THE LORD OF THEIR DATA UNDER THE GDPR?

Empowering Users Through Usable Transparency, Intervenability, and Consent

FARZANEH KAREGAR

The Lord of Their Data Under the GDPR?

Empowering Users Through Usable Transparency, Intervenability, and Consent

Farzaneh Karegar

Faculty of Health, Science and Technology

Computer Science

DOCTORAL THESIS | Karlstad University Studies | 2020:36

The Lord of Their Data Under the GDPR?

Empowering Users Through Usable Transparency, Intervenability, and Consent

Farzaneh Karegar

DOCTORAL THESIS | Karlstad University Studies | 2020:36

The Lord of Their Data Under the GDPR? - Empowering Users Through Usable Transparency, Intervenability, and Consent

Farzaneh Karegar

DOCTORAL THESIS

Karlstad University Studies | 2020:36

urn:nbn:se:kau:diva-81235

ISSN 1403-8099

ISBN 978-91-7867-170-0 (print)

ISBN 978-91-7867-169-4 (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 2020

WWW.KAU.SE

If this book is an accomplishment,

I dedicate it to all innocent children all over the world deprived of their right to education. The more significant achievement is yet to be gained when I can contribute to making their lives fairer and happier.

I also dedicate it to my son, Noyan. May you never stop learning.

The Lord of Their Data Under the GDPR?

Empowering Users Through Usable Transparency, Intervenability, and Consent

Farzaneh Karegar
Department of Mathematics and Computer Science
Karlstad University

Abstract

The challenges imposed by the ever-growing online data processing make it difficult for people to control their data, which inevitably imperils the privacy of their personal information and making informed decisions. Thus, there is an increasing need for different societal, technological, and legal solutions that empower users to take control of their data. The intervenability rights and the enhanced transparency and consent requirements in the General Data Protection Regulation (GDPR) aim to enable users to gain control of their data. However, these rights and requirements will not be beneficial for users in practice without considering their Human-Computer Interaction (HCI) implications.

The objective of this thesis is to propose usable tools and solutions which improve user-centred transparency, intervenability, and consent, thereby empowering users to take control of their data and make informed decisions. To this end, we employ quantitative and qualitative empirical HCI research methods and consider users through the development cycles of the proposed tools and solutions. We investigate how usable ex-post transparency can facilitate intervenability by implementing and testing Transparency-Enhancing Tools (TETs) that run on users' devices. Further, we analyse the effectiveness of engaging users with policy information through different types of interaction techniques on drawing user attention to consent form contents. We extend our investigation to the robustness of varying consent form designs to habituation. Moreover, we study how users perceive our design of adapted consent based on the demands and challenges of the technology at hand.

This thesis contributes to bridging the gap between legally compliant and usable tools and techniques that aim to enable users to maintain control of their data, resulting in several artefacts, design guidelines, and empirical contributions. The artefacts comprise prototypes and mockups of usable TETs and consent forms. The guidelines encompass a set of design requirements for ex-post TETs that run based on privacy notifications and recommendations on how to engage users with consent form contents. Finally, the empirical contributions include the analysis of the effectiveness of the proposed means and methods on enabling users to exercise their intervenability rights and provide informed consent.

Keywords: Control of personal data, Data privacy, GDPR, HCI, Informed consent, Transparency-enhancing tool, Usability, User interface design

Acknowledgments

"Now, this is not the end. It is not even the beginning of the end. But it is, perhaps, the end of the beginning." Although fortunately, it does not concern the Second Battle of El Alamein as was the case in Winston Churchill's speech in 1942, it is still about a battle; the bittersweet struggle of life, during which one decided to gain a PhD. I want to thank all the people who helped me to reach the end of my PhD journey, which is the beginning to discover the world through new eyes.

For my bachelor thesis, I implemented a low-power asynchronous NoC. For the master thesis, I investigated low-power adders in different number systems. The superficial commonality of the term "power" in what I did in the past with what I would work on during my PhD might not have been convincing enough to make me eligible for the position announced. However, my professional, genius, and caring supervisor, Prof. Simone Fischer Hübner, took a significant risk and gave me the chance of experiencing a whole new world in academia. I would like to express my deepest gratitude to her. I hope that I have not failed her. Without her steadfast support and guidance, I would not have the ability and confidence to realise the goal of reaching the end of my PhD. I would like to pay my special regards to my knowledgeable co-supervisor, Prof. John Sören Pettersson, who has always been available to help me unconditionally from reviewing my works to even finding participants for my studies. I likewise thank my former co-supervisor, Prof. Melanie Volkamer, from whom I learned a lot during the time she advised me at Karlstad University.

I wish to extend my gratitude to my collaborators, Patrick Murmann and Daniel Lindegren, and my co-authors. I am grateful for their contributions to the work presented in this thesis which has been funded by CREDENTIAL and PAPAYA EU projects under grant agreements No. 653454 and No. 786767, respectively.

In the mid of January 2015, I left Tehran to Karlstad to accompany my best friend for life, Kyoomars, who wanted to pursue his PhD abroad. In the beginning, the future was nothing but a dark tunnel to nowhere. I was feeling that I left the whole world behind me. Soon afterwards everything got more joyful thanks to new people I befriended and a warm welcome at Karlstad University. I am indebted to Susanne Larsson for her unconditional support from the very first day I arrived in Karlstad. My special thanks go to Aga, Jenni, Patrick, Zeeshan and Khadija, Ricardo, and Nurul and Rahnuma. I am whole-heartedly grateful that life brought them all to Karlstad. Most importantly, Karlstad became the hometown of the cutest creature I love the most in the world, Noyan. Thank you, Karlstad! I never imagined that one day you could even compete with Tehran in stealing my heart. Now, I have two homes thousands of kilometres away from each other.

I want to say a heartfelt "thank you" to my mum, my dad, and my sister, Faezeh, for their continuous and exceptional love and support. Maman, Baba, and Faezeh jan, I genuinely regret all the special moments I missed spending

beside you during the past few years. I could not be with you when my beloved nephew, Sobhan, was born. I could not even share Noyan's pictures with you for four days after his birth due to the Internet blackout in Iran in late November 2019. My special thanks also go to my in-laws. I cannot express my gratitude and feelings for my family members in a limited space in my non-mother tongue. I simply say that I love you all and keep the rest until we meet and perhaps can hug if the mysterious COVID-19 virus abates and hopefully disappears.

Finally, I wish to thank Kyoomars. Q jan, thank you for standing beside me through all ups and downs of this journey, for your understanding, your big heart, and the supports you provided to me. Life is short, some people say, but sweet for sure with you.

Karlstad University, November 5, 2020 Farzaneh Karegar

List of Appended Papers

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

I. **Farzaneh Karegar**, Tobias Pulls, Simone Fischer-Hübner. Visualizing Exports of Personal Data by Exercising the Right of Data Portability in the Data Track—Are People Ready for This?. In: *Privacy and Identity Management. Facing up to Next Steps: Privacy and Identity, Proceedings of the IFIP International Summer School*, pp. 164–181. Springer, 2016.

II. Patrick Murmann, **Farzaneh Karegar**. From Design Requirements to Effective Privacy Notifications: Empowering mHealth Users to Make Informed Decisions. Under submission.

III. **Farzaneh Karegar**, Daniel Lindegren, John Sören Pettersson, and Simone Fischer-Hübner. User Evaluations of an App Interface for Cloud-based Identity Management. In: *Advances in Information Systems Development*, Vol. 26, pp. 205–223. Springer, 2018.

A prior version of this paper won the **Best Paper Award** at ISD2017 and is published in the ISD2017 Proceedings.

IV. **Farzaneh Karegar**, Nina Gerber, Melanie Volkamer, and Simone Fischer-Hübner. Helping John to Make Informed Decisions on Using Social Login. In: *Proceedings of the 33rd ACM Annual Symposium on Applied Computing (SAC)*, pp. 1165–1174. ACM, 2018. **(Best Paper Award)**.

V. Daniel Lindegren, **Farzaneh Karegar**, Bridget Kane, and John Sören Pettersson. An Evaluation of Three Designs to Engage Users When Providing Their Consent on Smartphones. In: *Behaviour and Information Technology*, pp. 1–17. Taylor & Francis, 2019.

VI. **Farzaneh Karegar**, John Sören Pettersson, and Simone Fischer-Hübner. The Dilemma of User Engagement in Privacy Notices: Effects of Interaction Modes and Habituation on User Attention. In: *ACM Transactions on Privacy and Security (TOPS)*, Vol. 23, No. 1, Art. 5, pp. 1–38. ACM, 2020.

VII. **Farzaneh Karegar**, John Sören Pettersson, and Simone Fischer-Hübner. Fingerprint Recognition on Mobile Devices: Widely Deployed, Rarely Understood. In: *Proceedings of the 13th ACM International Conference on Availability, Reliability and Security (ARES)*, Art. 39, pp. 1–9. ACM, 2018.

VIII. Eva Schlehahn, Patrick Murmann, **Farzaneh Karegar**, and Simone Fischer-Hübner. Opportunities and Challenges of Dynamic Consent in Commercial Big Data Analytics. In: *Privacy and Identity Management. Data for Better Living: AI and Privacy, Proceedings of the IFIP International Summer School*, pp. 29–44. Springer, 2019.

Some of the appended papers have been subject to a few minor editorial changes.

Comments on My Participation

Paper I The idea of this paper, as well as the design of the user study, originated from a discussion with my supervisor, Simone Fischer-Hübner. I conducted all the interviews; Simone Fischer-Hübner assisted me in four of the ten interviews and improved and elaborated my text in the introduction, background, and related work sections. I was the sole author of other sections on which I received valuable comments from Simone Fischer-Hübner and Tobias Pulls. Tobias Pulls implemented the back-end of the tool and helped me with the front-end development especially with the map view.

