism for people to control how they project their identity to others, but it does not explain the way in which identity itself is constructed. From a philosophical perspective, the question of self has long been discussed. This research will not seek to understand what the self is, instead focusing on a theory of identity which relates to the narrative focus of this research. To do this, we will explore the self from an autobiographical perspective, suggesting people shape the story of their lives (and in parallel their identities) through the joining of narratives developed from lived events (Buitelaar, 2014). However, unlike a story the past events of a person's life are not fixed in their interpretation or in their significance to a person's broader identity. Buitelaar (2014) makes the point that when memories of past events are recalled, they are done so through an action in the present, which has the unavoidable consequence of affecting the way past events are remembered. In contrast to the fallible nature of human memory, data of our online self is stored on computerised devices, often backed up, cached and copies many times over. These electronic identities cannot be dynamically remembered, reinterpreted and reconstructed like human memory (Buitelaar, 2014). Because of this, the function of privacy in the online space is different to that in the offline, as the data sets that form online identities are much more persistent and static in design.

4.2 HIV Disclosure

This section of the review will explore the research on HIV disclosure which has three main focuses: the influence the information receiver has on disclosure; antecedent disclosure factors; and the perceived costs and benefits of disclosure. Lastly, this section will review literature which has explored disclosure of HIV in online environments and discuss these findings in relation to existing privacy models.

On being diagnosed with HIV, the condition becomes a new aspect of a person's self (Flowers, Davis, Larkin, Church, & Marriott, 2011). Individuals face the decision of whether to disclose their condition to certain people within their social environment. They may wish to discuss their status with family, friends and loved ones, but each disclosure comes with risks to the individual's privacy. Violations to their privacy through unintended or intentional disclosures could be harmful and discrediting to both their online and offline identities (Derlega, Winstead, Green, Serovich, & Elwood, 2004). Whilst disclosure may not always be a choice, with certain conditions creating a legal requirement to disclose (aidsmap.com, n.d.), where a choice does exist, it is important to understand the factors which affect this behaviour.

When reviewing the literature on HIV disclosure, a key area of focus is on the information recipients. The groups that are typically focused on are close family, intimate partners, and friends. In the following studies, the researchers found that people with HIV were more likely to disclosure their status to their intimate partners and close friends (Hays et al., 1993; Mansergh, Marks, & Simoni, 1995; Manson, Marks, Simoni, Ruiz, & Richardson, 1995; Marks et al., 1992; Zea et al., 2004). However, in a study of HIV positive Latino women, the rates of disclosure to extended and close family were lower than with intimate partners and friends (Simoni et al., 1995).

In a study of HIV positive men and women (n=331) the researchers found that friends were disclosed to more often than family members, with friends being perceived as more supportive; whilst female family members were perceived as being more supportive than male family members (Kalichman et al., 2003) Similar research conducted in Uganda with both male and female participants (n=949) being treated with anti-retroviral therapy (ART) drugs, found higher rates of reported early disclosure to family and intimate partners than with friends (Winchester et al., 2013).

Research into the antecedent disclosure factors and their effect on different groups found that prior knowledge of sexual orientation was associated with increased levels of disclosure (Zea et al. 2004), suggesting that the experience of disclosing sexual orientation adds to the individual’s prior state of knowledge, helping them form future disclosure decisions. As an example, having disclosed an intimate piece of information to a friend, prior knowledge around how the person reacted, the emotions felt and the conditions of the environment after disclosing may help to build subjective knowledge for future disclosures in similar conditions.

Derlega et al.'s (2004) study explored the reasons for serostatus disclosure to different groups and found that women were more likely to disclose to close friends and intimate partners to test their reaction. Whilst men exhibited similar behaviour towards intimate partners, they did not show this behaviour towards close friends (Derlega et al., 2004). Health concerns and honesty were identified as the most frequent reason for disclosing to intimate partners, with family members often being disclosed to out of a sense of loyalty and to avoid them finding out through third parties (Derlega et al., 2004). This concern over third party disclosures is related to privacy, and the act of self-disclosure in this case can be used as a tool to increase the individuals control. By choosing to disclose, they can present the information in a narrative, contextualising it and adding emotion.

Privacy was explicitly identified as a reason for non-disclosure to close friends in both male and female participants but had less of an effect on the decision to disclose to family members (Holt et al., 1998). Privacy in this context may be felt as a reason for non-disclosure to friends due to the choice that is felt around disclosing, whilst a sense of duty to disclose may exist with family members and intimate partners.

4.2.1 The Cost/Benefits of Disclosure

As has been discussed, the sensitive and stigmatised nature of HIV means disclosure is unlikely to occur without some benefit being offered. This section will explore the literature which examines both the benefits and costs people perceive when disclosing.

HIV disclosure can have a positive impact on a person’s life and wellbeing through increased levels of social support, and helping to reduce the amount of stress and anxiety felt from living with the condition (Kalichman et al., 2003). From a health perspective, the immune system can be negatively impacted by the suppression of certain thoughts, feelings and behaviours (Pennebaker, 1997), and serostatus disclosure has been shown to help response to ART treatment (Stirratt et al., 2006; Strachan et al., 2007; Trinh et al., 2016). The unburdening of a secret to a close friend or relation can play an important role in the recovery process from psychological states of stress and anxiety (Derlega et al., 1993; Hays et al., 1993; Schatzow & Herman, 1989). Disclosure of serostatus can also be used to educate others to reduce the anachronistic discourse that exists around the condition (Murphy, Hevey, O’Dea, Ni Rathaille, & Mulcahy, 2015).

When an individual discloses their status, they help create more openness, reducing stigma and normalising disclosure within society (Chaudoir & Fisher, 2010). Educating others has been identified as a reason to disclose amongst both males and females with HIV (Derlega et al., 2004), helping to reduce the stigma associated through anachronistic discourse of depravity and infectiousness that still exists (Murphy et al., 2015).

The stigma attached to the condition, and behaviour associated with the condition may lead to increased perceived costs when disclosing to loves ones (Leary & Schreindorfer, 1998). Derlega et al. (2004) also identified a concern over the stigma that may be associated to their loved ones by association, if their status was to become known. Similar to these findings, a study in Uganda reported privacy concerns as being the most significant reason for non-disclosure of HIV, together with a belief that disclosure was simply not necessary (Winchester et al., 2013). The privacy concerns reported in these studies are an indication of the impact the stigmatised nature of the condition may have on a person's identity (Winchester et al., 2013). The believe that disclosure is not always necessary may be affected by the external symptoms the individual is experiencing, with research suggesting that people showing external symptoms (symptomatic) are more likely to disclose than those with no visible symptoms (asymptomatic) (Hays et al., 1993; Mansergh et al., 1995; Marks et al., 1992; O'Brien et al., 2003)

4.2.2 Disclosing Online

This section will explore literature on the disclosure of HIV online; however, prior to this we will explore some of the differences between online and offline interactions, and how these can impact on the way people disclosure and present their identities.

Online interactions can be more limited when compared to face-to-face communications, with certain non-verbal stimuli, such as body language and facial expressions no longer available. However, as social beings we have become quick to adapt to these new communication mediums, developing new techniques, such as "emoticons" to bridge these gaps (Attrill, 2015). It's not just the way online interactions have changed the way emotions are communicated, the entire dynamics of our social and interactions have changed. People are now able to stay connected to more people over longer distances for longer periods of time.

Communication are no longer synchronous, with people having to reply to one another immediately. Whilst face-to-face communication flows naturally, with replies immediate and often overlapping, typed conversations can continue with large time delays between responses; allowing for more "slow time" cognitive thought between replies. Online, people can review what they are about to disclose, and may also have the option of editing or deleting messages after disclosure. These conditions in the online world may help people to test new aspect of their self in environments void of judgement. The anonymity of the internet may provide this identity exploration environment, helping people in the transition period after diagnosis to better understand the social impact of their condition. It may provide a space in which new aspects of their identity can be developed, creating coherent and emotional narratives used to engage in acquisitive self-presentation in other environments (DeHaan, Kuper, Magee, & Bigelow, 2013)

Alongside the changes in the way people communication, there have also been significant developments in HIV treatment, with Highly Active ART (HAART) drugs increasing life expectance and reducing transmission rates. In 2008, the Swiss National AIDS Commission issued a statement stating that if certain conditions were met, HIV was no longer a sexually infectious virus. This statement became known as the 'Swiss statement', and whilst the commission rolled back on its zero risk statement, it did maintain that the risk was significantly reduced to around 1 in 100,000 (NAM, n.d.). These improvements in transmission rates, as well as improved quality of life of those with HIV may also affect status disclosure in certain groups.

When self-presenting online to engage in sexual activity, before engaging in their first sexual encounter HIV positive MSM were found to be less likely to disclose their status (44.7%) than HIV negative MSM (62.8%) (Carballo-Diéguez, Miner, Dolezal, Rosser, & Jacoby, 2006). Their research also found that HIV positive men were less likely to discover their partner’s serostatus than HIV negative men, whilst both groups were more likely to disclose their status online than in person (Carballo-Diéguez et al. 2006). Supporting this finding, a later study showed that 50% of those diagnosed HIV positive had shared their status on all or some of their online profiles (Horvath, Oakes, & Rosser, 2008).

The relative anonymity that the Internet provides, in comparison to face-to-face communication is suggested as the reason for this increase in online disclosure. From an identity development perspective, Internet users can develop a plurality of contextually constructed online identities through the creation of alternative accounts (Chester & Bretherton, 2012). Users can reinvent themselves by setting up new user profiles, or moving to different online platforms. This can make the spoiling of an online identity feel less permanent than in the offline world, where anonymity and reinvention of identities is more difficult to achieve. Whilst Diéguez et al.'s (2006) research provides a useful insight into the disclosure behaviour of HIV MSM engaging in online sexual negotiations, it is limited in only addressing the most recent sexual partners of the participants, and exploring disclosure through limited communication strategies. Privacy preserving behaviour, including the selective disclosure of information is contextually rich, and dependent on different factors, such as trust, judgement of the sensitivity of the information being disclosed, as well as context specific cost-benefit factors associated to disclosing (Adams & Sasse, 2001). Their research was carried out prior to the popular adoption of online social networks, including location aware dating applications which are now commonly in used for dating and sexual negotiations (Birnholtz, Fitzpatrick, Handel, & Brubaker, 2014; Bull & McFarlane, 2000; Liau, Millett, & Marks, 2006; Mcfarlane & Rietmeijer, 2005).

4.3 Privacy Narratives

An important aspect of this research is in understanding how people make online disclosure decisions. This section of the state of the art will review literature on behavioural decision-making, with a specific focus on a theory developed to understand the formation of narratives and their use in developing decision conviction.

The privacy model developed by Adams and Sasse (2001) provides a view of the decision-making processes around information disclosure, with a cost-benefit analysis being proposed to ascertain the utility of disclosure. The model introduces trust in the recipient of the information and judgement of the sensitivity of the information being disclosed; two subjective and emotionally influenced factors. Together with the uncertainty over both the short and long-term costs to privacy, these factors are explored here with the use of conviction narrative theory (CNT) (Chong & Tuckett, 2015; Tuckett & Nikolic, 2016).

Many of the decision-making theories take a dual model approach, with Daniel Kahneman (2011) popularising this with System 1 and System 2; System 1 describing the cognitively demanding, slow but more rational decision-making process and System 2 describing the fast and emotional process, often affected by cognitive biases. These dual models suggest that people evaluate decisions using either System 1 or System 2, whilst CNT proposed a circular interaction exists between the two. Dual models of decision-making provide an important understanding of the different states and processes people use when forming decisions, but they do not address the way in which people evaluate the outcome of thoughts and subjective knowledge generated when anticipating the outcome of an action.

CNT is a social-psychological theory which is proposed in this current research as an extension to the Adams and Sasse (2001) privacy model. 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 technology evolving, changing the complex socio-technical systems within which people interact.

CNT proposes that in conditions of uncertainty, when the probability of a successful action cannot be known, 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 disclosure (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 MSM are diagnosed with HIV, the risk disclosure has on their identity creates an environment of considerable uncertainty.

Because of these concerns, seropositive MSM are unlikely to disclose their status 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 person’s 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 website that allow them to browse without giving over their name or any personal details.

Once an opportunity has been identified, the individual will start evaluating possible future disclosure actions through the identified opportunities. The Adams and Sasse (2001) privacy model proposes three constructs 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.

