The Wicked Problem of Privacy

Design Challenge for Crypto-based Solutions

Ala Sarah Alaqra

Faculty of Health, Science and Technology

Computer Science

LICENTIATE THESIS | Karlstad University Studies | 2018:23

The Wicked Problem of Privacy

Design Challenge for Crypto-based Solutions

Ala Sarah Alaqra

LICENTIATE THESIS | Karlstad University Studies | 2018:23

The Wicked Problem of Privacy - Design Challenge for Crypto-based Solutions

Ala Sarah Alaqra

LICENTIATE THESIS

Karlstad University Studies | 2018:23

urn:nbn:se:kau:diva-67134

ISSN 1403-8099

ISBN 978-91-7063-856-5 (print)

ISBN 978-91-7063-951-7 (pdf)

Distribution:
Karlstad University
Faculty of Health, Science and Technology
Department of Mathematics and Computer Science
SE-651 88 Karlstad, Sweden
+46 54 700 10 00

Print: Universitetstryckeriet, Karlstad 2018

WWW.KAU.SE

The Wicked Problem of Privacy
Design for Crypto-based Solutions

ALA SARAH ALAQRA
Department of Mathematics and Computer Science
Karlstad University

Abstract

Data privacy has been growing in importance in recent years, especially with the continuous increase of online activity. Researchers continuously study, design, and develop solutions aimed at enhancing users' data privacy. The wicked problem of data privacy is a continuous challenge that defies straightforward solutions. Since there are many factors involved in data privacy, such as technological, legal, and human aspects, we can only aim at mitigating rather than solving this wicked problem. Our aim was to focus on human aspects for designing usable crypto-based privacy-enhancing solutions. In this thesis, we followed a user-centred design method by using empirical qualitative means for investigating user's perceptions and opinions of our solutions. Most of our work has focused on redactable signatures in the cloud context within an eHealth use-case. Redactable signatures are a privacy-enhancing scheme, which allow the removal of parts of a signed document by a specified party, for achieving data minimisation without invalidating the respective signature. We mainly used semi-structures interviews and focus groups in our investigations. Our results yielded key Human Computer Interaction considerations as well as guidelines of different means for supporting the design of future solutions.

Keywords: Data privacy, wicked problems, user-centred design, crypto-based solutions, usability, data minimisation, redactable signatures

Acknowledgements

My acknowledgement goes to all entities, human and non-human alike, which contributed to the fuelling of my thoughts, knowledge, and *mana*.

Specific thanks goes to my main supervisor for her valuable mentorship and generous support, and to my co-supervisor for our fruitful discussions and interesting talks. I would like to express appreciation to the challenges and discussions provided by my previous and current colleagues.

A special gratitude goes to my family and friends, who nurtured me in my recent impediment and continue to have my back, in every way possible. In addition, I am particularly deeply grateful to the unconditional support, encouragement, and love of my special family; I would have not been able to re-spawn if it were not for you. Finally, I would like to thank those who contributed in our user-studies to the knowledge body of this work, my Compiler for being the black box wizard, and my special board-gaming friends for priceless evenings.

Karlstad University, May 10, 2018 Ala Sarah Alaqra

List of Appended Papers

This thesis is based on the work presented in the following papers:

I. **Ala Alaqra**, Simone Fischer-Hübner, Thomas Groß, Thomas Lorünser, Daniel Slamanig. Signatures for Privacy, Trust and Accountability in the Cloud: Applications and Requirements. In: IFIP Summer School on Privacy and Identity Management. Time for a Revolution?, pp. 79-96, Springer International Publishing, 2016.

II. **Ala Alaqra**, Simone Fischer-Hübner, John Sören Pettersson, Erik Wästlund. Stakeholders' Perspectives on Malleable Signatures in a Cloud-based eHealth Scenario. In: Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance (HAISA), pp. 220-230, 2016.

III. **Ala Alaqra**, Simone Fischer-Hübner, Erik Framner. Enhancing Privacy Controls for Patients via a Selective Authentic EHR Exchange Service – Perspectives by Medical Professionals and Patients. Under Submission.