Paper II Patrick Murmann came up with the idea of extracting design requirements for privacy notifications from the literature and evaluating them. Patrick Murmann compiled the preliminary version of the requirements from the literature. I contributed to the progressive iterations of the compilation of the requirements. I came up with the initial draft of the user study that served as the means to evaluate our research question. Then, together with Patrick Murmann, we designed the prototypes, the final version of the user study to evaluate them, and conducted the studies. Patrick Murmann did the actual implementation of the prototypes. I took the role of a note keeper, and Patrick Murmann was the moderator of the studies conducted. We analysed the data collected together and discussed them. I provided content for the discussion section and the subsection on design recommendations to support intervenability. I wrote the study design subsection and the results section. Patrick Murmann wrote all the other parts of the paper.

Paper III Daniel Lindegren, our assistant in the CREDENTIAL project, and I prepared the test design for all three tests in the paper and the relevant test objectives together with my supervisors, Simone Fischer-Hübner and John Sören Pettersson. The content of the paper and the test designs built on my work on a project deliverable. I also wrote the related work section of the paper. My co-supervisor, John Sören Pettersson, guided the assistants conducting the second test, and also outlined the paper and reduced the text from the deliverable to make a comprehensive and comparative text fit within the limits of a conference paper. My supervisor, Simone Fischer-Hübner, and I contributed to the structure and correctness of the text.

Paper IV I was the principal author of the paper and conducted all the 80 user studies. A discussion with my co-supervisor, Melanie Volkamer, led to the idea of this paper. Melanie Volkamer gave me feedback throughout the whole process and advised me on the structure of the user study. Nina Gerber conducted most of the statistical analysis based on what I described as hypotheses and variables defined to check them. Nina Gerber also contributed to writing the result section. My supervisor, Simone Fischer-Hübner, gave me valuable feedback and comments for all parts and contributed significantly in writing the introduction, analysis of legal requirements, and conclusion sections.

Paper V The results reported in this paper are the outcomes of the conducted studies by Daniel Lindegren for his master thesis. The idea for Daniel Lindegren's master thesis originated from a discussion with my co-supervisor, John Sören Pettersson, and I as part of the CREDENTIAL project. I consulted Daniel Lindegren for designing the UI prototypes and the user study to evaluate them. Daniel Lindegren designed the prototypes, conducted all of the user studies, and analysed the data collected from the user studies with Bridget Kane's help. I wrote the introduction, related work, methodology and study design, and conclusion sections. Daniel Lindegren and Bridget Kane provided the materials for the results and discussion sections which I reviewed, restructured, and elaborated. John Sören Pettersson was Daniel Lindegren's supervisor for his master thesis and provided valuable feedback on the paper.

Paper VI The initial idea of this paper on using eye-tracking to investigate people's attention to what data they disclose originated from a discussion with my supervisors, Simone Fischer-Hübner and John Sören Pettersson. I developed the idea further to see the effects of habituation, formed the research questions, designed a user study to evaluate them, conducted all of the 80 studies, analysed the results, and wrote the paper. Simone Fishcer-Hübner contributed in writing the ethics and the proposed design guidelines sections in the paper. My supervisors provided me with valuable feedback through the entire process.

Paper VII The idea of this paper originated from a discussion with my supervisors, Simone Fischer-Hübner and John Sören Pettersson. I was the main author, designed the study, and analysed the results. My supervisors gave me valuable feedback during the whole process. My co-supervisor, John Sören Pettersson, guided me in structuring and analysing the results and writing the conclusion section.

Paper VIII Eva Schlehahn introduced the idea of the paper as part of the SPECIAL project. Patrick Murmann and I designed the UI prototypes. All authors contributed to structuring and conducting a workshop to gain feedback on the designed prototypes and their underlying concepts. All authors took the role of either a note keeper or a moderator of a group in the workshop. I did a literature review and wrote the related work section. I contributed to the background section and provided content to the results section. Patrick Murmann added to the background section and wrote the methodology, results, and discussion sections. Simone Fischer Hübner wrote the introduction and conclusion sections and provided content for the results section.

Other Publications

- 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: *Trust Management X, Proceedings of the IFIP International Conference on Trust Management (IFIPTM)*, pp. 3–14. Springer, 2016. (Invited paper)

Simone Fischer-Hübner is the main author of the paper. I was a team member with Julio Angulo, and Tobias Pulls for implementing the *GenomSynlig* version of the Data Track and worked with Tobias Pulls for the latest stand-alone version of the tool. I conducted pilot tests for the latest stand-alone version of the Data Track tool and contributed by reporting the results of that for this paper.

- **Farzaneh Karegar**, Christoph Striecks, Stephan Krenn, Felix Hörandner, Thomas Lorünser, and Simone Fischer-Hübner. Opportunities and Challenges of CREDENTIAL: Towards a Metadata-Privacy Respecting Identity Provider. In: *Privacy and Identity Management. Facing up to Next Steps: Privacy and Identity, Proceedings of the IFIP International Summer School*, pp. 76–91. Springer, 2016.

I analysed and reported the data collected in the focus groups held at the IFIP Summer School (21–26 August, Karlstad, Sweden, 2016) to discuss research challenges concerning the trade-off between privacy, efficiency, and usability, end-user trust, and adoption factors identified for the CREDENTIAL project. I also wrote a section on why metadata privacy matters and discussed how metadata in the context of identity providers and data sharing might reveal more information, providing some examples.

- **Farzaneh Karegar** and John Sören Pettersson (eds.). UI Prototypes V1. CREDENTIAL Deliverable D3.1. Technical report, CREDENTIAL EU project, March 2017.

Besides editing, I was the principal author of two sections: i) task analysis of use cases in all three eGovernment, eHealth, and eBusiness domains, and ii) description of user interfaces (V1) and user evaluations in the CREDENTIAL project.

- **Farzaneh Karegar** and John Sören Pettersson (eds.). UI Prototypes V2 and HCI Patterns. CREDENTIAL Deliverable D3.2. Technical report, CREDENTIAL EU project, June 2018.

Besides editing, I was the main author of the HCI patterns section that, among others, presents the patterns for obtaining informed consent. I also contributed to designing and presenting the final UI prototypes and reporting their accessibility assessment.

- Tobias Pulls (eds.). Risk Management Artefacts for Increased Transparency. PAPAYA Deliverable D3.2. Technical report, PAPAYA EU project, July 2019.

I was the main author of the privacy-utility trade-off state of the art section that presents the results of a literature review on how to provide transparency and explanation on the underlying privacy-preserving algorithms.

- **Farzaneh Karegar**. Towards Improving Transparency, Intervenability, and Consent in HCI (Licentiate dissertation). Karlstad University Press. 2018.

Contents

Introductory Summary

"The most common way people give up their power is by thinking they don't have any."

Alice Walker
The Best Liberal Quotes Ever : Why the Left is Right — by William P. Martin (2004), p. 173.

1 Introduction

Since the birth of the Internet, the advancement of technology has augmented the collection, processing, and storage of personal data [57]. A massive amount of information is collected daily on individuals who are confronted with different media and services through various devices. The new information tools and technologies such as big data, machine learning, and data mining have leveraged online transactions and the consumption of collected personal data to a whole new level. The distributed nature of the Internet, technological complexities, and multiple data-exploiting practices make it difficult for people to gain control of their data and keep track of where their information is stored, to whom it is dispensed, and for what purposes it is used [85]. Moreover, information asymmetry and power imbalance exist between entities that process personal data, such as Service Providers (SPs) and individuals who may be affected by data breaches or other failures in the processing of their data.

Conceptually speaking, privacy can be defined as i) the right to be let alone, ii) limited access to the self, iii) secrecy, iv) control of personal information, v) personhood, and vi) intimacy [109]. Considering privacy as individuals' control of their data, Alan Westin, in his Privacy and Freedom, defines 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" [123]. Thus, the lack of control over personal data imperils individuals' privacy of personal information and their ability to make informed privacy decisions. The significantly low prices of collecting and analysing large amounts of data may lure service providers into collecting more data than necessary. Consequently, this lack of data minimisation leads to the misuse of personal data and making them vulnerable to privacy breaches [22]. Therefore, there is an increasing need for different societal, technological, and legal solutions addressing the challenges imposed by massive collection and processing of personal data and empowering users to take control of their data and making informed privacy decisions.

The General Data Protection Regulation (GDPR) [114] adheres to the principle of data subject control as a foundational concept for upholding informational self-determination and protection of personal data. In the GDPR, the need for individuals' control over their data, compared to earlier regulations, appears to be addressed more explicitly and with exceptional care [118]. The GDPR contains several references to the individuals' control. For example, it is mentioned that "natural persons should have control of their own personal data" (Recital 7, GDPR) [114]. Similarly, the idea of control over personal data in the GDPR appears in the increased transparency requirements for data collection practices of service providers, the stricter provision of consent, and the rights of the data subject. Consent represents one of the six legal bases of data processing. By consenting, an individual approves that his/her data can be used for one or more specific purposes. The rights of the data subject, referred to as subjective or control rights [68] or intervenability rights [48], can be divided into i) the rights to information and access to personal data; ii) the

rights to rectification, restriction, erasure, and withdraw consent; iii) the right to data portability; and iv) the right to object and object to the automated processing. The first category is the prerequisite for exercising other rights.

The GDPR continuously challenges service providers to adhere to the rules that aim to protect users' data privacy. Nonetheless, it raises the question of whether these rules yield improved user privacy in practice or whether they create more hindrances for users to understand and exercise their rights. Recently, two longitudinal large-scale empirical studies measured the actual impact of the GDPR on the web and privacy policies online [33, 66]. The percentage of websites with privacy policies has been growing, although the level of detail and delineation in the policies has increased, which has resulted in diminished readability and clarity [33, 66]. Both studies reveal a large gap that still exists between the current status quo and the ultimate goals of the GDPR that calls for further research in this regard.