As these different constructs of the model interrelate, a decision made for one (e.g. trust in the information receiver) may affect the decision of another (e.g. judgement of information sensitivity). In developing the decisions for each construct, it is proposed that people use both slow, cognitively demanding (System 1), and fast emotion decision-making process (System 2). From a System 2 perspective, past experiences in the form of behavioural schemas may be used to help individuals evaluate the expected outcome of the disclosure, in what Klein (2008) refers to as Recognition-Primed Decision-Making (RPD). These "fast and frugal" decision-making mechanisms are used to assess these elements of the model against the goals pursued by the individual (Goldstein & Gigerenzer, 2002).

RPD suggests that people use experiences to help them visualise, or simulate potential future outcomes (Klein, 2008) . It is proposed here that these simulations take the form of narratives, constructed to allowing people to visualize and compare different scenarios resulting from the various actions identified. These narratives are developed as a result of a human capacity to visualise, describe and communicate the future with their ability to use memory to mentally travel both into the past and the future (Chong & Tuckett, 2015; Gilbert, 2007; Suddendorf & Corballis, 1997; Tulving, 1993). This simulation of the future allows individuals to "test" their actions, developing and simulating different narratives for different scenarios, creating subjective "knowledge" on their outcomes, creating either approach or avoidance emotions. When evaluating the action of disclosure, individuals may discover privacy invasive information resulting in avoidance emotions, or details related to a feature within the technology which creates feelings of approach. Depending on the state of the individual, this new information may change the developed narrative, or it may simply be ignored. CNT refers to these two states as 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 reflect upon it, perhaps until the person’s state changes.

In the social environment, when making decisions in uncertain conditions, Tuckett and Nikolic (2016) suggest that narratives are used to 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, may result in either stronger feelings of accuracy or re-evaluation of the disclosure action. 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. Using Goffman (1959) dramaturgical approach to identity, this information will be used to present a version of the persons self to their external audience, after which they can evaluate 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 perceives them to be may 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 and act as a form of social learning for others, in what Gilbert (2007) describes as surrogates, or other peoples' narratives. Using these surrogates may help people predict the outcome of their decisions more successfully than if they were to just simulate the possible future outcome (Gilbert, 2007). As well as helping other people develop better decision, these past events are stored as schemas of behaviour in memory. These can be used by the individual to make better predictions of outcomes when performing future decision-making in similar conditions (Klein, 2008).

5 Proposed Approach

As this research is exploratory, its primary contribution is to better understand the factors that influence the effective management of a person's online identity when diagnosed with HIV. The research will contribute to the existing state of the art, developing a narrative based approach to understanding online privacy decision-making. To better support those who have been diagnosed to manage their online relationships and interactions, it is important to gain an empirical understanding of the effect online privacy concerns have on self-disclosure and self-presentation behaviour, and its impact on identity.

The research will study the behaviour of men who have sex with men (MSM) recently diagnosed with HIV, providing a unique context in which to study privacy and identity management due to the high information sensitive and stigmatised nature of the condition.

6 Research Methodology

This section provides an overview of the proposed studies planned throughout this research. Detailed thematic analysis will be conducted on data collected from a series of qualitative studies, including online focus groups, semi structured interviews with MSM, as well as interviews with sexual health professionals. The data collected and the analysis methods used will provide greater insight into the effect privacy has on identity management.

It will also provide an understanding of behaviours and factors involved in the effective management of identity in online environments. As our research will also explore MSM who have been tested negative, as well as healthcare professions, the research will provide insight from different perspectives, and identify how these perceptions differ.

Finally, throughout this research, existing privacy, behavioural decision-making and narrative identity theories will be used to understand the qualitative data collected and to develop a behavioural model which will be tested in the final stage of this research.

6.1 Phase 1: Systematic Literature Review

The first part of the research will consist of a comprehensive review of the literature on HIV disclosure, self-disclosure, and self-presentation in both offline and online environments. The review will focus on research conducted around HIV, but will also draw from more broader literature with research conducted around stigmatised conditions prioritised. In conducting this literature review, an exploration into privacy and disclosure decision-making research, as well as theoretical work around key concepts such as stigma and the self will be reviewed. The findings of this research will inform the development of a preliminary privacy disclosure decision-making model, further developed throughout the research. The review will also provide the research with the background required to develop a set of questions for both sexual health professions and MSM.

6.2 Phase 2: Interviews with Sexual Health Professionals

Forming the first of the data collection studies will be a review of existing online and offline guidance made available to people with HIV to help them manage their online communications. The study will inform semi structured interviews with a minimum of 3 sexual health professionals in the South-East of the UK, who provide guidance to HIV patients. The purpose of this study is to understand the type of verbal, visual and electronic guidance that is currently provided, and to ascertain its perceived effectiveness from the perspective of healthcare professionals.

6.3 Phase 3: Online Focus Group

The data collection methods are a particularly challenging aspect of this research, as the researcher is requesting participants to self-disclose and self-present, two of the concepts being explored. The stigmatised nature of HIV may reduce the richness of information disclosed due to privacy and confidentiality of the information being discussed, as well as the comfort level of the participants in discussing intimate subjects with the researcher.

Whilst focus groups can provide greater breadth of understanding of perceptions and experiences (Blandford, Furniss, & Makri, 2016), the face-to-face nature of focus groups make it difficult to achieve anonymity. When discussing topics of a sensitive nature, participant anonymity has been shown to reduce inhibitions and facilitate more open, detailed discussion (Joinson, 1999; Montoya-weiss & Massey, 1998; Stewart & Shamdasani, 2017; Suler, 2004; Tates et al., 2009).

Using online focus groups as a methodology for research also provides the researcher with insight into the way in which HIV positive MSM discuss and disclose details of their self in an online setting, and the online environmental factors that support positive disclosure and interaction decisions. It is envisaged that conducting this study online allows the group to reflect on their disclosures and the disclosures of others over a longer period, a benefit not available in face-to-face groups.

6.4 Phase 4: Semi-Structured Interviews with MSM

Semi-structured qualitative interviews will be conducted with MSM whom are un-tested, tested negative and tested positive for HIV. This data collection method is well suited for understanding the perceptions and behaviours of people and their interactions with technologies; allowing for more detailed and thorough means of investigating areas of interest to the research (Adams & Cox, 2008; Blandford et al., 2016). Broadly, this study will be informed by the online focus groups and will be designed to focus and probe in more detail into factors and behaviours identified in the previous study.

Focusing on both HIV negative and positive MSM will allow the researcher to interview MSM without requiring them to disclose their HIV status unless they choose to, and provides a basis for comparison. Each participant will be asked to complete a pre-interview questionnaire with the intention of identifying their base line personality traits This will provide insight into whether these personality factors impact on disclosure and self-presentation behaviour.

6.5 Phase 5: Behaviour Model Tests

Throughout phases 1-4, the data collected will be used to develop a behavioural model to understanding how MSM, when diagnosed with HIV, develop conviction to disclose their status online. Phase 5 will test this model with the development, distribution and analysis of the results from a questionnaire; distributed to the target group through support networks and sexual health clinics. Questionnaires are a good way of measuring attitudes, knowledge and behaviour (Oppenheim, 2000), the results of which can be used to generalise to the wider target group (Boynton & Greenhalgh, 2004).

In understanding and testing this model, it is expected to be able to inform technology designers developing applications for people with HIV which require some form of identity management, through self-disclosure and self-presentation. These could include online support groups, discussion forums or dating applications.

7 Work Plan

To help the researcher maintain a schedule of work and to set mile stones for each of the phases of the project, a work plan for the period September 2016 – September 2019 has been developed (Figure 1). The plan shows clear periods of time in which each of the phases should be completed, marks the periods where each VIVA should occur, and provides suitable time for writing up the results and completing the final thesis towards the end of the period.

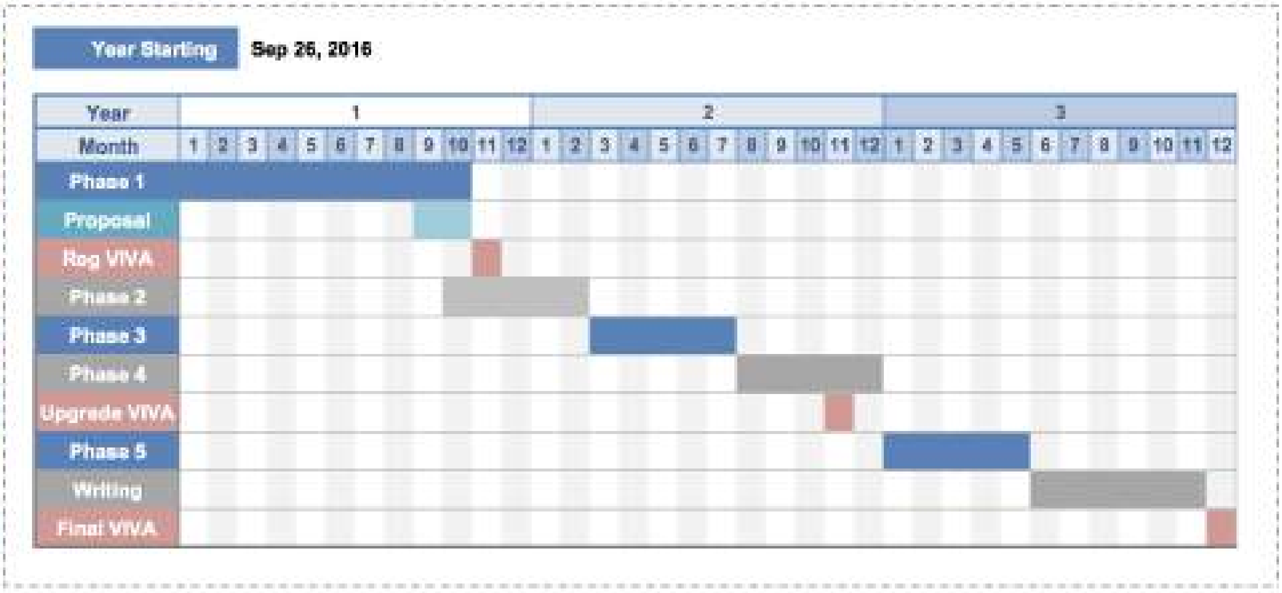


Figure 1

8 References

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*. Retrieved from http://ieeexplore.ieee.org/abstract/document/1392696/

Adams, A., & Cox, A. (2008). Questionnaires , in-depth interviews and focus groups. In P. Cairns & A. Cox (Eds.), *Research Methods for Human-Computer Interaction* (pp. 17–34). Cambridge University Press.

Adams, A., & Sasse, M. (2001). Privacy in multimedia communications: Protecting users, not just data. *In People and Computers XV—Interaction without Frontiers*, 49–64. Retrieved from http://link.springer.com/chapter/10.1007/978-1-4471-0353-0_4

aidsmap.com. (n.d.). Transmission of HIV as a criminal offence. Retrieved May 7, 2017, from http://www.aidsmap.com/Timeline-of-developments-in-the-criminalisation-of-HIV-and-STI-transmission-in-the-UK/page/1504201/

Altman, I., & Taylor, D. (1973). *Social penetration: The development of interpersonal relationships.* Retrieved from http://psycnet.apa.org/psycinfo/1973-28661-000

Arkin, R. (1981). Self-presentation styles. *Impression Management Theory and Social*. Retrieved from https://books.google.co.uk/books?hl=en&lr=&id=ee9FBQAAQBAJ&oi=fnd&pg=PA311&dq=arkin+1981+self+presentation&ots=eIp75IEiJ7&sig=Qd6dk5Mh8nwTWqSsnw6onJcyOZc

Attrill, A. (2015). *The Manipulation of Online Self-Presentation: Create, Edit, Re-edit and Present*. https://doi.org/10.1057/9781137483416

Baym, N. (2010). *Personal Connections in the Digital Age*. *Digital Media and Society Series*. Polity Press. https://doi.org/10.1080/10714421.2011.573442

Birnholtz, J., Fitzpatrick, C., Handel, M., & Brubaker, J. R. (2014). Identity, Identification and Identifiability: The Language of Self-Presentation on a Location-Based Mobile Dating App. *To Appear in Proc. MobileHCI 2014*, 3–12. https://doi.org/http://dx.doi.org/10.1145/2628363.2628406

Blandford, A., Furniss, D., & Makri, S. (2016). Qualitative HCI Research: Going Behind the Scenes. *Synthesis Lectures on Human-Centered Informatics*, *9*(1), 1–115. https://doi.org/10.2200/S00706ED1V01Y201602HCI034

Boynton, P. M., & Greenhalgh, T. (2004). Selecting, designing, and developing your questionnaire. *BMJ : British Medical Journal*, *328*(7451), 1312–1315. https://doi.org/10.1136/bmj.328.7451.1312