IV. Thomas Länger, **Ala Alaqra**, Simone Fischer-Hübner, Erik Framner, John Sören Pettersson, Katrin Riemer. HCI Patterns for Cryptographically Equipped Cloud Services. To appear in: HCI International 2018 (20th International conference on Human Computer Interaction), Springer International Publishing, August 2018.

The papers have been subjected to minor editorial changes.

Comments on my Participation

Paper I I have designed and led the moderating and conducting of the interactive workshop study (part 1). Co-Authors were responsible for the tutorial part of the workshop and helped in part 1 and also in summarising results.

Paper II I was the main responsible for the paper. I have designed and led the conducting of studies, analysed results and participated in the requirements elicitation. John Sören helped in conducting the interviews, Simone Fischer-Hübner helped in moderating the workshop. Co-authors contributed to the discussions and analysis of the requirements.

Paper III I was the main responsible for the paper's work, and have led the conducting of the studies, and evaluations of results. Co-authors helped in conducting the studies, writing, and reviewing the paper.

Paper IV I have been involved throughout the paper's work. Thomas Länger was the main responsible for the paper. I took part in the paper's contribution (patterns) analysis and was responsible for 2/3 of the patterns evaluation studies and writing.

Contents

Paper IV: HCI Patterns for Cryptographically Equipped Cloud Services 89

Introductory Summary

1 Introduction

In design, a wicked problem is a complex one that has no definite solution [8]. Wicked privacy is a term introduced in this thesis that corresponds to the design challenge of addressing privacy solutions. We posit that privacy, specifically in the context of data privacy, is a wicked problem. It refers to the challenge of designing for usable privacy enhancing solutions, while taking into consideration the trade-offs and dynamics of technological, legal, and human factors. The growth of security threats and privacy invasive portals and applications calls for proactive measures aimed at data privacy and security protection [13]. Privacy Enhancing Technologies (PETs) aim to tackle threats to personal data, by providing means to eliminate or minimise personal data processing, for protecting privacy [31]. Crypto-based PETs may be considered counter intuitive to users [33]; therefore, a challenge is to design for usability and user's adoption of privacy technologies at hand [4]. Our strategy to address the wicked privacy design challenge involves collaboration with different users as an approach to tackle wicked problems [6]. In this work, we aim to shed a light on design criteria for usable crypto-based privacy enhancing services, which are newly developed in the PRISMACLOUD project. We addressed different types of users throughout our empirical user studies. We presented user-centred design guidelines for privacy enhancing solutions, focusing on malleable signatures used in eHealth applications.

The remainder of this summary is structured as follows. Section 2 sets the stage for the thesis with corresponding background and related work. The research question is presented in Section 3. An overview of the approach and methods used are presented in Section 4. Contributions are presented in Section 5. Summaries of appended papers are found in Section 6. Finally, conclusions are presented in Section 7.

2 Background and Related Work

In the following subsections, we will present the relevant background and related work corresponding to the thesis.

2.1 HCI and Design

The field study of Human Computer Interaction (HCI) is considered the fastest growing and most visible part of computer science [9]. HCI is a multidisciplinary discipline that focuses on human factors and computer systems integration and interactions. Through observations, analysis, evaluation and implementation, HCI aims to design systems for human use. Concepts like usability and user experience are shown to be important in designing functionality of systems for users [28]. On the one hand, usability involves meeting up with usability criteria: effectiveness, efficiency, safety, utility, learnability, and memorability [28]. While on the other hand, user experience focuses on qualities of the experience: satisfying, enjoyable, fun, entertaining, helpful, motivating, aesthetically pleasing, supportive of creativity, rewarding, and emotionally fulfilling [28]. Designing for the two concepts usually involves trade-offs depending on the context of use, task, and untended users [9]. When dealing with human factors in design, it is essential to take both concepts into consideration for design [28].