The GDPR adopts a technology-neutral approach. Although the GDPR requires services to provide individuals with information regarding how their data are processed "in a concise, transparent, intelligible and easily accessible form, using clear and plain language" (Art. 12 (1), GDPR), it only specifies the *legal* requirements of consent, transparency, and intervenability, which, if appropriately obtained, can enable users to retain control of their data and protect their privacy. It is the reason why, despite the considerable attention given to data subjects' control in the GDPR, researchers still discuss and criticise the ability of the GDPR to address the threats to individuals' control of their data [118]. Researchers show that small design implementation decisions can impact whether and how people interact with consent forms and how they make choices [69, 117]. The results of the studies conducted by Utz et al. [117] and Machuletz and Böhme [69] on the design of cookie consent notices demonstrate the importance of providing clear guidance and design requirements for how consent must be obtained apart from its legal requirements.

The legal privacy requirements have Human-Computer Interaction (HCI) implications as they describe "mental processes and behaviour of the end user that must be supported in order to adhere to the principle" [86]. In other words, the answer to the question regarding how these HCI implications should be addressed depends on the attempts to decrease the gap between legal and user-centred transparency, intervenability, and consent. In the context of social media, Custers et al. [31] compare user expectations concerning privacy and consent with the EU legal framework for personal data protection and report that there is a disconnect between the legal provisions and concrete, practical implementations. We can argue—based on the research conducted by Pollach [88], Böhme and Köpsell [18], and Adjerid et al. [2] as some examples—that providing users with more transparency and control, without considering the disconnect between legal transparency and intervenability and the current practice in which users agree to almost every consent request [31], do not have the effect desired by lawmakers. Moreover, with the growth of invasive digital technologies and algorithmic decision-making, the challenges for control over data indeed become more significant [28].

Tsormpatzoudi et al. [115] emphasise the importance of involving end users in the "Privacy by Design" process, as the end users should ultimately profit from it. Moreover, Cavoukian emphasises that the "Respect for Privacy" principle of "Privacy by Design" extends to the need for User Interfaces (UIs) to be user-centred, and user-friendly [27]. Thus, apart from aiming for legal compliance, different ways to provide usable and user-centred transparency, intervenability, and informed consent are required, which can consequently enable users to take control of their data and make informed privacy decisions.

1.1 Objective

The objective of this thesis is to propose usable tools and solutions which improve user-centred transparency, intervenability, and consent, thereby empowering users to take control of their data and making informed decisions.

1.2 Structure

This thesis presents an introductory summary and a collection of eight papers in the area of improved transparency, intervenability, and informed consent to empower people to take control of their data. The remainder of the introductory summary is structured in the following manner: Section 2 provides the fundamental background for the work presented in this thesis. Section 3 outlines the research questions of this thesis, and Section 4 discusses the research methodologies applied. Section 5 presents the main contributions of this thesis followed by the related work in Section 6. Section 7 provides a summary of the appended papers. Section 8 concludes the introductory summary with a concise explanation of the results of this thesis with regard to the research questions and a brief discussion on future work.

2 Background

This section provides the necessary background to understand the topics under discussion and forms the foundations for the terms and concepts used in this thesis. However, the background information in this section is not intended to be exhaustive or elaborate, but rather to provide satisfactory definitions for readers.

2.1 User Empowerment in HCI

Schneider et al. [104] present a framework which aims to analyse the notion of empowerment in current HCI research. The framework is derived from analysing 54 CHI conference publications using the terms "empower" and "empowerment". The framework comprises four categories elicited from the prior work on the concepts of power and empowerment in social and political sciences as well as from design research in HCI. Schneider et al. utilise their framework to cluster their set of papers to unravel prevailing lines of research

on empowerment in HCI, which results in eight different lines of research including protective and self-enhancement technologies [104]. In the following section, we explain the four categories in Schneider et al.'s framework. In Section 5, we elaborate on how the appended papers of this thesis are clustered using this framework.

Concept of power: Schneider et al. report that there are two fundamentally different notions of power in literature: *power-to* and *power-over*. The former is about an ability to act and the latter concerns the power relationship between actors. In their framework, for the notion of power-to, Schneider et al. adopt the definition of Arendt who defines power as "something—anything—which makes or renders somebody able to do, capable of doing something. Power is the capacity, potential, ability, or wherewithal" [7]. With power-over, Schneider et al. refer to the Dahl's definition of power according to which "A has power over B to the extent that he can get B to do something that B would not otherwise do" [32].

Psychological component: The effect of empowerment varies greatly from the feeling of power to skill development or taking action [104]. Therefore, derived from Zimmerman's theory on psychological empowerment [126], Schneider et al. define three components—*feeling*, *knowing*, and *doing*—as the effects of empowerment. Although the components are, by definition, interdependent, Schneider et al. categorise their sample of HCI papers according to the effect of empowerment in the main focus of the papers.

Persistence of empowerment: Empowerment can be *transient* or *persistent*. Some technologies may expand users' knowledge and skills after and beyond using the system, while some tools and techniques empower their users only while the technologies are in use.

Design mindset: Schneider et al. adopt the distinction between an expert mindset and participatory mindset used by Sanders [98] to describe the design research landscape. Design researchers refer to people as "subjects", "users", and "consumers" in the expert mindset and "value people as co-creators in the design process" in the participatory mindset [98]. Schneider et al. argue that obtaining a balance between the two mindsets seems ideal as the view of ordinary people and the knowledge and competences of experts are both essential [104].

2.2 Transparency-Enhancing Tools/Technologies

High information asymmetry typifies the relationship between Internet users and SPs who collect user information [102]. Targeting at reducing the information asymmetry, Transparency-Enhancing Tools (TETs) increase the transparency for users in terms of more information, knowledge, and control of their data. Hansen defines TETs as "tools which can provide to the individual concerned clear visibility of aspects relevant to these data and the individual's privacy" [46]. Accordingly, while Privacy-Enhancing Tools (PETs) aim at data minimisation, TETs aim at providing users with insight into data handling behaviours. In addition to asserting the appropriate level of transparency, the

providers of TETs must assure that the TETs are secure and are not used against their end users [92].

Researchers propose different classifications of TETs based on various parameters [50, 52, 59, 80, 127, 128]. For example, TETs can be categorised into client-side, server-side, and trusted third-party based on their execution environments [127, 128]. Server-side TETs such as Google Dashboard allow authenticated users to receive information about collected and processed data. In a third-party TET such as the DataBait tool presented by Popescu et al. [89], the user trusts a third-party to have access to his/her data for providing transparency functions. Client-side TETs including Mozilla's Lightbeam[1] make the users' data transparent; these data are stored locally on users' devices under their control. From the usability perspective, client-side TETs may be more demanding to set up and their security is dependent on the security of users' devices. However, as users retain control of their data in client-side TETs, they are theoretically the more privacy-friendly solutions.

TETs can further be categorised based on the relationship between the time at which they provide users with transparency information and the time at which personal data are collected and processed by controllers [127]. Consequently, TETs can be classified as i) ex-ante TETs such as the Platform for Privacy Preferences (P3P) [29] and the PrimeLife Policy Language [6] which provide information to an end user prior to data disclosure to a service provider; ii) ex-post TETs such as A4Cloud Data Track [5, 16], Acxiom's AboutTheData portal[2], Datacoup[3], and DataSelfie[4] which provide data to the user after personal data disclosure to a service provider; and iii) real-time TETs such as some browser extensions including Mozilla's Lightbeam, Ghostery[5], and Privacy Badger[6] which provide transparency during data collection and processing, for example, by providing users with a real-time visualisation of companies that follow them on the Internet.

In this thesis, Papers I and II propose ex-post TETs that run on users' devices and Papers III–VIII investigate the methods to improve ex-ante transparency and consent.

2.3 General Data Protection Regulation

The GDPR [114] is a European legal framework intended to coordinate data privacy laws across European countries, protect the privacy of personal data, and transform the manner in which organisations approach data privacy. The GDPR has an extraterritorial scope and may apply to entities outside Europe that process the personal data of data subjects who are in the European Union "regardless of whether the processing takes place in the Union or not" (Art. 3 (1), GDPR). The European Data Protection Board (EDPB) provides guidelines on

[1] https://www.mozilla.org/lightbeam/
[2] https://www.aboutthedata.com/
[3] https://datacoup.com/
[4] https://dataselfie.it/
[5] https://www.ghostery.com
[6] https://www.eff.org/privacybadger

the territorial scope of the GDPR [35]. Two terms from the GDPR which are used repeatedly in this section are *data subject* and *controller*. The data subject is any identified or identifiable natural person to whom data are related, and the controller is the entity that determines the purposes and means of personal data processing.

In the GDPR, transparency is an explicit requirement and a core principle of data protection: pursuant to Art. 5 (1), personal data must be processed fairly, lawfully, and in a transparent manner. In Art. 12 (1), the GDPR obliges controllers to provide transparency: all information and communications concerning the processing of personal data must be provided to data subjects "in a concise, transparent, intelligible and easily accessible form, using clear and plain language" [114]. Requiring transparency as a precondition, consent provisions and intervenability rights aim to give users control of their data in the GDPR. In this thesis, in order to attain our objective (see Section 1.1), we attempt to address the HCI implications of the legal provisions for transparency, intervenability, and consent. Therefore, in the following subsections, we outline the legal principles of transparency, informed consent, and intervenability under different recitals and articles of the GDPR with the intention of describing the context rather than giving legal guidance.

2.3.1 Ex-ante Transparency and Informed Consent

Ex-ante transparency is a precondition for data subjects to be in control and for rendering consent (Art. 7 and 9, GDPR). In other words, before disclosing their data to different services, ex-ante transparency provides data subjects with the information which can aid them in making informed consent. Consent enables data subjects to authorise controllers to process their data. In the GDPR, the definition of consent in Art. 4 (11) expands the old definition of consent provided in the Data Protection Directive (DPD) and has stricter requirements regarding obtaining informed consent. However, there is a burgeoning doubt regarding the effectiveness of informed consent in the context of personal data processing [2, 18, 103] and the GDPR does not discuss what makes consent effective. The GDPR clarifies what should legally be provided to data subjects when giving consent. Nonetheless, it does not argue (and it is beyond the scope of the GDPR) to what extent data subjects are capable of providing informed consent and making conscious and autonomous choices, using legally compliant services. It is the role of ex-ante transparency tools and techniques to address these issues and help people provide informed consent.