Brown, J. (2014). *The self*. Psychology Press. Retrieved from https://books.google.co.uk/books?hl=en&lr=&id=7FK3AwAAQBAJ&oi=fnd&pg=PP1&dq=%22the+self%22+brown&ots=40vPDWwHJ3&sig=d1apfdbOy9UTiEDyrS_NjKWBJBM

Buitelaar, J. C. (2014). Privacy and Narrativity in the Internet Era. *The Information Society*, *30*(4), 266–281. https://doi.org/10.1080/01972243.2014.915278

Bull, S. S., & McFarlane, M. (2000). Soliciting sex on the Internet: what are the risks for sexually transmitted diseases and HIV? *Sexually Transmitted Diseases*, *27*(9), 545–50. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/11034529

Carballo-Diéguez, A., Miner, M., Dolezal, C., Rosser, B. R. S., & Jacoby, S. (2006). Sexual negotiation, HIV-status disclosure, and sexual risk behavior among latino men who use the internet to seek sex with other men. *Archives of Sexual Behavior*, *35*(4), 473–481. https://doi.org/10.1007/s10508-006-9078-7

Chaudoir, S. R., & Fisher, J. D. (2010). The disclosure processes model: Understanding disclosure decision making and postdisclosure outcomes among people living with a concealable stigmatized identity. *Psychological Bulletin*, *136*(2), 236–256. https://doi.org/10.1037/a0018193

Chaudoir, S. R., Fisher, J. D., & Simoni, J. M. (2011). Understanding HIV disclosure: A review and application of the Disclosure Processes Model. *Social Science and Medicine*, *72*(10), 1618–1629. https://doi.org/10.1016/j.socscimed.2011.03.028

Chester, A., & Bretherton, D. (2012). Impression management and identity online. *Oxford Handbook of Internet Psychology*, 1–18. https://doi.org/10.1093/oxfordhb/9780199561803.013.0015

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

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-*

Mediated Communication, *15*(1), 83–108. https://doi.org/10.1111/j.1083-6101.2009.01494.x

DeHaan, S., Kuper, L., Magee, J., & Bigelow, L. (2013). The interplay between online and offline explorations of identity, relationships, and sex: A mixed-methods study with LGBT youth. *Journal of Sex*. Retrieved from http://www.tandfonline.com/doi/abs/10.1080/00224499.2012.661489

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.

Derlega, V. J., & Barbee, A. P. (1998). HIV and social interaction. *(1998).HIV and Social Interaction.x, 269 pp.Thousand Oaks, CA, US: Sage Publications, Inc*.

Derlega, V. J., & Grzelak, J. (1979). *Appropriateness of self-disclosure*. *Self-disclosure: Origins, patterns, and implications of openness in interpersonal relationships*. Retrieved from http://www.tandfonline.com/doi/abs/10.1080/07362999408809355

Derlega, V. J., Metts, S., Petronio, S., & Margulis, S. T. (1993). *Self-Disclosure*. *Sage series on close relationships*.

Derlega, V. J., Winstead, B. a, Green, K., Serovich, J., & Elwood, W. N. (2004). Reasons for Hiv Disclosure / Nondisclosure in Close Relationships : Testing a Model of Hiv – Disclosure Decision Making. *Journal of Social and Clinical Psychology*, *23*(6), 747–767. https://doi.org/10.1521/jscp.23.6.747.54804

Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*, *10*(2), 7–29.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*. Retrieved from http://pubsonline.informs.org/doi/abs/10.1287/isre.1060.0080

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance - An empirical investigation. *Journal of Strategic Information Systems*, *17*(3), 214–233. https://doi.org/10.1016/j.jsis.2007.09.002

Dwyer, C., Hiltz, S., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *AMCIS 2007 Proceedings*. Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1849&context=amcis2007

Emlet, C. a. (2008). Truth and consequences: a qualitative exploration of HIV disclosure in older adults. *AIDS Care*, *20*(6), 710–7. https://doi.org/10.1080/09540120701694014

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

Flowers, P., Davis, M. M., Larkin, M., Church, S., & Marriott, C. (2011). Understanding the impact of HIV diagnosis amongst gay men in Scotland: An interpretative phenomenological analysis. *Psychology & Health*, *26*(10), 1378–1391. https://doi.org/10.1080/08870446.2010.551213

Fried, C. (1968). Privacy. *Yale Law Journal*, *77*, 475–93.

Froomkin, A. M. (2000). The Death of Privacy? *Stanford Law Review*, *52*(5), 1461. https://doi.org/10.2307/1229519

Frost, J. H., & Massagli, M. P. (2008). Social uses of personal health information within PatientsLikeMe, an online patient community: What can happen when patients have access to one another’s data. *Journal of Medical Internet Research*, *10*(3). https://doi.org/10.2196/jmir.1053

Gavison, R. (1980). Privacy and the Limits of Law. *The Yale Law Journal*. Retrieved from http://www.jstor.org/stable/795891

Gilbert, D. (2007). Stumbling on Happiness. *Psychology*, *37*, 336. https://doi.org/10.1108/09534810710760108

Goffman, E. (1956). *The presentation of self in everyday life*. *Anchor Books*. (Vol. 21). https://doi.org/10.2307/258197

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

Goldstein, D. G., & Gigerenzer, G. (2002). Models of ecological rational- ity: The recognition heuristic. *Psychological Review*, *109*(1), 75–90. https://doi.org/10.1037//0033-295X.109.1.75

Greene, K., Derlega, V., Yep, G., & Petronio, S. (2003). *Privacy and disclosure of HIV in interpersonal relationships: A sourcebook for researchers and practitioners*. Retrieved from https://books.google.co.uk/books?hl=en&lr=&id=wBWQAgAAQBAJ&oi=fnd&pg=PP1&dq=Privacy+and+Disclosure+of+Hiv+in+Interpersonal+Relationships:+A+&ots=hAgxZkmoBs&sig=7WCFDgmGtvnw8T648nI27RUUkTE

Greene, K., Parrott, R., & Serovich, J. (1993). Privacy, HIV testing, and AIDS: College students' versus parents' perspectives. *Health Communication*. Retrieved from http://www.tandfonline.com/doi/abs/10.1207/s15327027hc0501_4

Hays, R., McKusick, L., Pollack, L., Hilliard, R., Hoff, C., & Coates, T. (1993). Disclosing HIV seropositivity to significant others. *Aids*. Retrieved from http://ovidsp.ovid.com/ovidweb.cgi?T=JS&PAGE=reference&D=emed3&NEWS=N&AN=1993104562

Higgins, E. T. (1987). Self-discrepancy: a theory relating self and affect. *Psychological Review*, *94*(3), 319–340. https://doi.org/10.1037/0033-295X.94.3.319

Holt, R., Court, P., Vedhara, K., Nott, K. H., Holmes, J., & Snow, M. H. (1998). The Role of Disclosure in Coping with HIV Infection. *AIDS Care*, *10*(1), 49–60. https://doi.org/10.1080/09540129850124578

Horvath, K. J., Oakes, J. M., & Rosser, B. R. S. (2008). Sexual negotiation and HIV serodisclosure among men who have sex with men with their online and offline partners. *Journal of Urban Health*, *85*(5), 744–758. https://doi.org/10.1007/s11524-008-9299-2

Joinson, A. (1999). Social desirability, anonymity, and Internet-based questionnaires. *Behavior Research Methods, Instruments, &*. Retrieved from http://link.springer.com/article/10.3758/BF03200723

Joinson, A. N. (2001). Knowing me, knowing you: Reciprocal self-disclosure in Internet-based surveys, *4*(5), 587–591. https://doi.org/10.1089/109493101753235179

Joinson, A. N., & Paine, C. B. (2012). Self-disclosure, Privacy and the Internet. *Oxford Handbook of Internet Psychology*, 1–23. https://doi.org/10.1093/oxfordhb/9780199561803.013.0016

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

Kalichman, S. C., DiMarco, M., Austin, J., Luke, W., & DiFonzo, K. (2003). Stress, social support, and HIV-status disclosure to family and friends among HIV-positive men and women. *Journal of Behavioral Medicine*, *26*(4), 315–332. https://doi.org/10.1023/A:1024252926930

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

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences of the United States of America*, *110*(15), 5802–5. https://doi.org/10.1073/pnas.1218772110

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. https://doi.org/10.1007/s12394-009-0019-1

Leary, M. (1995). Self-presentation: Impression management and interpersonal behavior. Retrieved from http://psycnet.apa.org/psycinfo/1994-98598-000

Leary, M. R., & Schreindorfer, L. S. (1998). The Stigmatization of HIV and AIDS: Rubbing Salt in the Wound. In *HIV AND SOCIAL INTERACTION BT - HIV AND SOCIAL INTERACTION* (pp. 12–29). Retrieved from http://search.proquest.com/docview/60054737?accountid=17215%5Cnhttp://limo.libis.be/resolver?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:book&genre=bookitem&sid=ProQ:Sociological+Abstracts&atitle=The+Stigmatization+of+HIV+and+AIDS%3A+Rubbing+Salt

Liau, A., Millett, G., & Marks, G. (2006). Meta-analytic examination of online sex-seeking and sexual risk behavior among men who have sex with men. *Sexually Transmitted Diseases*, *33*(9), 576–584. https://doi.org/10.1097/01.olq.0000204710.35332.c5

Malheiros, M., Preibusch, S., & Sasse, M. (2013). “Fairly truthful”: The impact of perceived effort, fairness, relevance, and sensitivity on personal data disclosure. *International Conference on Trust*. Retrieved from http://link.springer.com/10.1007/978-3-642-38908-5_19

Mansergh, G., Marks, G., & Simoni, J. M. (1995). Self-disclosure of HIV infection among men who vary in time since seropositive diagnosis and symptomatic status. *AIDS*, *9*(6), 639–644. Retrieved from http://journals.lww.com/aidsonline/abstract/1995/06000/self_disclosure_of_hiv_infection_among_men_who.17.aspx

Manson, H. R. C., Marks, G., Simoni, J. M., Ruiz, M. S., & Richardson, J. L. (1995). Culturally sanctioned secrets? Latino men’s nondisclosure of HIV infection to family, friends, and lovers. *Health Psychology*, *14*(1), 6–12. https://doi.org/http://dx.doi.org/10.1037/0278-6133.14.1.6

Marks, G., Bundek, N. I., Richardson, J. L., Ruiz, M. S., Maldonado, N., & Mason, H. R. C. (1992). Self-Disclosure of Hiv-Infection - Preliminary-Results from a Sample of Hispanic Men. *Health Psychology*, *11*(5), 300–306. Retrieved from http://psycnet.apa.org/journals/hea/11/5/300/

Mcfarlane, M., & Rietmeijer, C. A. (2005). The Internet as a Newly Emerging Risk Environment for Sexually Transmitted Diseases, *284*(4).

Montoya-weiss, M. M., & Massey, A. P. (1998). On-line focus groups : conceptual issues and a research tool, *32*(7), 713–723.

Murphy, P. J., Hevey, D., O'Dea, S., Ni Rathaille, N., & Mulcahy, F. (2015). Serostatus Disclosure, Stigma Resistance, and Identity Management Among HIV-Positive Gay Men in Ireland. *Qualitative Health Research*, 1049732315606687. https://doi.org/10.1177/1049732315606687

NAM. (n.d.). HIV & AIDS Information :: Viral load and the risk of transmission - Expert statements and guidance for individuals. Retrieved March 28, 2017, from http://www.aidsmap.com/Expert-statements-and-guidance-for-individuals/page/1322904/#item1322913

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

O'Brien, M. E., Richardson-Alston, G., Ayoub, M., Magnus, M., Peterman, T. a, & Kissinger, P. (2003). Prevalence and correlates of HIV serostatus disclosure. *Sexually Transmitted Diseases*, *30*(9), 731–735. https://doi.org/10.1097/01.OLQ.0000079049.73800.C2

Omarzu, J. (2000). A disclosure decision model: Determining how and when individuals will self-disclose. *Personality and Social Psychology Review*, *4*(2), 174–185. https://doi.org/10.1207/S15327957PSPR0402_05

Oppenheim, A. (2000). *Questionnaire design, interviewing and attitude measurement*. Retrieved from https://books.google.co.uk/books?hl=en&lr=&id=6V4GnZS7TO4C&oi=fnd&pg=PA5&dq=Questionnaire+design,+interviewing+and+attitude+measure-+ment.+London:&ots=sBL4amULcH&sig=rM6tJTBftbehx6yZDATEofBD9qM

Pennebaker, J. W. (1997). Writing About Emotional Experiences as a Therapeutic Process. *Psychological Science*, *8*(3), 162–166. https://doi.org/10.1111/j.1467-9280.1997.tb00403.x

Posner, R. (1977). Right of privacy, the. *Ga. L. Rev.* Retrieved from http://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/geolr12&section=27

Post, R. (2000). Three concepts of privacy. *Geo. LJ*. Retrieved from http://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/glj89&section=52

Reiman, J. (1995). Driving to the panopticon: A philosophical exploration of the risks to privacy posed by the highway technology of the future. *Santa Clara Computer & High Tech. LJ*. Retrieved from http://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/sccj11&section=14

Schatzow, E., & Herman, J. (1989). Breaking secrecy: Adult survivors disclose to their families. *Psychiatric Clinics of North America*. Retrieved from http://psycnet.apa.org/psycinfo/1990-02159-001

Schau, H. J., & Gilly, M. C. (2003). We are what we post? Self- presentation in personal web space. *Journal of Consumer Research*, *30*(3), 385–404. https://doi.org/10.1086/378616

Serovich, J. M., & Mosack, K. E. (2006). Reasons for Hiv Disclosure or Nondisclosure To Casual Sexual Partners. *Aids*, *15*(1), 70–80.