2.2 Privacy and Data

Whether it is personal space or private belongings, privacy is valued to a certain extent subjectively from one person to the other [23]. What is *privacy*? The answer would differ based on the perspective. Privacy, as Warren and Brandeis define it is "the right to be let alone" [32]. That definition indicates the intrusive role of the exterior environment that could threaten one's (un)conscious sense of own privacy. In a computer science perspective, intrusion of privacy tend to be focused on users' data. Ordinary users tend to overlook the consequences and implications of direct and indirect intrusions to their information. Intrusive applications and portals tend to threaten one's data privacy implicitly as well as explicitly. Studies show how private information can be derived from digital records e.g., Facebook likes deriving personal attributes [21]. For instance inferred data (expecting a baby), which can be derived from apparently non-sensitive data (shopping list), is usually overlooked by many users, however acquiring that information can still in many cases be considered an intrusion [20].

Another definition of privacy by Westin is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" [34]. Informational self-determination directly relates to the privacy aspects of user control and selective disclosure that we are addressing in our studies.

2.3 Wicked Privacy Design

Wicked problems is a concept that refers to a complexity of a problem that deems it unsolvable, especially in design where indeterminacy of conditions and limitations are prominent [8]. In contrast, "tame" problems, like for example mathematical integrals, have a clear solution and are thus considered solvable [8,14]. A great amount of research on data privacy, from technological, legal, and social perspectives as well, has been shown to take part in many disciplines [29]. For instance, Regan (1995) focused on three forms of privacy concerns: communicational, informational, and psychological . And it was shown that technological advancements have an adverse influence on data privacy. It was stated that privacy as a collective social value is an important factor for addressing privacy concerns [27].

Technology that aims to enhance the privacy and security of tools and applications follows the privacy by design principle [11]. Whereas laws regulating privacy and data protection focus on the legal perspective, such as the GDPR (General Data Protection Regulation) in Europe [1] requires following privacy by default principle. Human factors taken into consideration in early development stages follow privacy by design and user-centred design approaches [3, 25]. Considering the above-mentioned entities involved in data privacy and their entanglements, it is credible to declare data privacy a wicked problem. A consideration that was the bases for our studies design and we will highlight three main positions of this wicked privacy design challenge in the following paragraphs: technological, legal, and human aspects. All of which change dynamically by time, and would require continuous updating to correspond to new technologies, laws, and experiences.

2.3.1 Technological

Technological advancements in data privacy research deal with enhancing privacy by developing improved solutions. Privacy Enhancing Technologies (PETs) aim to mitigate the privacy challenge by providing several means for users to adopt. Related work has given an account for the shortcomings of privacy enhancing technology work [15]. Danezis and Grüses surveyed the field of privacy research of PETs and highlighted the complexities of privacy scope and definitions. They presented key technologies, and showed that privacy research is usually tackled within the boundaries of their narrow scope and definitions. They concluded that in order for privacy research to progress, we need to address the bigger picture [15]. This entails the wickedness of privacy, since the bigger the picture the greater the complexity when dealing with privacy solutions.

2.3.2 Legal

Not only the definition of privacy varies with context, so do the legal rules for what constitutes privacy in different systems. For instance, the European charter of the fundamental rights clearly defines privacy and data protection as human rights in articles 7 and 8 [2]. Whereas the US constitution does not explicitly mention the word *privacy*, but rather security against intrusions in the fourth amendment (*search and seizure*). Previous work has shown conflicts and contrast between U.S. and EU regulations in privacy policies, and specially implications of those on trade and transaction in globalisation and digital age [24].

2.3.3 Human Behaviours and Experiences

The privacy paradox is a phenomenon where users indicate their concerns about privacy while their behaviours state otherwise [7, 30]. It is believed that this is partially because users are primarily seeing the immediate benefits of services while being unaware of the long-term consequences and implications of the digital interactions [30]. We can easily understand the financial implications of sharing a credit card number, whereas on the other hand sharing a location online may seem harmless at the first glance. The privacy paradox alongside human's subjectivity to perceive privacy, are clear challenges for designing privacy solutions.