Consent must be given by a clear affirmative action (Art. 4 (11), GDPR). According to Recital 32 of the GDPR, the affirmative action could include ticking a box or choosing technical settings or other statements which indicate the acceptance of the data subject of the proposed processing of his/her data. Thus, implicit and opt-out consent and particularly silence, pre-ticked boxes, or inactivity are presumed inadequate to confer consent. Consent must also be informed, unambiguous, freely given, and specific. According to the Opinion 15/2011 of Article 29 Working Party on the definition of consent [8] and

the Guidelines of Article 29 Working Party on consent under Regulation 2016/679 [10], to be specific, the scope and consequences of data processing in the consent must be clear and precise. To be freely given, there must be no risk of compulsion, deception, intimidation, or significant negative consequences if users do not consent. Doubt is removed from the procedure of providing consent by individuals, thereby making consent unambiguous. In other words, there must be no ambiguity regarding the data subject's intentions to provide consent.

Finally, in order to be informed, the GDPR obliges controllers to provide specific information to data subjects. There are several references to the articles and the recitals of the GDPR that add a few insights into the *informed* term: pursuant to Art. 13 (1) and as emphasised in Recital 42 of the GDPR, when personal data are collected from data subjects, e.g. in different consent forms, individuals must be made aware at least about what data will be collected and used, the identity of the controller, and the intended purposes of the processing of data. Further, according to Art. 13 (2) of the GDPR, the controller shall provide certain additional information to the data subject to ensure fair and transparent processing. Such policy information includes, but is not limited to, information of recipients/categories of recipients, the period for which the personal data will be stored and information of the existence of the right to withdraw consent at any time[7], access and rectify data, and data portability. Guidelines of Article 29 Working Party on consent under Regulation 2016/679 [10] also list the minimum content requirements for consent to be *informed* as certain crucial elements which are necessary to make a choice.

Apart from the legal requirements of consent, some researchers working on consent in the context of information privacy adopted the theory of informed consent [36] and considered how it could be applied in an online environment [39, 40, 76]. The most remarkable research study is that of Friedman et al.'s [39] model of informed consent in the context of online interactions. The model is aligned with the definition of informed consent subsequently developed in the GDPR. The model proposed by Friedman et al. is based on six components: i) Disclosure, ii) Comprehension, iii) Voluntariness, iv) Competence, v) Agreement, and vi) Minimal Distraction. Disclosure and Comprehension assure consciousness. Voluntariness, Competence, and Agreement constitute the consent. Moreover, the activities for informing users and helping them to provide their consent must happen with Minimal Distraction.

2.3.2 Ex-post Transparency and Intervenability

In addition to certain obligations regarding providing information when obtaining data from individuals, controllers are obliged to provide ex-post transparency. Ex-post transparency provides information regarding how personal data have been processed and is a prerequisite for intervenability—one of the

[7] Being informed of the right to withdraw consent at any time before giving consent is also mentioned in Art. 7 (3).

privacy protection goals. Intervenability "aims at the possibility for parties involved in any privacy-relevant data processing to interfere with the ongoing or planned data processing", as defined by Hansen [47]. For data subjects, the right to access personal data (Art. 15), the right to rectification (Art. 16), the right to erasure (Art. 17), the right to restriction of processing (Art. 18) as well as the right to object (Art. 21), the right to withdraw consent (Art. 7(3)), the right to data portability (Art. 20), and the right concerning automated decision-making including profiling (Art. 22) are all aspects of intervenability. Data subjects must be aware of the existence of intervenability rights and how to exercise them.

There are practical boundaries concerning how far ex-post TETs can actively assist data subjects in exercising their intervenability rights [79]. Nonetheless, ex-post TETs can still provide their users with information regarding how their data have been processed and guidance on the appropriate actions to take to intervene in the processing of their data. In this thesis, we implement two prototypical ex-post TETs which facilitate exercising intervenability rights for data subjects. In Paper I, the Data Track tool aims to facilitate exercising the right to data portability. In Paper II, privacy notifications help users decide if and how they need to intervene in the processing of their data based on the scenario. In the following account, we elaborate on the right to access, a prerequisite right for exercising certain other rights of the data subject, and the right to data portability.

The Right to Access (Art. 15) comprises the right to have access to the information regarding the data being processed, data processing purposes, and data recipients or categories of recipients. The right to access extends the information to be provided by the controller to include information regarding the data retention period, the right to lodge a complaint with the supervisory authority, and safeguards taken to transfer data to a third country. In addition, data subjects shall be informed about the existence of automatic decision-making, including profiling, and at least in those cases, the logic involved and the consequences of data processing. The data subjects shall also have the right to obtain a copy of their personal data which are being processed by the controller. If data subjects make their requests by electronic means, they shall be able to receive their copies of personal data in a commonly used electronic format.

The Right to Data Portability (Art. 20) provides both transparency and intervenability. It is the right to receive personal data regarding the data subject which are *provided by the data subject* to a controller and the right to transmit the data to another controller. The data subject has the right to have his/her data transmitted directly from one controller to another one where it is technically feasible. Without being specific regarding the format, the received data must be structured, commonly used, and machine-readable to ensure interoperability. The objective is to prevent data subjects from being locked into privacy-unfriendly SPs by providing the opportunity to change the providers and easily transfer their data. The Guidelines of Article 29 Working Party on data portability [12] elaborate on what exactly *provided*

data implies and which types of personal data fall or do not fall under the right to data portability. When requesting to exercise their right to data portability, data subjects must receive the data that are provided by them actively and intentionally [12]—for example, submitted via online forms. They must also receive observed data [12] which may, for example, include a person's search history, traffic data, and location data. Nonetheless, they may not receive derived and inferred data. The controllers are not obliged to include inferred and derived data as they are created by the data controllers on the basis of the data provided by the data subjects [12].

2.4 Challenges of Providing Consent

Privacy notices, generally speaking, are the different channels and means of conveying privacy policy information to users and the de facto means of informing them regarding the available opportunities to maintain control of their data. In other words, privacy notices are the conventional means to implement the paradigm of notice and choice. The notice is a presentation of terms, and the choice is an action that implies the acceptance of the terms. Privacy notices come in various forms and range from general privacy policy and consent forms to cookie consents and authorisation (permission) dialogues in the context of Identity Providers (IdPs) and mobile applications.

The status quo in different contexts indicates the ineffectiveness of consent forms and privacy notices [88]. Schaub et al. [100, 101] discuss the ineffectiveness of privacy notices and report the common problems which include notice complexity, lack of real choices, notice fatigue and habituation, and decoupled notices. Users simply provide their consent whenever the consent is requested [18]. Even if users intended to read policies, it would be practically impossible to spend hundreds of hours to read the privacy policies of the websites they visit every year. McDonald and Cranor estimated the total time for reading policies in 2008 [73]. The number would be much more significant if the study were replicated in the post-GDPR era, as more websites have privacy policies which are longer and more complicated according to the studies conducted in [33, 66]. In Section 6.1, we report and discuss work that attempts to solve the problem of ineffective consent forms.

In three particular circumstances (Art. 9, 22, and 49) where a high level of control over data is considered appropriate [10], the GDPR refers to "explicit" consent as a means to legitimise specific data processing. Nonetheless, in the GDPR, explicit consent is not separately defined. The Guidelines of Article 29 Working Party on consent under Regulation 2016/679 [10] state that the term "explicit" refers to the manner in which the data subject expresses consent. The data subject must provide an express statement of consent, for example, in a written and signed statement [10]. Similarly, the required express statement can be given by filling in an electronic form, sending an email, uploading a scanned document carrying the signature of the data subject, using an electronic signature, or a two-stage verification of consent [10]. Nonetheless, the requirement of obtaining explicit consent makes it more challenging to

design usable consent forms and request applicable express statements from users, depending on the context. Therefore, the HCI implications of obtaining explicit consent should be further studied in addition to the attempts to improve the effectiveness of consent notices to acquire informed consent based on the technologies at hand.

Consent holds a notable role in data protection as an indication of self-determination [34] and functions as an expression of individual autonomy. Eoin Carolan [25], aligned with Schermer et al.'s view on the active role of people in providing consent [103], argues that active consent not only requires users to make a choice actively but also assumes that the individual is capable of making a choice autonomously. Not surprisingly, there is growing scepticism over the active role of people, emphasised in the legal frameworks, in providing informed consent and the efficiency of consent as a legal ground for legitimate personal data processing. Schermer et al. argue that the legal requirements for providing and obtaining consent can be relaxed if different users in different societies have a common understanding of i) the actions or inactions constituting consent and ii) fair use of personal data [103]. However, privacy is a very complex concept which is dependent on the context, social norms, and specific individuals' characteristics; thus, obtaining a common understanding of consent and fair use of data to relax consent requirements is impractical. Nissen et al. [82] propose an alternative approach whereby users can opt to delegate consent decisions to an ecosystem of third-parties, including friends, experts, groups, and artificial intelligent entities. They present the results of a study that explores initial public responses to consent delegation. Their results reveal public interest in delegating consent and identify differing preferences depending on the privacy context. However, the proposal by Nissen et al. [82] relies on the offer of choice as the real agency of users and the users' ability to decide if and how to consent. Having more choices with regard to when to consent, when to delegate, and when to automate decision-making is itself a new challenge.

In this thesis, we refer to the requirements of consent in the current legal framework of the GDPR rather than attempting to suggest alternatives and replacement or reframing the concept of consent. Our work is not legal research but a study in the realm of usable privacy that aims to decrease the gap between legal and user-centred transparency, intervenability, and consent. Similar to Schaub et al.'s arguments regarding the role of privacy notices and choice [101], we believe that the problem is not fundamentally inherent in the requirements of control and transparency but in how we currently design notices and choice. Therefore, we adopt a neutral view on the effectiveness of active consent or autonomous authorisation model of consent and investigate the actual effects by involving users for whom the regulations must ultimately provide privacy protection.

3 Research Questions

As a stepping stone to attain the objective of this thesis, we address two research questions which are outlined in this section. Through the first research question, RQ1, we aim to investigate how usable transparency can help users intervene in the processing of their data. In the second question, RQ2, we seek to design consent forms in a usable manner which facilitate making informed decisions.