Simoni, J., Mason, H., Marks, G., Ruiz, M., Richardson, J., & Reed, D. (1995). Women’s Self-Disclosure of HIV Infection: Rates, Reasons, and Reactions. *Journal of Consulting* *and Clinical Psychology*, *63*(3), 474–478. https://doi.org/10.1158/1078-0432.CCR-15-0428.Bioactivity

Smith, J. ., Milberg, S., & Burke, S. (1996). Information privacy: measuring individuals concerns about organizational practices. *MIS Quaterly*, 167–196. Retrieved from http://www.jstor.org/stable/249477

Solove, D. (2007). I've got nothing to hide and other misunderstandings of privacy. *San Diego Law Review*, *44*(4), 745–772.

Stewart, D. W., & Shamdasani, P. (2017). Online Focus Groups. *Journal of Advertising*, *46*(1), 48–60. https://doi.org/10.1080/00913367.2016.1252288

Stirratt, M. J., Remien, R. H., Smith, A., Copeland, O. Q., Dolezal, C., & Krieger, D. (2006). The Role of HIV Serostatus Disclosure in Antiretroviral Medication Adherence, 483–493. https://doi.org/10.1007/s10461-006-9106-6

Strachan, E., Bennett, M., Russo, J., & Roy-Byrne, P. (2007). Disclosure of HIV Status and Sexual Orientation Independently Predicts Increased Absolute CD4 Cell Counts Over Time for Psychiatric Patients. *Psychosomatic Medicine*, *80*, 74–80. https://doi.org/10.1097/01.psy.0000249900.34885.46

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

Suler, J. (2002). Identity management in cyberspace. *Journal of Applied Psychoanalytic Studies*, *4*(4), 445–459. Retrieved from http://www.springerlink.com/index/L322287N68344640.pdf

Suler, J. (2004). The online disinhibition effect. *CyberPsychology & Behavior*, *7*(3), 321–326. https://doi.org/10.1089/1094931041291295

Tates, K., Zwaanswijk, M., Otten, R., van Dulmen, S., Hoogerbrugge, P. M., Kamps, W. A., & Bensing, J. M. (2009). Online focus groups as a tool to collect data in hard-to-include populations: examples from paediatric oncology. *BMC Medical Research Methodology*, *9*, 15. https://doi.org/10.1186/1471-2288-9-15

Trinh, T. T., Yatich, N., Ngomoa, R., Mcgrath, C. J., Richardson, A., Sakr, S. R., … Chung, H. (2016). Partner Disclosure and Early CD4 Response among HIV-Infected Adults Initiating Antiretroviral Treatment in Nairobi Kenya, 1–7. https://doi.org/10.1371/journal.pone.0163594

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

Wheeless, L. (1978). A follow-up study of the relationships among trust, disclosure, and interpersonal solidarity. *Human Communication Research*, *4*(2), 143–157. https://doi.org/10.1111/j.1468-2958.1978.tb00604.x

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. (2007). The effects of self-construal and perceived control on privacy concerns. *ICIS 2007 Proceedings*, 125.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual’s privacy concerns: Toward an integrative view. *ICIS 2008 Proceedings*, 6.

Zea, M. C., Reisen, C. A., Poppen, P. J., Echeverry, J. J., & Bianchi, F. T. (2004). Disclosure of HIV-positive status to Latino gay men's social networks. *American Journal of Community Psychology*, *33*(1–2), 107–116. https://doi.org/10.1023/B:AJCP.0000014322.33616.ae

Mark Warner (ESR12), University College London (UCL)

1 Career Development Plan Year 1

I. Personal and Organizational Information

ESR´s Personal Information			
Name:	**Mark Warner**	**ID number**:	16138629
Office Address:	66-72 Gower Street, London, WC1E 6AA, UK	**Phone**:	+44 (0)20 7679 2000
Mobile:	x	**E-Mail:**	mark.warner@ucl.ac.uk

ESR´s Host Organization Information			
Name:	**University College London**	**Phone**:	+44 (0)20 7679 2000
Address:	66-72 Gower Street, London, WC1E 6AA, UK		
***If enrolled organization is different from host organization, please specify:**			
Name:	**n/a**	**Phone:**	**n/a**
Office Address:	**n/a**		

II. Supervision

Supervision			
Supervisor´s Name:	**Ann Blandford**	**Title**:	Professor
Place of Employment:	University College London	**Phone**:	+44 (0)203 108 7049
Responsibility Distr.:	Primary Supervision	**E-Mail:**	a.blandford@ucl.ac.uk
Co-Supervision			
Co-Supervisor´s Name:	**Joachim Meyer**	**Title**:	Professor
Place of Employment:	Tel Aviv University	**Phone**:	+972 (0)3-6405994
Responsibility Distr.:	Modelling User Behaviour	**E-Mail:**	jmeyer@tau.ac.il
Conduct of Supervision (per activity describe form of supervision and estimated supervision hours)**:**			
Professor Ann Blandford provides me with regularly day-to-day supervision, with structured, weekly one-to-one meetings (1h), complemented with bi-monthly team meeting (2h) with other students and researchers under her guidance. At this stage in my research, supervision from Professor Meyer has consisted of occasional conference call (1h) to discuss user modelling aspects of my work.			

III. Secondment

ESR´s Secondment			
Supervisor's Name:	**Dr Hubert Jäger**	**Position**:	CTO
Organization´s Name:	**UNISCON**	**Phone**:	+49 89 416 159 88 101
Address:	Agnes-Pockels-Bogen 1 80992 München, Germany	**E-mail:**	hubert.jaeger@uniscon.de

IV. Research Project

ESR´s Project			
Title:	**Privacy preserving online identity management through self-disclosure and self-presentation when diagnosed with HIV**	**Ref. No:**	12

Overview and background

When new technologies enter into society and challenge perceptions of privacy, it is often suggested that only those who have something to hide have something to fear (Solove, 2007). However, this idea is based on the premise that people only hide things for nefarious reasons, an idea which will be challenged in this current research. Controlling the disclosure of information about the self provides people with an instrument for presenting themselves to people in different ways, depending on the goals within a given context or interaction. When someone is diagnosed with a sensitive, stigmatising condition such as HIV, it can be challenging to integrate this new aspect of their self into their online lives. Privacy allows people to manage self-disclosure of information so they can develop and manage a plurality of contextually constructed, goal driven identities across different online environments, without fear of damaging the reputations of these identities. This research will conduct a series of qualitative studies to understand the factors that influence the effective management of people's online identities when diagnosed with HIV. Through these studies, a behavioural model will be developed and tested using quantitative methods. The model will provide a better understanding of how people diagnosed with HIV build conviction for the decisions they make when disclosing across different online environments. The model and the research findings from each study can be used to inform designers developing communication technologies intended for people diagnosed with HIV.

References

Solove, D. (2007). I've got nothing to hide and other misunderstandings of privacy. *San Diego Law Review*, *44*(4), 745–772.

V. Long-Term Career Objectives

Long-Term Career Objectives (over five years)

PhD Period

Over the next 3 years, I plan to develop and enhance the skills required for: successful completion of my PhD research, publishing 3-4 high quality academic papers and presenting at 1 – 2 international conferences. I believe that in collaboration with University College London (UCL), the Privacy & Us network will provide me with the support, guidance and training I need to meet these goals.

Post PhD

After completing my PhD, my aim is to develop a career in academia overseas, ideally in SE Asia – an area of the world I enjoy exploring and feel a cultural comfort with. When conducting research, it is important to me that the topic is engaging, and that the outcome has a positive human and social impact, and for this reason I would aim to continue research in privacy and digital health.

As I pursue my career in academia, I aim to develop my skills as a lecturer, learning how to engage affectively with a class to enhance the academic experience of the next generation. To achieve this, I plan to develop novel methods to engage, stimulate and encourage students in their learning. I believe that the strong academic program being delivered through the Privacy & Us project, in partnership with the UCL and its staff will provide me with the foundational expertise, knowledge and experience to meet this objective.

Volunteering and Social Impact Objectives
To maximise the social impact of the opportunities I have been afforded and the skills and knowledge I will obtain, I will volunteer portions of my time to help others, both within my own community, and in other areas of the world. I plan to use my skills as a lecturer through volunteering roles in areas of poverty and reduced opportunity; in support of one of my wife's aspirations to volunteer at a midwife lead charity in Ethiopia.

Alongside my PhD research, I also plan to run for local council in my home town of Colchester in 2018. I have always enjoyed public service, and know that the critical thinking, research rigor and communication and presentation skills this program has, and will continue to provide will enhance my chances of success in this voluntary role.

VI. Short-Term Career Objectives

A. Project Research Results

Project Research Results
Presented according to Privacy & Us project Plan.

Milestones	Expected Results
Literature Review	Reviewing the existing literature to inform future studies and to identify research gaps
Research Proposal	Submit the proposal for my research, providing an overview of the approach, methods and my contribution to the literature
Career Development Plan	Submit a 5-year career development plan to help me identify gaps in knowledge and skills that should be addressed to increase success after my studies have been completed.
Registration VIVA	Prepare my year 1 UCL registration VIVA report.
Study 2 Plan	Develop the plan for my initial study, interviewing sexual health professions in the South East of UK

Deliverables
3.1- Initial formulations of the models and the modelling approaches 4.1-User Interface Requirements 6.7-Research Project Plan and CDP

Anticipated Publications
Journal Article - The Information Society, Findings from an empirical study into the online privacy concerns of online social messaging users

Anticipated Conference/Workshop Attendance & Courses/Seminar Presentations
Data Dialogue: At War with Data – Science Engineering South

B. Training

Research and Technical Training
GDPR – Next Step?, Aug 16 (Karlstad, Sweden via Online Conference Call) Principles of Cognition MSc Module – Dept. Psychology, UCL – Sept 16 – Jan 17 Interaction Science HCI MSc Module – Dept. Computer Science, UCL – Sept 16 – Jan 17 Privacy Enhancing Technologies, Dept. Computer Science, UCL – Jan 17 – Mar 17

Secondment Plan
UNISCON are an agile, innovative start-up, developing novel privacy enhancing cloud based solutions with a predominantly b2b marketing model. Whilst UNISON is a very technically focused company, and my research is situated in understanding of human interactions, I aim to identify areas where my research interests and skills can benefit from, and be a benefit to their work. In doing so, I aim to: - evaluate, identify and develop privacy enhancing technology on PARADISE, as project to manage the health reporting of professional athletes. - develop my Java application development skills within a professional environment - better understand the role of sealed cloud broadly, and to explore its applicability within the healthcare domain - interact and knowledge share with the other hosted ESR's and explore potential future collaboration

Interdisciplinary Training
Values in IT - Privacy's wider context, June 17 (Vienna, Austria) Economics of Privacy, June 17 (Vienna, Austria)

Professional Training
Scientific Paper Writing, Aug 16 (Karlstad, Sweden via Online Conference Call) Professional Networking, Aug 16 (Karlstad, Sweden via Online Conference Call) Peer Review workshop, May 17 (Vienna, Austria)

Other Training Activities
No actives to report

C. *Networking Activities*

KPMG Event - Innovation and Information Protection in Digital Health, Sep 16
Attending weekly HCI workshops/presentations and networking event
Attending weekly InfoSec workshops/presentation and networking event
Data Dialogue: At War with Data after seminar networking event

D. *Research Management*

No actives to report

E. *Other activities*

Other Activities (professional relevant)
No actives to report

VII. Signatures

Date & Signature of fellow

Date & Signature of supervisor

Privacy Preserving Transaction Authentication

Andreas Gutmann (ESR13), VASCO Data Security (VDS)

Abstract. Intangible objects such as software, services, entertainment, and information can be instantly delivered online. They can be purchased in small quantities based per use or per time frame, requiring prompt payment of small amounts of money, called micro-transactions. Fine-grained access patterns, such as the history and other meta data of micro-transactions, have the potential to reveal sensitive information about the purchaser, independent from being a natural person or corporate entity. Especially the observation of the transaction network threatens to reveal such information from multiple entities at the same time. Thus, to protect such information from unauthorised access by third parties, the traffic within the transaction network has to be anonymized. In this project, we aim at developing a brokered system for usable and secure micro-transactions that mitigates the threat of leaking customer's data and involve: (1) high usability and security of the user interface, (2) anonymization of payment meta data on a network level and (3) economic incentives for payment service providers other than transaction fees.