2.4 PRISMACLOUD Context

The work of this thesis took place within the scope of PRISMACLOUD (PRIvacy and Security MAintaining services in the CLOUD), which is a research project funded by the European Union's Horizon 2020 research and innovation program [26]. PRISMACLOUD develops cloud-based solutions, which use cryptographic schemes to enhance security and privacy. The project develops novel services from crypto schemes into Use-cases within the project are in the areas of eHealth, eGovernment, and Smart city. The main crypto-scheme addressed in this thesis work is a data minimisation solution called Malleable signatures within an eHealth use-case.[1]A malleable (also called redactable) signature is a cryptographic scheme that allows specified redaction (removing or blacking out) of fields within a digitally signed document while maintaining the validity of the signature [12, 16]. One of the PRISMACLOUD eHealth use-cases [2] allows patients to redact specified fields of documents that were digitally signed by their medical doctor. Using malleable signatures allows users to minimize the amount of information on their signed digital documents and thus enhancing their data privacy. User-control is inferred by using malleable signatures, as it enables users to first redact and then selectively disclose authentic data.

2.5 Other Related Work

When it comes to designing for usable privacy, many related work has attempted to address that challenge in different areas. In [36] they presented security and privacy requirements in the context of online social networks, and highlighted their design challenges as well as trade-offs for social benefits. Additionally they also highlighted the need for a collaborate effort among disciplines in the field of privacy and security research. In Paper 1, we have combined experts with the different backgrounds in order to address opportunities and challenges collectively. In their users' studies of authentication technologies [19], they highlighted the need to address technological and social factors interplay for acceptance. Control of information is one of the issues resulted by their studies to be a hinder for the acceptance. we address control of information through data minimisation in our work mainly of Paper III. Users are not at fault when it comes to accepting and using security-based solutions. In their work with user passwords in work practice [5], they addressed the need for user-centred design and communication with users. Their case highlighted the challenge of motivating users to secure actions as part of the understanding gap between security departments and users. In [35], they showed how user

[1] Data minimisation is a privacy principle that deals with limiting the collection and use of personal data as according to Art. 5 I (c) of the GDPR [1].

[2] The use-case involves the implementation of a "Selective Authentic Exchange Service"

interface standards aren't enough for usability. Users, who were not familiar with the technology used in the program, failed in the usability test of their security program. In the user studies of Paper III, we selected users who are not familiar with malleable signatures.We focused on addressing users with different technical backgrounds, and highlighted requirements addressing usability of malleable signatures.

3 Research Questions

We address the following research question in this thesis:

How to design for usable crypto-based privacy services? The adoption of crypto-based services relies mainly on their usability. Understanding users' intuitive perception is especially important when addressing the usability of privacy enhancing crypto-based services. In our studies, we addressed novel services developed within the PRISMACLOUD project with a focus on a Selective Authentic Exchange Service used in eHealth, which is based on malleable signatures. In that case, the complexity is increased due to the different roles and views that users have in the process of redaction. Our approach focuses on user's involvement early in the design and development processes of crypto solutions. Their involvement includes the investigation of their perspectives, opinions, concerns, needs, and requirements. For addressing the research question, we investigated different users and stakeholders throughout our design and development stages.

4 Research Methods

4.1 UCD Approach

To answer our research question, we had to consider users as an important factor for designing usable solutions [3]. We therefore focused on the users within our User-Centred Design (UCD) approach. UCD enables better understanding of user's needs and goals throughout the iterative cycles of development and design processes [3, 25]. We chose qualitative methods as means for collecting data and exploring the complexities of user's perspectives: semi-structured interviews and focus groups (see below subsections). We used a combination of the two qualitative methods in our triangulation of Paper I, which allowed us to collect data that are more comprehensive and enhance our understanding in the earlier stages of the project. Triangulation is the use of a combination of methodologies in addressing the same question [22]. The combination can be either within method (all e.g. qualitative), or mixed (qualitative and quantitative). As for Paper III, we used the two methods corresponding to the study design and the two different users.