- **RQ1:** *How can we facilitate intervenability through usable transparency?*

To address RQ1, we investigate how ex-post transparency can be employed to help users intervene in the processing of their personal data using the TETs in Papers I and II. Paper I introduces a new version of a TET called Data Track which visualises exports of personal data and sheds light on what people think about data portability and how it can be exercised using TETs. In Paper II, we provide a proof of concept in the form of a prototypical implementation of a TET that facilitates usable transparency and intervenability based on privacy notifications. Paper II provides a set of validated design requirements for privacy notifications which inform their recipients of their intervenability rights and enable them to make informed follow-up decisions to improve their privacy.

- **RQ2:** *How can we design consent forms to enable users to provide informed consent?*

To address RQ2, we divided it into two sub-questions, each of which contributes to the design of usable consent forms but in different ways.

- **RQ2.1:** *How can we engage users with policy information, via different types of interaction techniques, in consent forms to enable them to provide informed consent?*

Obtaining meaningful and informed user consent is increasingly problematic in a world of various digital services. Current approaches to obtain informed consent usually provide users with a surfeit of information conveyed in long, jargon-filled texts that are difficult to comprehend and ignored by users [26, 67]. The GDPR, while specifying the legal requirements of consent and the need for affirmative actions, does not clarify the extent to which affirmative actions such as ticking boxes are effective for obtaining informed consent. Different interaction techniques which can serve as affirmative actions may influence the number of user actions and user memory of the content [112]. Consequently, we discuss RQ2.1 in this thesis in Papers III–VI.

In Papers III–VI , we propose HCI solutions to help users pay more attention to the actual data they disclose and conditions of consent by improving ex-ante transparency, engaging users with the consent forms, and thus improving the quality of providing consent. The consent forms we designed in Papers III–VI are the authorisation dialogues (permission dialogues) of identity

providers either on mobile phones (Papers III and V) or on desktop (Papers IV and VI). However, the methods employed to actively involve users apply to all circumstances in which users need to make a choice and agree to the processing of their personal information. We evaluate user attention to different policy information, including requested personal data, data processing purposes, and the conditions of consent. Consequently, our results are not restricted to the permission dialogues of identity providers; they can be extended to other consent forms such as the permission dialogues of browser extensions, mobile apps, and cookie consent forms.

Paper III investigates users' awareness and understanding of their personal data flow when they sign up for a service provider using an identity provider offering its services via a mobile app. The prototypes in Paper III utilise checkboxes to select the personal information, even that which is mandatory, to be shared. In Paper IV, we focus on widely used authorisation dialogues—Facebook Single Sign-On (SSO) authorisation dialogues—and propose HCI solutions to make the dialogues both legally compliant and effective for obtaining informed consent by engaging users with policy information. Paper IV utilises Drag-and-Drop (DAD) for data selection and the question-and-answer method to engage users with the conditions of consent. In Paper V, we propose and compare interfaces in which three different types of active selection of personal information—that is swiping, checkboxes and DAD—are utilised in the context of authorisation dialogues of IdPs on mobile devices. Finally, in Paper VI, we investigate whether user engagement with policy information, including personal data to be shared and data processing purposes, via different types of interactions plays a significant role in effectively drawing user attention to the content, even after repeated exposure. Paper VI compares the consent forms integrating interaction techniques with situations lacking active user engagement before and after becoming habituated to the designed consent forms. Contrary to Papers III–V, we measure user attention using both direct and indirect measures in Paper VI.

- **RQ2.2:** *How may the technologies at hand pose challenges in the provision of informed consent, and how can those challenges be addressed?*

Designing legally compliant systems which rely on consent for lawful data processing requires adaptation of consent by taking into consideration the characteristics of the technology at hand [41]. Different technologies bring particular challenges and demands for obtaining informed consent. Moreover, when the process is not transparent, nor is it possible to predict and stipulate the purposes before data disclosure, obtaining informed and unambiguous consent for specified data processing purposes would be challenging. Therefore, this thesis discusses RQ2.2 in Papers VII and VIII.

Using fingerprint recognition to confirm consent may pose new challenges in obtaining informed consent—including misunderstanding among users of their sensitive data flow first revealed in Paper III—particularly in the context of IdPs. Further, misunderstanding of access to authentication tokens may affect withdrawing consent. For example, to effectively exercise the right to

withdraw consent, users should not think that they are endangering a piece of their sensitive information to stop the processing of their other personal information if fingerprint recognition is used to confirm the request. Therefore, in Paper VII, we investigate people's perception of privacy and sensitivity of fingerprint data on mobile devices in the context of IdPs. We extend our investigation to see if the misunderstanding of the flow of fingerprint data stems from how fingerprint recognition is prototyped in our studies.

Online data services demand to change their data processing scenarios to create new products or services based on the characteristics of the available technologies. Nonetheless, such changes may pose new challenges to data services for obtaining informed consent from their customers. For example, using big data analytics, new types of information may be derived that could be utilised legally—if users provide their consent—for new purposes which were previously unforeseen. However, lengthy and barely comprehensible consent forms encompassing all possible future cases do not suffice to obtain informed consent from users in this context. Hence, in Paper VIII, we explore how the UIs for dynamic consent can be designed to facilitate repurposing in a specific use case. Dynamic consent, similar to the current practices of obtaining consent, may suffer from a couple of problems, including consent fatigue and habituation. To benefit from the potential advantages of dynamic consent, we must consider its HCI implications. Therefore, in Paper VIII, we extend our exploration to see how people perceive the concept of dynamic consent using our proposed UIs.

4 Research Methods

The work in this thesis belongs to the field of HCI. To answer our research questions, we employ quantitative and qualitative empirical HCI research methods. The methods employed consider users through the development cycles of the proposed and tested tools and solutions which, to a certain extent, follow a human-centred design approach [58]. Overall, the user studies in this thesis include both experimental methods and non-experimental methods comprising descriptive (or observational [71, p. 130]) methods [65]. Figure 1 represents an overview of the methodologies used in this thesis. In this section, we provide the methods used for each research question in detail and briefly explain the motivations for the choice of the methods. McGrath, in an influential paper on HCI research methodology, states that "all methods have inherent flaws, though each has certain potential advantages" [75, p. 154]. Therefore, we also briefly discuss the strengths and limitations of the methods exploited.

4.1 Methods to Address RQ1

RQ1 is an exploratory and broad research question which does not aim to identify the causal relationship between entities and events. Therefore, to address RQ1, we employ qualitative methods to explore users' attitudes, preferences, and understanding towards the transparency functions which aim to help users

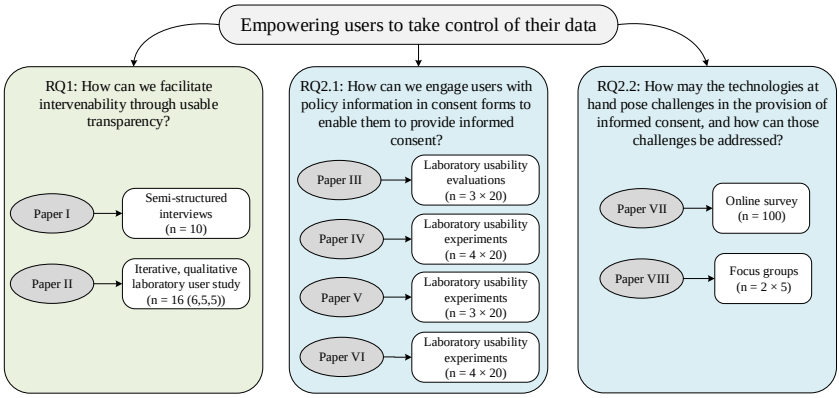

Figure 1: Overview of the methodologies used in the papers of this thesis for addressing the RQs.

exercise their intervenability rights. In the following section, we elaborate on the methods employed to address RQ1.

4.1.1 Interviews

Contrary to surveys, which are extensive but not profound, interviews can help obtain in-depth answers. Interviews are highly flexible in terms of structure. On the one hand, there are fully structured interviews with a firm script to present questions in a predefined order. On the other hand, there are unstructured interviews which may be based on a list of topics or questions to guide the interview [65]. However, if researchers want to avoid the challenges involved in conducting and interpreting the collected data from unstructured interviews, they can use semi-structured interviews. In semi-structured interviews, a few planned questions are asked, and other questions may emerge based on participants' answers and comments [65].

In Paper I, we conduct semi-structured interviews to study users' perception of transparency of data exports and their attitudes and preferences regarding data portability facilitated by the Data Track tool. The interview method is selected in Paper I because the aim is to investigate users' perceptions individually and in detail. Nonetheless, one of the shortcomings of the interviews is that the collected data are separated from the tasks and the context under question [65]. Consequently, interviews may cause the interviewees to suffer from the problems of recall. However, to reduce the effects of this drawback in Paper I, the semi-structured interviews are combined with other techniques—for example, role-playing. Interviewees are given a persona to role-play (see the details of role-playing as a facilitator for our studies in Section 4.4), a task to complete, and have the opportunity to work with the Data Track tool while answering the questions. During the interview sessions of Paper I, a moderator observes participants, a note-keeper takes notes, and the screen and voice are recorded for each individual to cross-check the data collected afterwards. Transcripts

from recordings are compared to notes taken during the studies to ensure the accuracy and comprehension of data collected. Transcripts serve as the input for data analysis that we conduct by grouping the codes representing similar concepts.

4.1.2 Qualitative User Study to Validate the Elicited Requirements

In Paper II, we extract a set of design requirements from the literature for TETs that run based on privacy notifications, present a prototype based on the requirements, and conduct an iterative and qualitative laboratory user study to evaluate the prototype and the requirements embodied by the prototype. Contrary to usability evaluations, our user study in Paper II does not aim to measure users' actions nor set a goal for them to achieve. The interaction with the prototype in our user study helps assess users' attitudes and feedback towards the implemented transparency functions required to facilitate intervenability in a TET that operates based on privacy notifications. The design and evaluation of the proposed prototype to validate the requirements employ the characteristics of human-centred and participatory design [58], as the process utilises the feedback of representatives of the target audience. We iteratively integrate the feedback into the prototype for three iterations. We stop after the third iteration, as we receive no new feedback on what can be realistically addressed by further changes in the prototype.