1 Introduction and background

Secure and usable authentication is a cornerstone of system security. It ensures reliability in the authenticity of both users and their actions. Security measures – and authentication in particular – are a mean and not a goal by themselves, and have to accommodate a system's user base. They furthermore have to be appropriate to the threats a system faces – the *threat model*. Online services are by nature confronted with a more diverse thread model than offline services, i.e. they are exposed to more and different threats and attack vectors. Security and usability are indefinitely linked together, with usability being a prerequisite of security. Usability is not to be confused with convenience: A convenient authentication method minimises a user's effort, but to be usable it needs to enable users to make informed decisions, when needed, and be able to act accordingly.

Credentials used for authentication are commonly categorised into three different factors: knowledge based, identity/biometrics based, and possession based. They are also commonly referred to as the *What I know*, *What I am*, and *What I have* principles. The combination of at least two principles is call Strong Customer Authentication (SCA) or Two Factor Authentication (TFA), as opposed to traditional Single Factor Authentication (SFA), which would typically be a password that the user knows.

The overwhelming majority of online services use passwords for SFA. Choosing a new password for every online service places high expectations on those system's users. As a result of this unrealistic burden, users develop coping strategies which enable them to use those systems in the first place, but also introduces new risks related to low complexity, re-used and recorded passwords.

Single Sign On (SSO) services partially address such problems by replacing multiple passwords with a single password, but introduce a new problem of privacy. The SSO service provider gains knowledge of all services a user is making use of, how often they are used, and when. There is a substantial danger to privacy and self-determination of this information being leaked because it could disclose sensitive information about a user.

SFA also suffers from numerous weaknesses that SSO can't address, particularly the vulnerability to malware. Passwords may be compromised by malware on the computer the user enters them on, or malware on the server which verifies the password. In both cases the compromised password could be abused to impersonate the user to the service the password was compromised from, and in the context of SSO or when passwords are being reused, for other services too. For these reasons, single-factor authentication is considered inadequate for high-security applications such as online banking.

To address the weakness of passwords, SCA systems that rely on one-time codes, derived from the users credentials but valid only for one-time use, were developed. They mitigate the risk of password compromise and password reuse, but are still vulnerable to the more sophisticated man-in-the-browser attacker. Here, the service requests one-time authentication credentials before carrying out an action that a criminal has initiated under the disguise the legitimate users. In this attack, victims are tricked (using a combination of malware and social engineering) into entering a valid one-time code because they believe that the service is going to carry out an action that they intend. This results in a (potentially) malicious actions being unintentionally authenticated by legitimate users.

Banks have suffered significant losses from the man-in-the-browser attack, leading to both financial damage and wider social costs. In response, banks are increasingly adopting transaction-authentication systems in which the customer not only authenticates their identity by demonstrating possession of a device, but also demonstrates their intent to authorise a transaction.

Within the European Union, since 2007, banks are regulated by the Payment Services Directive [57]. It regulates what kind of institutions can offer certain payment services, and the rules they have to follow. With the Payment Service Directive 2 (PSD2) [58], the European Parliament adopted a revision of this directive, which will soon be implemented by all EU member states. One of the major changes in PSD2 is the requirement for banks to implement SCA for transactions. Moreover, the authentication codes used must be correlated with the recipient and amount of the transaction, and the customer must be made aware of this. These changes will accelerate the trend in which banks implement SCA in which the customer is aware of the transaction to be executed and that the one-time-password is bound to this transaction.

To comply with PSD2 legal requirements the transaction authentication system must securely communicate the relevant properties of the transaction to the customer. The transaction may only be processed if the customer confirms that the transaction matches his or her intention. This criterion must be met despite attempts at social engineering, and subject to constraints in customer capability (e.g. that authenticating the transaction is not the primary task) and technical limitations (e.g. financial and portability constraints, the display size of the secondary device).

Online payments facilitate electronic commerce (e-commerce), the ability to buy and sell goods and services on the internet. E-commerce has been a driving factor contributing to economic development. Intangible goods (e.g. information) can be delivered in an instant at negligible cost. This facilitates smaller and more frequent purchases.

Instant delivery of intangible goods requires either instant payment or legally enforceable guarantees. Micro-transactions, payments of small amounts of money, are challenging as transaction fees can be uneconomical. Where instant payment is not available or reasonable, personally identifiable information (PII) can be exchanged to guarantee delayed payment. Given the provision of PII, debt can be accumulated until payment becomes reasonable.

To minimise the spread of PII across multiple vendors, brokered systems can be implemented. A payment service provider can guarantee payment to each vendor, while holding the customers PII for legally enforceable guarantees. He collects the total amount of multiple purchases from each of multiple customers, requiring one transaction per customer. He then transfers the total amount of multiple purchases to each vendor, requiring one transaction per vendor. With this or similar approaches, transaction fees become feasible even for smaller and more frequent purchases.

Brokered systems have two drawbacks in terms of privacy: Firstly, similar to SSO session authentication, the transaction service provider learns in addition to his customers PII a lot about their behaviour. Secondly, given the centralist idea behind brokered systems, network surveillance of the payment service provider can leak customer data.

Profiling based on behavioural data is a well known method. It replaces uncertainty from statistical assumptions with fact-based assumptions and allows to draw conclusions about people with higher certainty. This can either be to the advantage or disadvantage for the individual.

Targeted advertisement, for example, makes finding and selling to new and current customers more effective. Consumers are–in best case–made aware of available products to make an informed decision or–in worst case–nudged into buying some products. More recently, this method transferred from economics to politics, advertising or discrediting political views and politicians instead of economic goods and assets. Behavioural profiling can also be used to reveal specific characteristics, personalities, or (political) views of citizens. It could lead to the identification of particularly vulnerable groups, such as political activists or whistleblowers, and their supporters.

Micro-transaction have the potential to reveal very fine-grained and highly sensitive behaviour data. This also applies to meta-data of transaction, e.g. time and recipient of payments. Given the potentially disastrous consequences for vulnerable groups, the protection of such data is of particular importance. This implies the necessity for anonymity on a network level against surveillance.

2 Problem statement

In this project, we aim at developing a brokered system for usable and secure micro-transactions that mitigates the threat of leaking customer's data.

Customers in e-commerce commonly authorise a payment service provider to make a payment, i.e. move money from their account to the vendors'. Security of the involved transaction authentication systems is of high priority. Because it's a human-computer-interface, this entails that ensuring high usability of such a system is vital.

Intangible objects such as software, services, entertainment, and information can be instantly delivered online. They can be purchased in small quantities based per use or per time frame, requiring prompt payment of small amounts of money, called micro-transactions. Fine-grained access patterns, such as the history and other meta data of micro-transactions, have the potential to reveal sensitive information about the purchaser, independent from being a natural person or corporate entity. Especially the observation of the transaction network threatens to reveal such information from multiple entities at the same time. Thus, to protect such information from unauthorised access by third parties, the traffic within the transaction network has to be anonymized.

Payment service providers are usually profit-oriented corporate entities and require transaction fees for their business model. As micro-transactions involve only small amounts of money, such fees can easily become uneconomically high and challenge the economic model. Thus, alternative monetary incentives for payment service providers need to be investigated.

In summary, this project aims to investigate technologies for micro-transaction systems that involve the following challenges:

1. High usability and security of the user interface.

2. Anonymization of payment meta data on a network level.

3. Economic incentives for payment service providers other than transaction fees.

3 Literature reviewed

The problem of integrating authentication into systems and services has long been established [12]. There are numerous challenges, both technical and human, but a long-standing concern is securing authentication between users and verifying systems [38].

Existing authentication solutions are best categorised as being reliant on something the user *is*, *holds* or *knows* [7].

Systems relying on something the user *is* are often favoured from a usability perspective. They make few demands on users as they are not *actual* secrets; the user has nothing to manage or maintain specifically for authentication purposes. Such credentials can not easily be lost, stolen or intentionally shared with others. An individual either explicitly presents some physiological characteristic or implicitly demonstrates some behavioural trait to authenticate [15, 33]. As systems can not rely on secrecy of the biometric features, they must endeavour for difficulty of replication. Successful replication attacks have been presented in the past [40] and countermeasures have been proposed [19]. The sensitivity of biometric data further ensures that implementation is challenging, especially in securing sensors, clients and communication channels [49]. Researchers and practitioners thus favour securing sensors on clients [10] rather than transmitting sensitive material.

Something the user *holds* is favoured as users are required to possess an *secure-by-definition* object to complete the authentication process. It can be referred to as *zero-interaction authentication* [13] or *one-time password authentication*, leveraging personal devices for stronger password authentication from untrusted computers [39]. An individual can use an zero-interaction authenticator, which is a secure storage devices containing a password (e.g. bankcard or smart card), to directly establish a secure channel by divulging the secret [29]. One-time password authenticators either utilise time synchronicity or conduct a challenge-response protocol, which might include the user to execution some physical activity as indicated by the device [43, 47]. Objects are frequently used in SCA with ‘something you know’ (which serves as an authenticator to the device) to mitigate risk of immediate fraudulence upon loss or theft. Additional safeguards are tamper-resistance and content encryption [29].

Something the user *knows* is the most common authentication factor and refers to the verification of a user’s identity by matching one or more pieces of user provided secret knowledge against verification data hold by the authenticating service [9]. The high rate of adoption is due to many reasons including simple implementation requirements, low cost of deployment and administration [44], and a high level of user acceptance. Alphanumeric passwords are the most common authentication method [5], although the practical security can be questioned [4]. Personal identification numbers (PINs) are especially common for banking systems [31, 32] and their security properties are questionable as well [6].

Single-factor authentication is especially prone to theft of credentials. For knowledge-based credentials, limited- or partial-disclosure ensures that single observations won’t reveal full credentials [50]. This is often used in telephone banking [2]. If biometric credentials are disclosed to an untrusted computer once, they are no longer reliable and cannot be trusted by any device [11] in the future. Methods to prevent this have since been developed [10].

Untrusted devices remain one of the most challenging attack vector for the implementation of secure authentication. Especially troublesome is the Man-in-the-Browser (MitB) attack, first described by Paes de Barros [3] in 2005. It is a Man-in-the-Middle attack between the user and the security mechanisms in the browser, effectively breaking the WYISWYG (what you see is what you get) concept of browsers. This attack can, for example, steal data, modify HTML, modify outgoing data, and intercept autonomous communication [22]. No traditional authentication method (PIN, TAN, iTAN, Client certificates, Secure-ID, SmartCards, Class3 Readers, OTP, ...) is able to prevent this attack because it works on the transaction, rather than session, level [30]. Server-side fraud detection systems are hampered to detect it, too, because, from the server's perspective, the observed activities come from an authenticated user on the same computer and Internet connection as usual [16]. Several Trojan bot-nets (e.g. URLzone/Bebloh, Torpig/Sinowal, and Zeus/Zbot/Kneber) use this attack method to target online banking to steal money from their victims bank accounts [22].

To protect against MitB attacks, transaction authentication is required [54]. This is the process of authenticating users on a transaction level rather than a session level, although both procedure are commonly combined [21]. Only if it utilises a second channel, e.g. an independent device, to enable the customer to verify that the details of a transaction are correct, including, for example, the destination account number and amount of payment, this attack can be prevented [16].