4.2 Measures for Studies Support

The following are means that we used for our tasks description throughout our data collection methodologies.

- *Use-cases:* A use-case defines tasks, or envisioned tasks in early project stages, with a focus on functionality from users' perspectives. use-cases mainly describe the interactions and activities between users and the system [28]. It is commonly the task of software developers to define use-cases for the system usages. In PRISMACLOUD, use-cases were defined in the areas of eHealth, eGovernment, and smart city (Paper I).

- *Scenarios:* A scenario is a description of tasks and activities that follow an informal and story-like format [9]. Scenarios are also considered one of the richest formats of design interaction representation and most flexible [17]. We have used scenarios in the descriptions of our use-cases in all our user studies (Papers I-IV). Scenarios facilitate the understanding of our use-cases and discussions with our correspondents due to easy language and narrative format.

- *Personas:* Personas are fictional roles or characters designed with descriptive profiles in order to mimic a realistic situation [28]. We used user personas in the study of Paper III to facilitate our discussion and to avoid the exposure of our correspondents' personal information: correspondents rather used the assigned personas in their tasks and discussions.

- *Metaphors:* In design, metaphors are used to convey new meanings to users and help understand ideas using comparison. By mapping the familiar to the unfamiliar, metaphors help in understanding the target domain and further address users' mental models [10]. We have used metaphors throughout Papers II-IV.

- *Mock-ups:* Mock-ups are low-fidelity prototypes that are designed in earlier stages of the development process, in order to capture user's feedback during evaluation. They aid in presenting functionality through visualisation in the users' interface [28]. We have designed mock-up UIs presented in Paper III.

- *HCI Patterns Template:* We used HCI patterns template to present our design solutions in our results. The template provided a framework for our patterns [18]. HCI patterns aid in communicating our solutions to designers and developers within the project as used in Paper IV.

4.3 Semi-structured Interviews

Semi-structured interviews are a form of inquiry that does not follow a strict structure, but rather allows deviations and flexibility. The facilitation of discussion openness is necessary for an in-depth understanding of the user's perspectives [28]. We have used this form of inquiry in both Papers II and

III. Semi structured interviews allow us to investigate user's perceptions and opinions while customising our inquiry during the interview. Though time-consuming, this form of interviews allows detailed discussions to understand correspondent's responses. In the work presented in Paper II, we used a set of predefined questions that acted as a guide for the interviews. However, in Paper III, the mock-ups interfaces acted as the framework for the interviews discussion themes.

4.4 Focus Groups

Similar to the interviews, focus groups methodology allow us to investigate user perceptions, opinions, attitudes and concerns. However, the dynamic of the focus group gives an added layer of interaction, where participants can agree, contradict, and/or elaborate on others' inputs [28]. We used focus groups' interactivity and dynamics of discussions as a second approach to interviews for Paper II. As for Paper III, the interaction among participants was essential for the study design, which included personas for the redaction (blacking out fields on Paper) exercise.

5 Contributions

To address different considerations for designing usable privacy enhancing technologies, varied user-studies have been conducted throughout this thesis. Overall, the user focus in our UCD approach have resulted in following contributions:

1. *Analysis of different user's perspectives and mental models*

   To address the design challenge of usable crypto-based privacy services, we need to understand the requirements and difficulties associated with them. We have investigated users' perspectives, attitudes, understandings, and opinions throughout the thesis with the focus on a selective authentic exchange service used in an eHealth use-case based on malleable signatures. (Papers I-III). Users with different technical background, roles in the services process (signing or redacting),and contextual influence (country-based comparison), were the factors considered. Outcomes included contributions to the understanding of end user and HCI challenges, which have helped identifying key HCI considerations and concerns for eliciting usability, trust, and privacy requirements. Additionally outcomes highlighted the need for rules, policies, and templates.