4.2 Methods to Address RQ2.1

To address RQ2.1, we design prototypes of the consent forms which integrate different ways of engaging users with policy information. We then compare and evaluate the effectiveness of the prototypes to enable users to provide informed consent. To evaluate our proposed consent forms, we expose users to our prototypes in experimental and non-experimental laboratory usability studies, and we measure their experiences, including their attention to policy information. User attention is a prerequisite to being informed and grasping the content. We measure and compare the usability of the proposed design solutions and quantitatively and qualitatively collect data regarding the user experience in our usability studies. Moreover, we test our proposed designs against habituation.

In the remainder of this section, we briefly elaborate on the usability studies conducted to address RQ2.1, including how we measure the efficiency and effectiveness of the proposed designs, and user satisfaction.

4.2.1 Usability Studies

In Papers III–VI, we conduct usability studies following the guidelines in [96] to evaluate our proposed prototypes of the consent forms engaging users with their contents. The ideas of Papers IV–VI originate from the results of the non-experimental study in Paper III in which the aim is to unravel the usability issues of the proposed UIs, drive further development, and understand the

potential utility of the proposed interfaces to users. The evaluation in Paper III serves as the basis for the experimental laboratory studies in Papers IV, V, and VI in which we make inferences regarding the differences among conditions.

In this thesis, a typical usability study session consists of introducing the study with a cover story, obtaining participants' consent, asking them to complete a pre-test questionnaire before tasks, asking participants to complete a set of tasks role-playing a persona using a prototyped UI, handing them a post-test questionnaire after completing the tasks, debriefing, and compensating the participants. Usability evaluations are selected because individuals' feedback, attitudes, and perception regarding the proposed interfaces and concepts in question are required. Moreover, the usability study is relatively simple and straightforward. To complement the usability studies, we combine them with other methods, such as questionnaires and post-test interviews. The inclusion of other methods also helps us infer certain conclusions from the participants' verbal opinions and the observations made by the test moderators. For elaborated descriptions of the user studies conducted in this thesis, please refer to Papers III–VI.

To measure usability, we adopt the usability definition of ISO 9241–210 provided in [58] in which usability is the "extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use" [58].

Hornbæk [55] summarises usability factors measured in HCI studies published in core related journals and proceedings. In the literature, as shown by Hornbæk [55], the prevailing measures of effectiveness include binary task completion, accuracy, recall, completeness, quality of outcome, and expert's assessment. Effectiveness is measured using the recall of information in Papers III–VI and notice adherence in Paper VI, as the indirect manifestation of user attention to policy information. Information recall indicates the extent to which users can remember the data items they share and notice adherence is the extent to which users reject or accept the consent request based on its critical content. In other words, notice adherence in Paper VI is a self-reported measure that shows whether a user has paid attention to the critical content (e.g. sensitive data shared or dubious data processing purposes) and confirmed consent. However, recall scores may not necessarily reflect user attention to the policy information since they depend on memory capacity as well, particularly for specific items visited for a short time.

Consequently, to complement the data obtained through subjective, self-reported measurements, we use eye-tracking data as the behavioural manifestation of user attention. We compare the effectiveness of different consent forms to draw user attention to their policy information, even after repeatedly exposing users to these consent forms—that is after habituation.

Habituation is a mental state which is difficult to be observed with conventional methods like notice adherence [20]. Researchers show that eye-tracking is a valid measure of the mental process of habituation to security warnings [119]. Moreover, a few studies demonstrate that with successive viewings of security warnings, users' visual sampling decreases [3] and that cross-sectional habitua-

tion studies are valid proxies for longitudinal studies [119]. Thus, in Paper VI, we use eye-tracking to measure the decrease in user attention and as a means to detect habituation.

In the literature, efficiency is mainly measured by time (e.g. task completion time), input rate, mental efforts, usage patterns, communication efforts, and learning [55]. Fifty-seven percent of the HCI studies included in Hornbæk's survey [55] measure time in terms of task completion time. Task completion time is also used to measure efficiency in this thesis.

Finally, satisfaction is primarily measured in the literature by standard questionnaires, preferences, satisfaction with the interface, and users' attitudes and perceptions [55]. Although certain studies use standard questionnaires for measuring satisfaction or build directly upon previous work for questions on overall users' satisfaction, numerous researchers use their own satisfaction measures [55]. Using existing scales, which are examined and re-validated by other researchers, advances the state of the art and disengages researchers from developing their own measurement instruments [91]. In Papers III–VI, we employ the SUS questionnaire [21] to measure the overall usability and satisfaction in the context of identity providers for two reasons. First, among the other validated questionnaires, the SUS has been selected and used in hundreds of usability studies [13] and there are also a large number of reviews and evaluations of its effectiveness, strengths, and weaknesses [14, 116]. Second, Ruoti et al. [97] report that the SUS questionnaire produces reliable and replicable results for web authentication systems and they recommend that the usability of the new authentication systems be formally evaluated using the SUS scale.

4.3 Methods to Address RQ2.2

Similar to RQ1, RQ2.2 is a broad research question which focuses on the challenges of obtaining informed consent with the emergence of new technologies. It also explores the potential solutions to the problems that surface. To address RQ2.2, we conduct qualitative and quantitative methods. In the following section, we elaborate on the methods employed to address RQ2.2.

4.3.1 Questionnaires and Surveys

Surveys are fundamentally used to ask a well-defined and well-written set of questions, of a sample of people from a population, to explain, explore, and describe that population [38]. Surveys are rather easy and cheap methods to collect data from a large number of people. However, they cannot provide in-depth and detailed data [65]. Although interesting concepts may appear in users' answers, it is not possible to ask follow-up questions which can investigate more about the concepts in surveys. Consequently, careful considerations are required for inappropriate, ambiguous, or biased responses. Moreover, questions—both open-ended and close-ended—should not be redundant, biased, and incomprehensible, and the number of questions should not cause fatigue among respondents [51]. The terms surveys and questionnaires are often

used interchangeably. Nevertheless, they may be occasionally differentiated—questionnaires may be defined as a list of questions and surveys may be defined as a complete methodological approach that includes questionnaires as one of their elements apart from, for example, sampling and incentives [65]. This thesis differentiates between self-administrated, electronic questionnaires and surveys and moderator-supervised questionnaires and surveys combined with usability tests and user studies to collect more data from users and help avoid misinterpreting questions as participants have the opportunity to interact with the moderator.

In Paper VII, we conduct a self-administrated, electronic questionnaire—that is an online survey to measure attitudes and self-reported behaviours. Participants are assigned to one of the four groups in the survey. After watching a video prototype, they answer a few questions, including related questions to the scenario shown in the video. To avoid respondent fatigue, we keep the number of questions small and the duration of the video prototypes short. The average duration of our video prototypes in Paper VII is 83 seconds.

As previously discussed in Section 4.2.1, our usability studies are combined with other data collection methods. In this thesis, moderator-supervised questionnaires are used in combination with the user studies conducted in Papers III–VI in order to measure participants' experience and capture their opinions of various aspects in the user studies. Both existing questionnaires[8] to collect data on subjective topics and researchers' own questions to collect data on more objective topics are used in Papers III–VI.

4.3.2 Focus Groups

The focus groups, similar to the interviews, help elicit perceptions, information, attitudes, and ideas from a group of participants [65]. Nonetheless, the distinguishable factor between a focus group and a one-to-one interview is capturing participants' ideas and attitudes through group interactions [110]; one participant's reaction to a topic in question elicits another one's response. Focus groups depend on dynamic interaction to provide the information sought [64] and an active role of the researcher in creating group discussion for data collection [77]. Focus groups can provide major insights into attitudes, beliefs, and opinions [24]. However, focus groups can silence individual disagreeing opinions [64] and a few participants may dominate the discussion [110], which accentuate the critical role of a skilled and vigilant moderator to conduct the focus group.

In Paper VIII, we are mainly interested in receiving feedback concerning the conceptual aspects of dynamic consent. Therefore, we involve domain experts rather than laypersons to evaluate our prototype. The workshop conducted in Paper VIII is a hybrid between a focus group and a cognitive walkthrough. It is a focus group because its fundamental purpose is to gauge opinions and attitudes regarding the high-level concept of dynamic consent in the context of

[8] We used the SUS to measure the overall usability and satisfaction and the IUIPC questionnaire [72] to measure the participants' privacy concern level.

repurposing the processing of personal data. We encourage a lively discussion among the participants to achieve as much feedback as possible. The study in Paper VIII also presents the features of a cognitive walkthrough. We use a paper mockup[9] to weigh whether the order of the operation steps of the prototype designed can help people understand the concept of dynamic consent.

4.4 Facilitators for Conducting Our User Studies

Cover stories. In Papers III–VI, we use cover stories to prevent participants from being primed for the actual objective of the studies. We do not want to prime our participants for privacy and attention to the content of the consent forms that we design. In other words, we want to avoid non-realistic attention due to the study setup. Therefore, the actual purpose is carefully and ethically obscured, both during the recruitment phase and during interactions with participants in the study sessions. Participants may form certain interpretations of the goal of the study and change their behaviour accordingly, which is called demand characteristics [84]. We use cover stories to reduce the effects of the cues that may reveal the real goal of the study to participants and become significant determinants of their behaviours.

In Paper II, we use the term "cover story" to refer to the introductory story that we tell our participants to set the scene and to provide a common ground for the prototype that the participants experience. Thus, the cover story we use in Paper II does not disguise the purpose of the study.

Role-playing. In four of the papers included in this thesis (Papers I, III, IV, and V), participants role-play a persona to complete their task(s). Participants receive a few instructions about the task(s) and the persona they are required to role-play on a role-playing card. Using a persona has two main reasons: i) it enables full control of what each participant encounters, providing a standard experience that can be compared among participants and ii) due to ethical reasons, it helps to avoid handling participants' sensitive information which has to be disclosed for the study, such as birth dates or page likes on Facebook in Paper IV and their locations over a period of time in Paper I.