A number of authors have been concerned with transaction authenticators, dedicated devices for the purpose of transaction authentication, in online banking. They focused on the impact of design decision for transaction authenticators and their integration into people's life, but neglected to investigate the actual user base and their mental models. Jøsang *et al.* [34] suggest general usable security principles and conclude with recommendations for the design of transaction authenticators. Kiljan *et al.* [36] adopt a web authentication scheme by Renaud [48] and conducted an expert evaluation of general transaction authentication systems. The highest overall rating received the system type with keypad, display, camera and smart card slot, that is not connected to user's computer. De Cristofaro *et al.* [18] found that ease of use, cognitive effort, and trustworthiness suffice as measurements to evaluate the usability of transaction authenticators. Weir *et al.* [59] found that transaction authenticators using a customer's banking card and PIN were not intuitive to use, but after learning it once the number of erros in usage was significantly reduced. The importance of familiarity with and its impact on perceived usability of such devices was confirmed in a second study [60]. Krol *et al.* [37] explored how transaction authenticators integrate into everyday life, and reported on several usability issues.

Only little research has been concerned whether the design of currently used transaction authenticators provides sufficient protection against MitB attacks. AlZomai *et al.* [1] investigated whether participants in a study noticed a MitB attack in a simulation with an adopted transaction authentication system, in which verification data was sent to participants by email, and found that the amount of changes in transaction data was correlated with detection rate. The study design limits the transferability of results to online banking transaction authentication due to several factors, e.g. participant selection and recruitment, potential participant priming, significant changes to the authentication procedure, and no realistic scenario/threat.

Microtransactions are payments involving only small amount of money. They are envisioned as future in electronic commerce since the late 90s to pay for intangible goods delivered online, such as information on websites per view or usage of (rented) software per hour [61]. One of the main issues holding microtransactions back is that of transactions fees: to be economical, they can only be a small fraction of the actual value of a product or service. Factors influencing transaction fees are, for example, technical cost, storage cost, computational cost, communication cost, administrative cost, and payment service provider margin [42].

Different sources of financial incentives are a topic of active investigation in literature, e.g. by Chaffey [8, p.63 ff.]. Especially the use of and benefit from customer data is central in e-commerce. Ensuring customer loyalty is among the highest priorities [46]. Traditionally, customer data facilitated selling of products, serving to inform the vendor whom to sell which product at which price [52]. Recent research developments focus on a shift towards use for customer value creation, especially for service-based business models, with the goal of facilitating customer loyalty [51]. The act of payment is only a small part of the customer life-cycle with a service provider, although the most important one [56].

Transaction service providers gain a lot of knowledge about their customers payment behaviour with different vendors. Privacy-preserving data analysis and statistics techniques could enable them to capitalise on this knowledge. Many systems have been developed that report statistics by trading utility of data for privacy of data owners (e.g. [26, 27]. These systems provide privacy guarantees based on the concept of Differential Privacy [23]. Other systems (e.g. [14,25,35,41,45,55]) provide cryptographic privacy guarantees.

In addition to authentication, any secure system for electronic payments and e-commerce, including microtransactions, must also address the issue of 'privacy of payment data and confidentiality of order information transmission' [28]. In times of mass surveillance, privacy and confidentiality of data transmission requires anonymous communication tools, which provide users with good, although not perfect, anonymity on the internet [17]. Transaction authentication, in general, refers to real-time applications and, thus, requires low-latency systems [24], such as Tor [20]. Tor, short for 'The onion router', as well as other anonymous communication tools, relies on mix network technology. Mix networks have been subject to scrutinised research and many variations exist. The work of Edman and Yener [24] and Sampigethaya and Poovendran [53], for example, provide an overview.

4 Proposed approach and contribution

Our approach to contribute a usable, secure, and economically reasonable micro-payment systems, which respect the customers privacy, is threefold: (1) A usable and secure user interface for transaction authentication; (2) A payment processing system that minimises data leakage on the network level; (3) Alternatives to transaction fees as economic incentives for payment service providers that respect customers' privacy.

Transaction authentication. The user interface of any transaction authentication system in Europe will have to satisfy PSD2 requirements. This means SCA with single-use authentication codes correlated to the recipient and transaction amount. Furthermore, the salient properties of each transaction shall be communicated to and verified by the legitimate customer in a usable and secure manner.

Following a user-centred approach, we will investigate user's mental models of transaction authenticators, which are commonly used to authenticate transactions in online banking, and evaluate whether they communicate each transaction's salient properties to the customer sufficiently well. If required, we will suggest improvements based on our gained insights.

The anticipated result is a choice of transaction authenticators suitable for our purposes. This addresses the first challenge in our problem statement in Sect. 2.

Network anonymisation. To protect customer privacy, the payment system anonymize transactions on a network level, while ensuring sufficient throughput and minimising latency.

We will evaluate existing network anonymisation PETs for their suitability for our project. For this purpose we will take multiple medium- and low-latency mix-net based networks into consideration.

The anticipated result is a choice of anonymisation networks suitable for our purposes. This addresses the second challenge in our problem statement in Sect. 2.

Economic incentives. For-profit payment service providers currently require transaction fees as economic incentive to provide their service. These can be a significant barrier for the adoption of micro-payment systems.

We will investigate options for payment service providers to commercialise statistical knowledge about their customers without infringing their privacy. Therefore, we will compare privacy-preserving data aggregation and statistics methods on this use-case.

The anticipated result is a privacy-preserving economic incentive other than high transaction fees for payment service providers.This addresses the third challenge in our problem statement in Sect. 2.

5 Research methodology and work plan

5.1 Transaction authentication

A literature review of previous research on usable security of transaction authenticators was conducted to uncover knowledge gaps. It has revealed the following relevant items:

- Little research was published on investigating/understanding the relevant user base. Who are archetypal users or personas of transaction authenticators and what is their mental model regarding transaction authenticators?
- Do transaction authenticators communicate the salient properties of each transaction to the customer sufficiently well? Do customers verify this data before authenticating a transaction and would they spot discrepancies?

User studies with current users of transaction authenticators in online banking are planned to investigate the aforementioned questions. Using questionnaires we want to collect demographics and personality data to better understand the relevant user base and during interviews we want to uncover our participants mental model of using transaction authenticators in online banking. In a laboratory study we want to assess in a realistic scenario whether our participants verify the transaction data communicated to them by transaction authenticators.

Results from our study can then be used to construct skeletons of personas and sketches of participants' mental models. The results might possibly uncover a correlation between certain personas and the verification of transaction data.

Validation of our results will depend on our findings. We could, for example, verify our insights quantitatively using surveys or triangulate them qualitatively by interviewing people who work in a bank's customer support.

5.2 Network anonymisation

A literature review of anonymisation networks has to be completed. Thereby focus on implemented low or medium latency networks is preferable. This will inform us of suitable candidates for our artefact.

Criteria and scenarios for an evaluation of the considered networks have to be defined. These could include security threat model, privacy/anonymity guarantees, latency, throughput, scalability, and efficiency.

Evaluation of the considered networks will be required to select a candidate. An evaluation can be purely theoretic, e.g. if suitable data and statistics from a current implementation are available, or require a simulation.

5.3 Evaluation of artefact

A prototype of the artefact should be developed. It can either be low fidelity or high fidelity, depending on the previous results.

The evaluation of the prototype should be done in a user study. Study design and evaluation criteria will depend on previous results in Sect. 5.1. Depending on previous results in Sect. 5.2, an in-depth analysis of security and privacy guarantees might be necessary or not.

5.4 Economic incentives

A literature review of privacy-preserving data aggregation and statistic techniques will provide us with a set of candidate technologies.

Evaluation of candidate technologies will take privacy guarantees for users' data, efficiency of the calculations, and utility of the resulting data points into account.

References

[1] AlZomai, Mohammed, AlFayyadh, Bander, J{\o}sang, Audun, McCullagh, Adrian: An Experimental Investigation of the Usability of Transaction Authorization in Online Bank Security Systems. Proceedings of the Sixth Australasian Conference on Information Security 81(1), 65–73 (2008)

[2] Aspinall, D., Just, M.: “Give Me Letters 2, 3 and 6!”: Partial Password Implementations and Attacks. In: Financial Cryptography and Data Security, pp. 126–143. Springer (2013)

[3] Paes de Barros, A.: O futuro dos backdoors, o prior dos mundos (2005), https://web.archive.org/web/20110706153819/http://www.paesdebarros.com.br/backdoors.pdf

[4] Bonneau, J.: The science of guessing: analyzing an anonymized corpus of 70 million passwords. In: Security and Privacy (SP), 2012 IEEE Symposium on. pp. 538–552. IEEE (2012)

[5] Bonneau, J., Herley, C., Van Oorschot, P.C., Stajano, F.: The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In: Security and Privacy (SP), 2012 IEEE Symposium on. pp. 553–567. IEEE (2012)

[6] Bonneau, J., Preibusch, S., Anderson, R.: A birthday present every eleven wallets? The security of customer-chosen banking PINs. In: Financial Cryptography and Data Security, pp. 25–40. Springer (2012)

[7] Brainard, J., Juels, A., Rivest, R.L., Szydlo, M., Yung, M.: Fourth-factor authentication: somebody you know. In: Proceedings of the 13th ACM conference on Computer and communications security. pp. 168–178. ACM (2006)

[8] Chaffey, D.: E-business and E-commerce Management: Strategy, Implementation and Practice. Pearson Education (2007)

[9] Chen, Y., Liginlal, D.: A maximum entropy approach to feature selection in knowledge-based authentication. Decision support systems 46(1), 388–398 (2008)

[10] Chung, Y., Moon, D., Kim, T., Pan, S.B.: A secure fingerprint authentication system on an untrusted computing environment. Lecture notes in computer science 3592, 299 (2005)

[11] Clarke, D., Gassend, B., Kotwal, T., Burnside, M., Van Dijk, M., Devadas, S., Rivest, R.: The untrusted computer problem and camera-based authentication. In: Pervasive computing, pp. 114–124. Springer (2002)

[12] Corbató, F.J.: On building systems that will fail. Communication of the ACM 34(9), 72–81 (1991)

[13] Corner, M.D., Noble, B.D.: Zero-interaction authentication. In: Proceedings of the 8th annual international conference on Mobile computing and networking. pp. 1–11. ACM (2002)

[14] Corrigan-Gibbs, H., Boneh, A.: Prio: Private, robust, and scalable computation of aggregate statistics. In: 14th USENIX Symposium on Networked Systems Design and Implementation (NSDI 17). pp. 259–282. USENIX Association (2017)

[15] Crawford, H.: Keystroke dynamics: Characteristics and opportunities. In: Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on. pp. 205–212. IEEE (2010)

[16] Cronto Limited: Beyond Phishing - De-mystifying the Growing Threat of Internet Banking Fraud. Tech. rep. (2008), https://www.cronto.com/internet_banking_fraud_beyond_phishing.htm

[17] Danezis, G., Wittneben, B.: The economics of mass surveillance-and the questionable value of anonymous communications. In: In Proceedings of the 5th Workshop on The Economics of Information Security (WEIS 2006. Citeseer (2006)

[18] De Cristofaro, E., Du, H., Freudiger, J., Norcie, G.: A Comparative Usability Study of Two-Factor Authentication. In: Proceedings of 2014 Workshop on Usable Security (USEC). Internet Society (2014)

[19] Derakhshani, R., Schuckers, S.A., Hornak, L.A., O'Gorman, L.: Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners. Pattern recognition 36(2), 383–396 (2003)

[20] Dingledine, R., Mathewson, N., Syverson, P.: Tor: The second-generation onion router. Tech. rep., DTIC Document (2004)

[21] Dmitrienko, A., Liebchen, C., Rossow, C., Sadeghi, A.R.: On the (In)Security of Mobile Two-Factor Authentication. In: Financial Cryptography and Data Security, pp. 365–383. No. 8437 in Lecture Notes in Computer Science, Springer (2014)

[22] Dougan, T., Curran, K.: Man in the Browser Attacks. International Journal of Ambient Computing and Intelligence 4(1), 29–39 (2012)

[23] Dwork, C., Roth, A., et al.: The algorithmic foundations of differential privacy. Foundations and Trends® in Theoretical Computer Science 9(3–4), 211–407 (2014)

[24] Edman, M., Yener, B.: On anonymity in an electronic society: A survey of anonymous communication systems. ACM Computing Surveys (CSUR) 42(1), 5 (2009)

[25] Elahi, T., Danezis, G., Goldberg, I.: Privex: Private collection of traffic statistics for anonymous communication networks. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. pp. 1068–1079. ACM (2014)

[26] Erlingsson, Ú., Pihur, V., Korolova, A.: Rappor: Randomized aggregatable privacy-preserving ordinal response. In: Proceedings of the 2014 ACM SIGSAC conference on computer and communications security. pp. 1054–1067. ACM (2014)

[27] Fanti, G., Pihur, V., Erlingsson, Ú.: Building a rappor with the unknown: Privacy-preserving learning of associations and data dictionaries. Proceedings on Privacy Enhancing Technologies 2016(3), 41–61 (2016)