2. *Usability and HCI requirements*

   The requirements for the selective authentic exchange service were elicited, analysed, and refined through several iterations (Papers I-III). The first iteration (Paper I), requirements were elicited via focus group workshops. The second iteration (Paper II) the requirements were refined by results from semi-structured stakeholder interviews. Mock-ups addressing those requirements were then designed and evaluated by walk-throughs used in interviews and focus groups. Consequently, The evaluations resulted in a 3rd iteration of requirements (Paper III).

3. *Guidelines for usable design solutions*

   We present different means of supporting the design of usable crypto-based privacy solutions.

   - General guidelines and recommendations of different stakeholders for end users adoption of PETs. Examples include (a) decreasing the cognitive burden on users and provide support through privacy by default (Paper II), (b) choice of alternatives corresponding to users' technical background knowledge (Paper III).
   - Mock-ups designs for Authentic Selective EHR[3] Exchange service[4], which were tested and evaluated in iterations and could act as a guide template for future applications design (Paper III).
   - HCI patterns, which include metaphors addressing user's mental models (Paper IV). These include HCI patterns for digital signature visualisation, the use of the *stencil* metaphor for the redaction process, and default configurations for a cloud-based archiving system[5].

6 Summary of Appended Papers

Paper I – Signatures for Privacy, Trust and Accountability in the Cloud: Applications and Requirements

The work in this paper addresses earlier stages of the PRISMACLOUD project. Results are based on the 2-days workshop held at IFIP Summer School 2015. Participants were therefore participants of the conference. Cryptographic tools and use-case scenarios of PRISMACLOUD were presented in the workshop. For Day 1, an interactive part of the workshop took place. There were 25 participants forming 5 interdisciplinary parallel focus groups. They discussed use-case scenarios and explored HCI challenges for eliciting usability, trust, and privacy requirements. The second day features a tutorial on graph signatures and topology certification, and technical discussion on further possible applications. The paper summarises the results of the 2-day workshop with a highlight on applications scenarios and the elicited end-user requirements.

Paper II – Stakeholders' Perspectives on Malleable Signatures in a Cloud-based eHealth Scenario

In this paper, malleable signatures scheme in the eHealth use-case of PRISMACLOUD was in focus. We investigated stakeholders representing end-users

[3] Electronic Health Record

[4] Service that is developed in PRISMACLOUD using malleable signatures, see http://archistar.at/

[5] Using secret sharing scheme for Archistar developed in PRISMACLOUD.

in the earlier stages of our UCD approach. The objective was to gain an understanding of user's opinions and concerns regarding the use of malleable signatures. We therefore elicited requirements addressing usability aspects as well as social factors. Results from our qualitative studies, semi-structured interviews and focus groups, have yielded our end-user requirements presented and evaluated in this paper. Examples included suitable metaphors and guidelines, usable templates, and clear redaction policies. Future work suggested decreasing the cognitive burden on users through technical and UI support, e.g., default privacy-friendly settings.

Paper III – Enhancing Privacy Controls for Patients via a Selective Authentic EHR Exchange Service – Perspectives by Medical Professionals and Patients

In this paper, we focus on two different users' perspectives, the medical professionals on one side, and prospective patients from the other. The Selective Authentic EHR Exchange service is a solution developed by PRISMACLOUD in the eHealth scenario. Privacy is enhanced, through data minimisation principle, and authenticity is ensured in EHR using redactable signatures. We investigated the perspectives and opinions of our participants, in both Germany and Sweden, using the designed low fidelity mock-ups (presented in the paper). For signer's perspectives, we interviewed 13 medical professionals. As for the redactors' perspectives, we conducted five focus groups of prospective patients (32 in total) with varying technical expertise. We presented and discussed the results from both perspectives, and refined our requirements and presented further ones for future implementations.

Paper IV – HCI Patterns for Cryptographically Equipped Cloud Services

This paper presents three HCI patterns for PRISMACLOUD Cloud based cryptographic privacy solutions. They address the challenge of how cryptographic solutions are counter-intuitive to users' mental models.Tackling security and privacy risks cryptographic solutions in the Cloud, HCI patterns provide means for communicating guidelines and requirements to designers and implementers. This approach was used within PRISMACLOUD development lifecycle of its two Cloud-based solutions. Details of the categories, analysis, and evaluation of the following patterns were described in the paper.