Role-playing may affect the generalisability of the results achieved from user studies. For example, in our studies, the recall scores might differ in each group if participants used their own accounts. However, role-playing does not affect the results obtained from the comparison of different test groups of participants (between-subject studies in Papers III–V) in this thesis. Moreover, in Paper I, the task defined for participants and the persona required to complete the task serve as the starting point of discussing the interview questions. Role-playing the persona while performing the tasks, in Paper I, provides all participants with a common ground and enables them to have a better insight into the meaning of downloading data from an SP and uploading the same data to another party. Nevertheless, the task is not used to measure the effectiveness

[9] A mockup looks quite similar to a prototype. However, it is a graphical representation that is not interactive and not clickable.

of the UIs (Google archive managing interfaces in Paper I) or to time the participants for efficiency.

Prototyping. Prototyping enables designers to check their ideas with users and to obtain feedback [90]. Prototyping is achieved using different techniques, tools, and materials, ranging from paper, pens, and cardboards to wireframes and more advanced programming languages [23]. Prototypes are classified based on their levels of complexity and detail (e.g. paper-based low-fidelity versus computer-based high-fidelity prototypes) [121]. Some research compares user testing with low and high-fidelity prototypes and reveals that low-fidelity prototypes are also good at uncovering usability issues [99, 121]. The results of the usability testing conducted by Walker et al. also demonstrate to be independent of medium, despite differences in the interaction style [121]. Consequently, in this thesis, the medium and the level of fidelity are selected based on what suits the practical needs and design goals for prototyping.

In this thesis, several high-fidelity prototypes have been created and tested with real users under varying conditions. In Paper I, the goal is to present a stand-alone, open-source TET that users can download on their computers to visualise their data exports. The prototype evolved over various incremental and evolutionary iterations of pilot tests. The prototype of the latest stand-alone Data Track tool described in Paper I is a high-fidelity, completely interactive prototype implemented to run in a browser using HTML, CSS, JavaScript, and some JavaScript libraries (e.g. Leaflet for interactive maps).

In Paper II, the goal is to emulate the behaviour and look of a native mobile app as accurately as possible. We use a combination of HTML/CSS/JavaScript, and the jQueryMobile framework to implement a high-fidelity interactive prototype in the form of a rich mobile application. During our studies in Paper II, the prototype ran in a standard Firefox web browser on an Android phone.

To test the design concepts for consent forms presented in Papers III–V, we create different interactive prototypes with a rapid prototyping tool: Axure software. The prototypes of different consent forms in Paper VI are high-fidelity prototypes that run on Chrome browsers and are designed using Bootstrap and JQuery libraries to test the effects of interaction techniques on user attention, before and after the habituation trial.

In Paper VII, to better communicate the scenarios in question and reveal the entire corresponding experience to the participants of our online survey, we use video prototyping. We make four different video prototypes, using Adobe After Effect and Photoshop, based on the types of the IdP in the scenarios and the authentication tokens to confirm the consent forms.

Finally, in Paper VIII, we design a click-through prototype, using the Balsamiq tool, which is an example of how the concept of dynamic consent could be implemented. However, we use the printed mockup in our focus groups as our objective is to discuss high-level concepts rather than detecting usability issues.

4.5 Participants in Our User Studies and Limitations

Generally speaking, we recruited people for our studies via word of mouth, a few mailing lists, posters pinned on the public bulletin boards of various faculties of Karlstad University and at public places at the city centre, and posting on several Facebook pages related to Karlstad city and university. However, in this section, we do not aim to provide exhaustive and detailed information on how we recruited our participants in each paper of this thesis, as the relevant information can be found in the appended papers. Alternatively, we briefly argue who and how many participants, in general, we recruited in our user studies and the corresponding limitations. Participants took part in the studies of this thesis individually and voluntarily. Nonetheless, volunteer participants have numerous discrepancies with the general population, indicating to be, for example, more well-educated, more intelligent, and of higher social class [95].

We did not limit our recruitment by only asking for student participants; nonetheless, most of our participants were connected to academia, including a large number of undergrads and graduate students, some administrators, and a few lecturers. However, we attempted to exclude people with computer-related backgrounds as much as possible and had participants from various other fields of study.

Barkhuus and Rode [15] report that approximately half of the studies in their sample of papers from the ACM CHI conferences over 24 years were conducted with either undergraduates or graduates students. Similarly, Sjøberg et al. [108] report that 81 out of a sample of 113 articles on software engineering used students. Nonetheless, Hornbæk [56] argues that reflecting on the characteristics of the participants may be of much greater significance in comparison with having student participants in an experiment which may not matter to a study. We acknowledge the limitation of our sample of participants. Despite our attempts to obtain a balanced sample of participants regarding age and gender, we have a relatively young sample of participants with females outnumbering males. However, we argue that it does not severely affect the results obtained from the comparison of different groups in Papers III–VII.

Guest et al. report that saturation occurs within the first twelve interviews, although essential elements for meta-themes are present as early as after six interviews [44]. Guest et al. discuss that as long as the aim is to understand common perceptions and experiences among a group of relatively homogeneous individuals, twelve interviews should suffice. Therefore, in Paper I, we recruit 10 participants because we observe that no new themes surface after interviewing the eighth participant.

In Paper II, we conduct an iterative user study to validate our set of requirements. We recruit 16 participants in total in the course of three iterations since, after the third iteration, we reach a demonstrable level of maturity. In each iteration, we recruit five to six participants. A small number of participants can still help recognise a considerable number of problems in a prototype [81].

In Papers III–VII, we have four different groups, and we stop the recruitment process once we have at least 20 in each group. Hornbæk [56] argues that the pragmatic answer to the question regarding the number of participants that

must be included in HCI studies is approximately 20 participants. Similarly in a critical review of psychology experiments, Simmons et al. [107] recommend 20 persons per condition because samples smaller than 20 per cell are simply not sufficiently powerful to detect most effects [107].

The recommended number of people per group varies for focus groups. For example, MacIntosh suggests six to ten participants [70], while Kitzinger believes that the ideal group size is between four to eight people [64]. In our workshop presented in Paper VIII, we receive a total of ten participants. To help the moderator to have better control over the discussion and provide our participants a better opportunity to interact with each other and express themselves in a limited time, we divide our participants into two focus groups with five participants in each group. Aiming to maximise the exploration of different perspectives, we distribute the participants evenly between the two groups according to their backgrounds. We obtain different results regarding the concept and usefulness of dynamic consent from the two groups of our study.

4.6 Ethics

As discussed previously in Section 4.4, we use cover stories in the studies of this thesis. Bortolotti and Mameli [19] argue that it is possible to use deceptive methods without causing severe harm to participants. In Papers III–VI, participants are not deceived in a manner that they experience an utterly irrelevant study compared to the one to which they are introduced. However, the main objective regarding privacy and attention to data sharing is disguised. The objective is presented as a study of testing the usability of a website, in Papers III–V, and a study of rating a few photos from different websites based on the hashtags assigned to them, in Paper VI, both of which are a part of what participants accomplish.

Although we employ cover stories, all necessary steps have been taken to adhere to the Swedish Research Council's principles of ethical research in the appended papers of this thesis [120]. This includes obtaining informed consent, not using participants' actual or sensitive data to complete the tasks, and debriefing participants at the end of the study. Furthermore, we applied for ethical approval for user studies conducted in Papers II and VIII. Our external co-author informed us about the ethical approval for Paper VIII and we were not involved in the process of applying for it. The study in Paper II is conducted after the official enforcement of a new decision at Karlstad University requiring all research projects to be ethically reviewed before the commencement of the project. Therefore, although none of our studies falls under the provisions of the Act concerning the Ethical Review of Research Involving Humans (2003:460) [1], our study in Paper II is ethically evaluated at the Faculty Ethics Review Group. Nonetheless, seeking ethical approval from the Research Ethics Committee has not been required.

Table 1: The appended papers of this thesis (except Paper VII) coded with the Schneider et al.'s framework [104].

	Concept of Power		Psychological Component			Persistence of Empowerment		Design Mindset	
List of Papers	Power-to	Power-over	Feeling	Knowing	Doing	Transient	Persistent	Participatory	Expert
Paper I		✓		✓	✓	✓			✓
Paper II		✓		✓	✓	✓			✓
Paper III	✓			✓	✓	✓			✓
Paper IV	✓			✓	✓	✓			✓
Paper V	✓			✓	✓	✓			✓
Paper VI	✓			✓	✓	✓			✓
Paper VIII	✓			✓	✓	✓			✓

5 Contributions

This thesis contributes to the body of knowledge on designing to empower users through usable transparency, intervenability, and consent. In this section, first, we cluster the appended papers through the lens of Schneider et al.'s framework [104] (see Section 2.1 for more details concerning the framework). Then, we present the partial contributions, made in Papers I–VIII, which reflect the general contribution of this thesis. The partial contributions comprise the empirical and artefactual contributions and contributions in the form of design guidelines. All three types of contributions are depicted in Figure 2 at the end of this section.

5.1 Contributions Coded Through the Lens of the Schneider's Framework

The overview of our papers (except Paper VII) clustered using Schneider et al.'s framework is presented in Table 1. We exclude Paper VII, as it does not propose concrete solutions for counteracting the issues revealed regarding users' understanding and attitudes towards the use of fingerprint recognition to confirm consent requests. If users were provided with appropriate UIs conveying the information regarding the privacy of fingerprint recognition in Paper VII, the concept of power would be classified as "power-to", manifest as "knowing", be "persistent", and be designed using either mindset dependent on the methodologies exploited. In the following account, we elaborate on how the appended papers of this thesis are clustered using the Schneider et al.'s framework.