[28] Furnell, S.M., Karweni, T.: Security implications of electronic commerce: a survey of consumers and businesses. Internet research 9(5), 372–382 (1999)

[29] Gorman, L.O.: Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE 91(12), 2021–2040 (2003)

[30] Gühring, Philipp: Concepts against Man-in-the-Browser Attacks (2006), http://www.cacert.at/svn/sourcerer/CAcert/SecureClient.pdf

[31] Gutmann, A., Volkamer, M., Renaud, K.: Memorable and secure: How do you choose your pin? In: Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016). p. 156 (2016)

[32] Gutmann, A., Renaud, K., Volkamer, M.: Nudging bank account holders towards more secure pin management. In: International Journal of Internet Technology and Secured Transactions. vol. 4, pp. 380–386. Infonomics Society (2015)

[33] Jain, A., Bolle, R., Pankanti, S.: Biometrics: personal identification in networked society, vol. 479. Springer Science & Business Media (2006)

[34] Jøsang, Audun, Zomai, Muhammed Al, Suriadi, Suriadi: Usability and privacy in identity management architectures. Proceedings of the fifth Australasian symposium on ACSW frontiers 68, 143–152 (2007)

[35] Joye, M., Libert, B.: A scalable scheme for privacy-preserving aggregation of time-series data. In: International Conference on Financial Cryptography and Data Security. pp. 111–125. Springer (2013)

[36] Kiljan, S., Vranken, H., van Eekelen, M.: Evaluation of transaction authentication methods for online banking. Future Generation Computer Systems (2016)

[37] Krol, K., Philippou, E., De Cristofaro, E., Sasse, M.A.: "They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking. In: Proceedings of 2015 Workshop on Usable Security (USEC). Internet Society (2015)

[38] Lamport, L.: Password authentication with insecure communication. Communications of the ACM 24(11), 770–772 (1981)

[39] Mannan, M., van Oorschot, P.C.: Leveraging personal devices for stronger password authentication from untrusted computers. Journal of Computer Security 19(4), 703–750 (2011)

[40] Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S.: Impact of artificial gummy fingers on fingerprint systems. In: Electronic Imaging 2002. pp. 275–289. International Society for Optics and Photonics (2002)

[41] Melis, L., Danezis, G., De Cristofaro, E.: Efficient private statistics with succinct sketches. In: Annual Network & Distributed System Security Symposium (NDSS). Internet Society (2016)

[42] Papaefstathiou, I., Manifavas, C.: Evaluation of micropayment transaction costs. Journal of Electronic Commerce Research 5(2), 99–113 (2004)

[43] Patel, S.N., Pierce, J.S., Abowd, G.D.: A gesture-based authentication scheme for untrusted public terminals. In: Proceedings of the 17th annual ACM symposium on User interface software and technology. pp. 157–160. ACM (2004)

[44] Piper, F.C., Robshaw, M.J., Schwiderski-Grosche, S.: Identities and authentication. Foresight Directorate (2004)

[45] Popa, R.A., Balakrishnan, H., Blumberg, A.J.: Vpriv: Protecting privacy in location-based vehicular services. In: USENIX security symposium. pp. 335–350 (2009)

[46] Reichheld, F.F., Schefter, P.: E-loyalty: your secret weapon on the web. Harvard business review 78(4), 105–113 (2000)

[47] Rekimoto, J., Ayatsuka, Y., Kohno, M.: Synctap: An interaction technique for mobile networking. In: Human-Computer Interaction with Mobile Devices and Services, pp. 104–115. Springer (2003)

[48] Renaud, K.: Quantifying the quality of web authentication mechanisms: a usability perspective. Journal of Web Engineering 3(2), 95–123 (2004)

[49] Renaud, K., Hoskins, A., von Solms, R.: Biometric identification: Are we ethically ready? In: Information Security South Africa. Johannesburg, South Africa (2015)

[50] Renaud, K.: Guidelines for designing graphical authentication mechanism interfaces. International Journal of Information and Computer Security 3(1), 60–85 (2009)

[51] Saarijärvi, H., Grönroos, C., Kuusela, H.: Reverse use of customer data: implications for service-based business models. Journal of Services Marketing 28(7), 529–537 (2014)

[52] Saarijärvi, H., Karjaluoto, H., Kuusela, H.: Customer relationship management: the evolving role of customer data. Marketing intelligence & planning 31(6), 584–600 (2013)

[53] Sampigethaya, K., Poovendran, R.: A survey on mix networks and their secure applications. Proceedings of the IEEE 94(12), 2142–2181 (2006)

[54] Schneier, B.: Two-factor authentication: too little, too late. Communications of the ACM 48(4), 136 (Apr 2005)

[55] Shi, E., Chan, H., Rieffel, E., Chow, R., Song, D.: Privacy-preserving aggregation of time-series data. In: Annual Network & Distributed System Security Symposium (NDSS). Internet Society (2011)

[56] Spiess, J., T'Joens, Y., Dragnea, R., Spencer, P., Philippart, L.: Using big data to improve customer experience and business performance. Bell Labs Technical Journal 18(4), 3–17 (2014)

[57] The European Parliament and the Council of the European Union: Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC. Official Journal of the European Union, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:0036:en:PDF

[58] The European Parliament and the Council of the European Union: Directive 2015/2366/EUof the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. Official Journal of the European Union, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN

[59] Weir, C.S., Douglas, G., Carruthers, M., Jack, M.: User perceptions of security, convenience and usability for ebanking authentication tokens. Computers & Security 28(1-2), 47–62 (2009)

[60] Weir, C.S., Douglas, G., Richardson, T., Jack, M.: Usable security: User preferences for authentication methods in eBanking and the effects of experience. Interacting with Computers 22(3), 153–164 (2010)

[61] Westland, J.C., Clark, T.H., et al.: Global electronic commerce: Theory and case studies. MIT Press Books 1 (1999)

Andreas Gutmann (ESR13), VASCO Data Security Innovation Centre (VDS)

1 Career Development Plan Year 1

Target audience and use of this document: The Career Development Plan is intended to be a document to guide the ESR and the supervisors as and where applicable the direct superior at the hiring institution with the procurement of the Marie Curie programme. It contains a series of personal information of the ESR and should be treated as confidential. Where necessary the document may be made available to the project leader, the management board or a designated group of persons for the purposes of mediation or dispute resolution. Where necessary and specifically asked for the document may be made available to the European Commission or the reviewers appointed by the EC for purposes of the evaluation of the project and other purposes specified in the programme's funding regulations.

I. *Personal and Organizational Information*

ESR´s Personal Information			
Name:	**Andreas Gutmann**	**ID number**:	UPI: AFBGU06
Office Address:	Cronto Limited, VASCO Innovation Centre, Hauser Forum, 21 JJ Thompson Avenue, Cambridge, CB3 0FA, United Kingdom	**Phone**:	
Mobile:		**E-Mail:**	andreas.gutmann@vasco.com

ESR´s Host Organization Information			
Name:	**Cronto Limited, subsidiary of VASCO**	**Phone**:	
Address:	Cronto Limited, VASCO Data Security Innovation Centre, Hauser Forum, 21 JJ Thompson Avenue, Cambridge, CB3 0FA, United Kingdom		
***If enrolled organization is different from host organization, please specify:**			
Name:	**University College London**	**Phone:**	
Office Address:			

II. *Supervision*

Supervision			
Supervisor´s Name:	**Steven J. Murdoch**	**Title**:	Dr.
Place of Employment:	VASCO / University College London	**Phone**:	
Responsibility Distr.:		**E-Mail:**	steven.murdoch@vasco.com
Co-Supervision			
Co-Supervisor´s Name:	**Jetzabel Serna-Olvera**	**Title**:	Dr.
Place of Employment:	Goethe University Frankfurt	**Phone**:	
Responsibility Distr.:		**E-Mail:**	jetzabel.serna@m-chair.de
Conduct of Supervision (per activity describe form of supervision and estimated supervision hours)**:**			

Weekly meetings with Steven Murdoch; ~1 hour per week. Additional online communication (e.g. email); time can't be estimated.

III. Secondment

ESR´s Secondment			
Supervisor's Name:	**Michael Bechinie**	**Position**:	Head of Experience Design
Organization´s Name:	**USECON GmbH**	**Phone**:	
Address:	Modecenterstraße 17, 1110 Vienna, Austria	**E-mail:**	bechinie@usecon.com

IV. Research Project

ESR´s Project			
Title:	**Privacy-preserving transaction authentication on mobile devices**	**Ref. No:**	13
Overview and background			

Secure authentication is one of the key requirements for allowing the use of online services. The predominant method of username and password fails to offer usability because the requirements put on users: of choosing a different complex password for every online service and not writing any down. Username and passwords also fail to provide adequate security for today's computing environment: malware on users' computers can harvest passwords and security breaches of servers reveal large databases of usernames and passwords likely shared over different websites. Single Sign On (SSO) services partially address these problems by replacing multiple passwords with a single password, but introduce a new problem of privacy. The SSO service operator gains knowledge of all services a user is making use of, how often they are used, and when. There is a substantial danger to privacy and self-determination of this information being leaked because it could disclose sensitive information about a user such as their health in the context of e-healthcare scenario.

SSO solutions have also not adapted to the new class of malware attacks – "man-in-the-browser" seen against online banking applications but likely to be extended to online services. These malware attacks do not merely record passwords, but misrepresent a user's intentions to the online service. In the case of online banking this is usually for the goal of moving a user's money to a criminal, but with a SSO service the malware could force a user to log into a service they did not wish to, or to reveal information which they have not consented to have revealed. Traditional authentication solutions such as one-time-passwords do not address this problem.

This project will design and evaluate new approaches for authentication, addressing the limitations of existing SSO systems. Firstly, unlinkable and anonymous credentials shall be used so that a SSO service provider is unable to discover the identity of the user they are providing authentication services to. This is achieved by ensuring that each authentication protocol run is unlinkable to the SSO service, but obviously not to the online service which needs to perform the authentication. Secondly protocols will be developed to prevent a network-based adversary being able to establish the identity of the user by observing or interfering with an authentication protocol exchange. This will prevent the attacker from being able to use targeted malware attacks against certain users. Thirdly, SSO protocols will be extended to provide not just protection of log-in information, but also transaction information so as to defend against man-in-the-browser attacks. To achieve these goals, it will be necessary that users are provided with a secure and usable mobile authentication device.

V. Long-Term Career Objectives

Long-Term Career Objectives (over five years)
Being a researcher on privacy-preserving and usable security technologies. **Contributing to the general understanding of psychological, social, ergonomic, and economic factors influencing user's adoption of, use of, and general behaviour with privacy-preserving and usable security technologies, as well as developing new methods/tools, or improving existing ones, to mitigate negative effects on the aforementioned.** **Identifying societal problems and challenges that require the application new privacy-preserving and usable security technologies. Contribute to the creation of solutions that address the aforementioned problems.** **The ability to conduct interdisciplinary research as well as networking with researchers in various disciplines will be beneficial to accomplishing this goal. I will improve my skill related to interdisciplinary research during my PhD by working at the intersection of privacy, security, and usability. By attending workshops and conferences I will furthermore be able to create a network of contacts in various disciplines.**

VI. Short-Term Career Objectives

A. Project Research Results

Project Research Results
Presented according to Privacy & Us project Plan.