- ***HCI.P1*** Digital Signature Visualisation, a visual representation of signers' handwritten signatures on digital documents. This resemblance with signatures on paper visualisation and location on the document acts as an intuitive means for using digital signatures.
- ***HCI.P2*** Stencil for Digital Document Redaction, a metaphor of blacking-out/greying-out fields on the document in a process of redaction. This process encompasses the data-minimisation principle of privacy protection.
- ***HCI.P3*** Secret Sharing Configuration Preferences, recommended default configurations settings based on the priority user selection of the 3 preferences:

"Cost Minimisation" , "Data Confidentiality Maximisation – High Data Protection", and "Data Availability Maximisation – High Data Loss Prevention".

7 Conclusions

In this thesis, we started with presenting the wicked problem of privacy, in the aim of highlighting the different aspects and factors involved. Thus paving the way for tackling the dynamic complexity of the design challenge for privacy enhancing solutions. In our work, we have presented our UCD exploratory approach with qualitative results shedding the light on guidelines for future design solutions. Since we are tackling a wicked problem, trade-offs between technological, legal, and human aspects need to be considered when designing for crypto-based privacy solutions. Users' familiarity with technology, their technical background, and their privacy attitudes are key factors to addressing the human aspects for design.

References

[1] EU Commission:General Data Protection Regulation (GDPR). http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN. (Accessed on 05/04/2018).

[2] Charter of fundamental rights of the european union. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT, 2012. (Accessed on 04/30/2018).

[3] C. Abras, D. Maloney-Krichmar, and J. Preece. User-centered design. *Bainbridge, W. Encyclopedia of Human-Computer Interaction. Thousand Oaks: Sage Publications*, 37(4):445–456, 2004.

[4] A. Adams. Users' perception of privacy in multimedia communication. In *CHI'99 Extended Abstracts on Human Factors in Computing Systems*, pages 53–54. ACM, 1999.

[5] A. Adams and M. A. Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[6] J. Alford and B. W. Head. Wicked and less wicked problems: a typology and a contingency framework. *Policy and Society*, 36(3):397–413, 2017.

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

[8] R. Buchanan. Wicked problems in design thinking. *Design issues*, 8(2):5–21, 1992.

[9] J. M. Carroll. *HCI models, theories, and frameworks: Toward a multidisciplinary science*. Elsevier, 2003.

[10] J. M. Carroll, R. L. Mack, and W. A. Kellogg. Interface metaphors and user interface design. In *Handbook of human-computer interaction*, pages 67–85. Elsevier, 1988.

[11] A. Cavoukian. Privacy by design. *Take the challenge. Information and privacy commissioner of Ontario, Canada*, 2009.

[12] M. Chase, M. Kohlweiss, A. Lysyanskaya, and S. Meiklejohn. Malleable signatures: Complex unary transformations and delegatable anonymous credentials. *IACR Cryptology ePrint Archive*, 2013:179, 2013.

[13] D. Chen and H. Zhao. Data security and privacy protection issues in cloud computing. In *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*, volume 1, pages 647–651. IEEE, 2012.

[14] R. Coyne. Wicked problems revisited. *Design studies*, 26(1):5–17, 2005.

[15] G. Danezis and S. Gürses. A critical review of 10 years of privacy technology. *Proceedings of surveillance cultures: a global surveillance society*, pages 1–16, 2010.

[16] D. Derler, H. C. Pöhls, K. Samelin, and D. Slamanig. A general framework for redactable signatures and new constructions. In *International Conference on Information Security and Cryptology*, pages 3–19. Springer, 2015.

[17] A. Dix. Human-computer interaction. In *Encyclopedia of database systems*, pages 1327–1331. Springer, 2009.

[18] S. Fischer-Hübner, C. Köffel, J. Pettersson, P. Wolkerstorfer, C. Graf, L. Holtz, U. König, H. Hedbom, and B. Kellermann. Hci pattern collection–version 2. *Priv. Identity Manag. Eur. Life*, 61, 2010.

[19] M. Harbach, S. Fahl, M. Rieger, and M. Smith. On the acceptance of privacy-preserving authentication technology: the curious case of national identity cards. In *International Symposium on Privacy Enhancing Technologies Symposium*, pages 245–264. Springer, 2013.

[20] K. Hill. How target figured out a teen girl was pregnant before her father did. *Forbes, Inc*, 2012.

[21] M. Kosinski, D. Stillwell, and T. Graepel. Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, 110(15):5802–5805, 2013.

[22] W. E. Mackay and A.-L. Fayard. Hci, natural science and design: a framework for triangulation across disciplines. In *Proceedings of the 2nd conference on Designing interactive systems: processes, practices, methods, and techniques*, pages 223–234. ACM, 1997.

[23] A. Morton and M. A. Sasse. Desperately seeking assurances: Segmenting users by their information-seeking preferences. In *Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on*, pages 102–111. IEEE, 2014.

[24] L. B. Movius and N. Krup. Us and eu privacy policy: comparison of regulatory approaches. *International Journal of Communication*, 3:19, 2009.

[25] D. A. Norman and S. W. Draper. *User centered system design: New perspectives on human-computer interaction*. CRC Press, 1986.

[26] PRISMACLOUD. Privacy and security maintaining services in the cloud. https://prismacloud.eu/. EU H2020 project(Accessed on 04/30/2018).

[27] P. M. Regan. *Legislating privacy: Technology, social values, and public policy*. Univ of North Carolina Press, 1995.

[28] Y. Rogers, H. Sharp, and J. Preece. *Interaction design: beyond human-computer interaction*. John Wiley & Sons, 2011.

[29] H. J. Smith, T. Dinev, and H. Xu. Information privacy research: an interdisciplinary review. *MIS quarterly*, 35(4):989–1016, 2011.

[30] M. Taddicken. The "privacy paradox" in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, 19(2):248–273, 2014.

[31] G. Van Blarkom, J. Borking, and J. Olk. Handbook of privacy and privacy-enhancing technologies. *Privacy Incorporated Software Agent (PISA) Consortium, The Hague*, 2003.

[32] S. D. Warren and L. D. Brandeis. The right to privacy. *Harvard law review*, pages 193–220, 1890.

[33] E. Wästlund, J. Angulo, and S. Fischer-Hübner. Evoking comprehensive mental models of anonymous credentials. In *Open problems in network security*, pages 1–14. Springer, 2012.

[34] A. F. Westin. Privacy and freedom, new york: H. *NY: Atheneum*, 1967.

[35] A. Whitten and J. D. Tygar. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *USENIX Security Symposium*, volume 348, 1999.

[36] C. Zhang, J. Sun, X. Zhu, and Y. Fang. Privacy and security for online social networks: challenges and opportunities. *IEEE network*, 24(4), 2010.

The Wicked Problem of Privacy

Data privacy has been growing in importance in recent years, especially with the continuous increase of online activity. Researchers continuously study, design, and develop solutions aimed at enhancing users' data privacy. The wicked problem of data privacy is the continuous challenge that defies straightforward solutions. Since there are many factors involved in data privacy, such as technological, legal, and human aspects, we can only aim at mitigating rather than solving this wicked problem.

Our aim was to focus on human aspects for designing usable crypto-based privacy-enhancing solutions. In this thesis, we followed a user centered design method by using empirical qualitative means for investigating user's perceptions and opinions of our solutions. Most of our work has focused on redactable signatures in the cloud context within an eHealth use-case. Redactable signatures are a privacy-enhancing scheme, which allow the removal of parts of a signed document by a specified party without invalidating the respective signature. Our results yielded key Human Computer Interaction considerations as well as guidelines of different means for supporting the design of future solutions.

ISBN 978-91-7063-856-5 (print)

ISBN 978-91-7063-951-7 (pdf)

ISSN 1403-8099

LICENTIATE THESIS | Karlstad University Studies | 2018:23