Milestones	Expected Results
Literature review	General authentication and transaction authentication literature; usable security literature; mix net and Tor literature; Differential Privacy literature; general PETs literature
Programming (Twisted)	Improve understanding of event-driven network programming language Twisted
Transaction authenticator study	Prepare usable security evaluation study of transaction authenticators and get ethical approval for it
Career development plan and Research Project Plan	Contribution to D6.7
User interface and artefact requirement analysis	Contribution to D2.1 & D4.1

Deliverables
D2.1 **D4.1** **D6.7**

Anticipated Publications

Anticipated Conference/Workshop Attendance & Courses/Seminar Presentations

- *New developments in data privacy workshop at University of Cambridge*
- *New approaches to anonymization workshop at University of Cambridge*
- *Engaging people in data privacy workshop at University of Cambridge*
- *Privacy: recent developments at the interface between economics and computer science at University of Cambridge*
- *IFIP Summer School 2016 at Karlstad University*

B. Training

Research and Technical Training

- **Distributed systems security reading group held by Alastair Beresford at the University of Cambridge Computer Laboratory.**
- **Distinguished seminar series of the Academic Centre of Excellence in Cyber Security Research at University College London.**
- **Introduction to PETs at 1st Privacy&Us Training Event**
- **Introduction to Usability at 1st Privacy&Us Training Event**
- **Privacy Enhancing Technologies Online Module at University College London**
- **Ethics, Equality and Diversity for University Researchers as part of the Doctoral Skills Development Programme at University College London**

Secondment Plan
Review of existing transaction authentication systems and attacks on them **Design a study of ethical and feasible user study for usable security evaluation of transaction authentication systems**

Interdisciplinary Training
• **Privacy of Personal Health Data at 1st Privacy&Us Training Event** • **General Data Protection Regulation – Next Step? at 1st Privacy&Us Training Event** • **Legal Privacy Workshop – Privacy by Design at 1st Privacy&Us Training Event** • **Data Protection by Design and Default at 1st Privacy&Us Training Event** • **The Future of Privacy and Identity Management at 1st Privacy&Us Training Event**

Professional Training
• **Self-management** • **Professional Networking at 1st Privacy&Us Training Event** • **Scientific Paper Writing at 1st Privacy&Us Training Event**

Other Training Activities

C. *Networking Activities*

- **Privacy&Us training event in Karlstad, Sweden**
- **IFIP Summer School 2016 at Karlstad University**
- **New developments in data privacy workshop at University of Cambridge**
- **New approaches to anonymization workshop at University of Cambridge**
- **Engaging people in data privacy workshop at University of Cambridge**
- **Privacy: recent developments at the interface between economics and computer science at University of Cambridge**

D. *Research Management*

E. Other activities

Other Activities (professional relevant)
Contributed as reviewer to international conferences such as the ACM SIGCHI (Special Interest Group on Computer-Human Interaction) flagship conference CHI (Human Factors in Computing Systems) **Contributed as reviewer to international journals such as the Elsevier International Journal of Human-Computer Studies**

VII. Signatures

Date & Signature of fellow

Date & Signature of supervisor

Appendix – Structures of the Research Project Plans and Career Development Plans

1 Structure of the Research Project Plan

The purpose of the research project plan is to provide an overview of the research project. This plan will be developed individually by each ESR, and must be submitted by M18. The research project plan should be presented orally to an evaluation committee comprising of supervisor, co-supervisor, and secondment's host representatives, and it should serve as a roadmap and timeline in the development of the ESR's research project during the 3-year training programme. The research project plan should therefore, include an extensive review of the literature, a research statement, the proposed approach and a detailed work plan specifically highlighting the different stages of research and the research methodologies to be applied at each stage.

a) Preliminary title

A "preliminary title" that summarizes the main idea or ideas of the research study should be developed early in the research process, as it will function as an anchor to focus the study.

b) Abstract

An abstract is a short summary of the research project plan manuscript.

c) Introduction / Motivation

The introduction gives an overview of the research project. It describes the background of the research project and briefly introduces the main issues justifying why those issues are worth attention in research. The introduction should include a concise presentation of the research question or statement, which should capture both the essence of the project and its delimiting boundaries. This should be followed by a clarification of the extent to which the outcomes will advance the state of the art of a specific domain.

d) Background

Background information expands upon the key points stated in the introduction but should not be the main focus of the report. Background information should support the reader to determine if there exists a basic understanding of the research problem being investigated, in other words, this information will provide the reader with the essential context needed to understand the research problem and its significance. In some areas of research, the background information can also include summaries of relevant research studies.

e) State of the art

The state of the art also known as literature review should be the more extensive part of the research project proposal. It should demonstrate a solid knowledge of the field and familiarity with the main issues at stake. It should show that key literature has been critically identified and evaluated while creating an innovative and coherent view that in turn will integrate and synthetize the main aspects of the field, in a way that a new perspective and research direction is proposed. The state of the art gives credit to the authors who laid the groundwork for the research project, so that the reader is able to recognise that the research project will likely make a significant contribution to the literature.

f) Proposed approach

This section is the core of the project and the primary concern of the evaluation committee. The proposed approach should be introduced as a high level description of the proposed 'solution' (e.g., framework, architecture, protocol, etc.) that will address the identified challenges and therefore, fill a research gap.

g) Research methodology

It is important to determine which research methodologies will be adopted in order to achieve the research goals. The research methodology should include the main research steps, which may go from the literature review to the validation of the proposed approach and the different research methods to be adopted e.g., qualitative or quantitative approach to your research, or both.

h) Work plan – general description of the main phases and activities until the end of the thesis including a time plan

Not all research proposals lend themselves to the creation of detailed work plans. However, it is desirable and valuable, to establish specific milestones and timelines for the project. The plan should anticipate the problems likely to be found along the way and describe the approaches to be followed in solving them. It should also anticipate the conferences and journals to which the work in progress is expected to be submitted and schedule them into the work plan. Keeping a work plan maintains the ESRs focus and motivation. The research work plan should be able to put in perspective the implications of the successive steps of the research work, reinforcing the conviction that the approach is solidly oriented towards results; moreover, that the topic is timely and relevant, and that the outcomes of the project will contribute significantly to the enhancement of the field.

i) References

This section should list all the references of cited work throughout the research proposal. It should comply with the referencing conventions or citation styles that have been established for your specific field.

j) Appendix (e.g. publications)

The appendix should include information that is not essential to explain the research findings in the report but that it may support your analysis and validate your conclusions.

2 Structure of the Career Development Plan

Each ESR will be enrolled in a postgraduate (PhD) program at their supervisor's host institution. ESRs together with their primary supervisor and co-supervisor will design/develop a personalised career development plan. The purpose of the career development plan is to provide guidance to the ESR on their chosen research topic, to facilitate the monitoring of their progress and to enable the early detection of potential issues that may hamper the overall progress of the research project. The CDP should include an individual training plan specifically tailored to the career development needs of the ESR and the individual training needed for the successful development of the research project for the forthcoming 12 months.

2.1 ESR's Organization and Personal Information

- ESR's host organization information containing: organization's name, address, and telephone.
- ESR's personal information containing: name, Student ID number, Office address, Phone, E-Mail
- *If the enrolled organization is different than the host organization,* include: name of the institution, department, address, and telephone.

2.2 Supervision and Co-Supervision

- Name and affiliations of supervisor and co-supervisor
- Distribution of supervisor responsibility between the main supervisor and co-supervisor
- Conduct of supervision: Describe all supervision activities planned for the coming 12th month period including the form of supervision and the number of meetings and estimated supervision hours.
- Secondment supervision include: name of supervisor, title, place of employment, e-mail.

2.3 ESR Project

- Reference (number) and title of the research project
- Overview of the research project

2.4 Long-term career objectives (over 5 years)

This section will describe the ESR’s individual long-term career goals and the steps needed to achieve those goals. Through a self-assessment the ESR should/will be able to identify the research, training and networking activities needed to support the achievement of her/his long-term career objectives taking into consideration her/his career path beyond the PhD studies. Supervisor and co-supervisor will inform ESRs about the opportunities and how could they be prepared for many variants.

a) Goals
b) What further research activity or other training is needed to attain these goals?

2.5 Short-term career objectives

This section will describe all activities needed to support the short-term career objectives; specifically this part will include the list of planned activities for the upcoming period.

a) Goals
b) What further research activity or other training is needed to attain these goals?

2.5.1 Project research results and milestones

Project intermediate results should be reported according to the milestones defined in the Privacy & Us project plan. ESRs will provide the information regarding the milestones for the coming 12 month period focusing on those that are directly associated to the ESR’s individual research project. The means by which the results are expected to be disseminated should also be included.

- Milestones and associated expected results
- List of deliverables (reference, title, expected contribution indicating its relation to the individual research project)
- Anticipated publications (conference title, scope of the conference, date, relevance to the project, ranking, etc.)
- Anticipated conference / workshop attendance, courses, and /or seminar presentations

2.5.2 Individual Training

This section will include the information corresponding to the planned research and technical training (list of training modules) and secondments (objectives, plan, etc.).

- Research and technical training: ESRs will participate in at least *three* research and technical modules during the first two years of the training programme. Research and technical modules will be provided by both the host supervising and co-supervising institutions. The modules will be selected together with the supervisor and co-supervisor according to the scientific knowledge and competency needs of each ESR in order to conduct their individual research project. The ESR should list the selected modules and their corresponding information for the forthcoming year.
- Secondments in academic and non-academic organizations: Following the structure of the three-year training programme, each year will include one secondment at a beneficiary or partner organisation. ESR should describe the objectives of the secondments, planned activities, duration, etc. The involvement in non-academic business oriented projects is encouraged, as well as, the contribution to medium-large research projects (e.g., national and EU-funded).

2.5.3 **Interdisciplinary Training** (network-wide/online)

The objective of the interdisciplinary training is to complement the individual research and technical training, and provide ESRs with a holistic view of privacy and usability (e.g. Privacy in eHealth, Economics of Privacy, Decision Making Regarding Privacy). Training modules covering different aspects of privacy and usability will be offered either within the network-wide events or via online training. During the first two years of the training programme, ESRs are expected to take at least three interdisciplinary training modules.

2.5.4 **Professional Training** (network-wide/online)

Professional training is focused on the development of competencies and skills that will be needed by ESRs in their career path, beyond the PhD. Professional training modules will include the development of strategies to successfully communicate the research results (e.g. scientific paper writing and publication process: knowledge transfer and exploitation of research results; and technology transfer Concepts) and the development of intellectual, communication, presentation, organizational and research skills (e.g. preparation for academic and industrial career: and innovation and entrepreneurship). Following the training programme structure, ESRs are expected to take at least five professional training modules. The list of planned modules should include title of the course, credits, etc.

2.5.5 Other training activities

Indicate other training activities relevant to the career development plan of the ESR.

- Teaching
- Organization of seminars
- Organization of workshops
- Contribution to standardisation activities

2.5.6 Research management

Indicate other funding applications planned (name of award; fellowships with entire funding periods, grants written/applied for/received, professional society presentation awards or travel awards, etc.)

2.5.7 Networking activities

List of anticipated networking activities; network-wide events, and business oriented conferences.

2.5.8 **Other activities** (with professional relevance)

List of other activities that do not fall into the categories listed above.

2.6 Overview of progress, achievements and performance

A brief overview of research progress and major achievements (e.g. papers published or submitted, deliverables, etc.) during the last period should be indicated in the CDP from the second year.

2.7 Adjustments

Any deviation from the initial plan and the analysis of the potential risks and their impact should be described in this section from the second year.

2.8 Signatures

Signatures of ESR, supervisor and co-supervisor.

3 Template - Career Development Plan Year 1

Target audience and use of this document: The Career Development Plan is intended to be a document to guide the ESR and the supervisors as and where applicable the direct superior at the hiring institution with the procurement of the Marie Curie programme. It contains a series of personal information of the ESR and should be treated as confidential. Where necessary the document may be made available to the project leader, the management board or a designated group of persons for the purposes of mediation or dispute resolution. Where necessary and specifically asked for the document may be made available to the European Commission or the reviewers appointed by the EC for purposes of the evaluation of the project and other purposes specified in the programme's funding regulations.

I. *Personal and Organizational Information*

ESR´s Personal Information			
Name:		**ID number**:	
Office Address:		**Phone**:	
Mobile:		**E-Mail:**	

ESR´s Host Organization Information			
Name:		**Phone**:	
Address:			
***If enrolled organization is different from host organization, please specify:**			
Name:		**Phone:**	
Office Address:			

II. *Supervision*

Supervision			
Supervisor´s Name:		**Title**:	
Place of Employment:		**Phone**:	
Responsibility Distr.:		**E-Mail:**	
Co-Supervision			
Co-Supervisor´s Name:		**Title**:	
Place of Employment:		**Phone**:	
Responsibility Distr.:		**E-Mail:**	
Conduct of Supervision (per activity describe form of supervision and estimated supervision hours)**:**			

III. Secondment

ESR´s Secondment			
Supervisor’s Name:		**Position**:	
Organization´s Name:		**Phone**:	
Address:		**E-mail:**	

IV. Research Project

ESR´s Project			
Title:		**Ref. No:**	
Overview and background			

V. Long-Term Career Objectives

Long-Term Career Objectives (over five years)

VI. Short-Term Career Objectives

A. Project Research Results

Project Research Results
Presented according to Privacy & Us project Plan.

Milestones	Expected Results

Deliverables

Anticipated Publications

Anticipated Conference/Workshop Attendance & Courses/Seminar Presentations

B. Training

Research and Technical Training

Secondment Plan

Interdisciplinary Training

Professional Training

Other Training Activities

C. *Networking Activities*

D. Research Management

E. Other activities

Other Activities (professional relevant)

VII. Signatures

____

Date & Signature of fellow supervisor

____

Date & Signature of