Concept of power: Apart from the primary effect of gaining the ability to control personal data, which is similar to the notion of power as "power-to", decreased power imbalance is the after-effect of achieving the objective of this thesis, which is similar to the notion of "power-over". Nonetheless, to cluster our work based on Schneider et al.'s framework, we distinguish between tools and techniques which should be provided by service providers (Papers III–VIII, excluding Paper VII) and the stand-alone TETs that enable users to visualise and maintain control of their data (Papers I and II). The concept of power in the former group is classified as "power-to" and in the latter group as "power-over".

Psychological component: In the appended papers to this thesis, except for Paper VII, the effect of empowerment can be classified as both "knowing" and "doing". In this thesis, the proposed tools and solutions empower users to keep control of their data by informing them about their personal data processing in a manner that leads them to make related informed privacy decisions and taking action. Nonetheless, taking action in certain circumstances—such as exercising intervenability rights directly in the ex-post TETs proposed by Papers I and II—have practical limits, as discussed in Section 2.3.2.

Persistence of empowerment: User empowerment over their data in Papers I–VIII, excluding Paper VII, is categorised as transient rather than persistent. The information users gain while handling the consent forms in Papers III–VI and Paper VIII, or utilising the TETs in Papers I and II, is case-sensitive and specific for individual scenarios. In other words, when a user responds to a consent form, the information conveyed may not necessarily empower him/her to make an informed consent in another situation or context. However, it may lead to more reflected and proactive behaviour in general and, therefore, facilitate empowerment persistently.

Design mindset: In the appended papers of this thesis, the initial version of the tools and techniques proposed are the results of the expert mindset. However, the evaluation methods employed consider users through the development cycles of the proposed and tested design solutions.

5.2 Artefactual Contributions

In the field of HCI, the artefactual contributions are systems, techniques, or design inventions initiated as, for example, prototypes, sketches, mockups, or demos and are often at least partially functional [124]. The outcome and contributions of the empirical evaluations accompanying the artefacts of this thesis are reported in Section 5.3. In summary, the artefactual contributions of this thesis comprise prototypes and mockups of usable TETs and consent forms designed to empower users to take control of their data; these contributions are listed below:

1. *Prototype of TETs facilitating intervenability through transparency*

   The Data Track tool is an example of a TET that provides users with visualised information regarding the personal data they have disclosed to different service providers under specific agreed-upon policies. In Paper I, we present a prototypical implementation of the latest standalone version of the tool that helps users visualise their data exports and facilitates exercising the right to data portability as an intermediary tool when users wish to transfer their data between services. The tool is a proof of concept contributing to addressing RQ1 by showing how usable ex-post transparency functions can aid data portability in the form of a TET running as a desktop tool under users' control.

   In Paper II, to validate our design requirements elicited from the literature, we provide a prototypical implementation of a TET. The prototype

is a proof of concept contributing to addressing RQ1 by showing how usable ex-post transparency can facilitate intervenability in the form of a TET that runs based on privacy notifications. The designated target platform of the tool is the user's smartphone. We design three privacy notifications as the central part of the prototype considering our proposed design requirements, where applicable. The notifications aim to provide users with sufficient guidance to make informed follow-up decisions about the processing of their health data.

2. *Prototype of consent forms engaging users with content via different interaction techniques*

   In Papers III–VI, we design a few consent forms which engage users with policy information. The consent forms serve as a proof of concept contributing to addressing RQ2.1 by revealing how different existing interaction techniques, including checkboxes, DAD, and swiping actions can be adapted and integrated into consent forms to engage users with different policy information—that is to select what to share for which purposes.

   In Paper III, we present the mobile prototype of authorisation dialogues of an IdP which engages users with policy information, using checkboxes. When users are confronted with an authorisation request, they select mandatory information and, if desired, some optional information to be shared with a service provider and confirm their consent using their fingerprint.

   In Paper IV, we move one step forward towards designing the effective consent forms engaging users with policy information and design desktop authorisation dialogues leveraging both DAD and the question-and-answer method. DAD is used to engage users with the personal information they disclose as a response to the consent request. The question-and-answer method is used to actively engage users with the policy information concerning the conditions under which they provide their consent. At the second step, after selecting the personal data to be disclosed, users answer to a few policy questions based on the policy information provided to them and check their answers until they provide the correct response to each question. In cases where the wrong answers are provided, the correct answers are shown to the users who must select the right answers and recheck them.

   In Paper V, we provide the prototypes of mobile authorisation dialogues of an IdP which leverage different interaction techniques—comprising DAD, swiping, and checkboxes—to engage users with the personal information they select to disclose. The prototypes proposed in Paper V complement the design in Paper III. Other policy information required for a consent to be informed, including data processing purposes, is provided to users as part of the consent request in Papers III and V. However, users do not necessarily engage with them using any interac-

tion techniques unless they proactively pay attention to the provided information.

Finally, in Paper VI, we design the prototypes of desktop authorisation dialogues of an IdP which employ DAD, swiping, and checkboxes to engage users not only with the personal information to be shared but also with the data processing purposes for each of the selected personal information. The prototypes presented in Paper VI complement the design in Paper IV. Other necessary policy information, including the right to withdraw consent, is provided to users as part of the consent request.

In Papers IV–VI, we adapt the suggestion by Pettersson et al. to use the Drag And Drop Agreements (DADAs) [87] as an alternative way to express consent. In Paper IV, users have to drag the items individually and drop them to a single shared destination embedded for all data requested. In Paper V, each draggable item has a single area for dropping, providing no other option. Contrary to Papers IV and V, users select where each draggable item should be dropped among available options in Paper VI, which may help users pay more attention to what they drag and where they drop it.

The swipe action integrated into consent forms in Paper VI is different from the swipe action in Paper V that is used on mobile devices. Although it is possible to accomplish the swipe action in Paper V via a mouse, it specifically targets touchscreen devices. Moreover, the swipe action in Paper V does not necessarily involve users with text. To highlight text, Paper VI slightly adapt the swipe action suggested by Bravo-Lillo et al. [20] by adding an arrow and combining it with a slider. Our slider-like design provides users with more control of data selection compared to standard text selection highlighting with a mouse.

3. *Prototype of dynamic consent forms for a commercial use case*

   In Paper VIII, we present a prototypical implementation that facilitates incremental consent forms based on dynamic consent. The prototype contributes to addressing RQ2.2 by indicating a potential solution for the challenge of acquiring consent for repurposing the processing of newly derived data in a commercial use case in the context of big data analytics. To develop our prototype, we assume that dividing bulky traditional privacy policies into multiple smaller parts requires less cognitive effort to read and understand.

5.3 Empirical Contributions

Empirical contributions are new findings based on systematically gathered data and the results of empirical research methods commonly used in HCI, such as formal experiments, interviews, focus groups, surveys, usability tests, and case studies [124]. Empirical contributions in HCI reveal, for example,

formerly unknown insights into human behaviour concerning information or technology [124]. In summary, the empirical contributions of this thesis comprise the analysis of users' ability to provide informed consent and exercise their intervenability rights using usable ex-ante and ex-post TETs proposed in this thesis.

1. *Illumination of people's perception of transparency of data exports and the concept of data portability*

   The results obtained from the evaluation of users' perception of the transparency functions of data exports and the concept of data portability in Paper I contribute to addressing RQ1. Users appreciate the transparency functions available in the Data Track tool. However, Paper I reveals a few HCI challenges that remain to be addressed. In particular, Paper I confirms the problem of users' perception of control of their data and understanding of locally and remotely stored data, an aspect previously reported in [5, 37], even while exercising their right to data portability. As reported in Paper I, benefits of the right to data portability and the usage scenario are unclear for participants. Nevertheless, when informed, they express their positive attitudes towards the stand-alone version of the Data Track to function as an intermediary tool which they can use to visualise (and edit) their mobile data between services. While exercising their right to data portability, participants are willing to select the method which provides them with more control of their data, even if it is not as efficient as the other methods.

2. *Evaluation of the effectiveness of different interaction techniques and their robustness to habituation*

   We conduct different user studies to evaluate the effectiveness of the prototypes we designed to actively engage users with policy information both on mobile (in Papers III and V), and desktop (in Papers IV and VI). The results of the evaluations partly address RQ2.1.

   Paper III reveals that users tend to maintain control of the data requested to be shared. Studies conducted in Paper III reveal that users prefer to select even mandatory information themselves and not to have them selected by default. This tendency indicates that speed is not always users' priority and can be explored as a means of slowing users down and cause them to reflect more. Moreover, the results of the user study in Paper III show the potential of a confirmation screen to contribute to the improvement of users' recall of what they shared.

   In Paper IV, users are actively interacting with the authorisation dialogues of social logins using DAD and the interactive question-and-answer method. The proposed interfaces of authorisation dialogues help users have a better recollection of what they shared under which conditions and decrease the level of uncertainty compared with the current practice of social logins.

Paper V demonstrates that although speedy checkboxes do not engage the user as much as DAD or swiping on mobile devices. Users who experience DAD and swiping in the consent forms have a slightly better recollection of the data they share. The different design patterns for engaging users with content have an impact on the perceived usability of the designs. The results of Paper V reveal that young users (below 30) handle the consent forms more quickly than others. Nonetheless, the time to handle the consent forms and the extent to which users recall the data they shared do not significantly correlate with each other.

The results of Paper VI show that different types of interactions may affect user attention to certain aspects of policy information. In particular, the DAD action results in significantly more user attention to the data items compared to other tested interaction techniques. However, it does not necessarily help draw user attention to data processing purposes compared to other interaction techniques in Paper VI. With repeated exposure to consent forms, the difference in drawing user attention to certain policy information disappears. In other words, users learn how to manage their time and resources to handle consent forms more effectively and efficiently.

3. *Analysis of people's perception of and challenges with using certain technologies and methods of providing consent*

   In Paper VII, we first discuss the importance of appropriate comprehension of the privacy of fingerprint data and its potential effects on obtaining and withdrawing consent. Then, we report the results of an online survey conducted to investigate different people's (users and non-users of fingerprint sensors and those who are familiar and non-familiar with IdP technologies) understanding of privacy of authentication tokens (both fingerprint data and PIN codes) in the context of IdPs and their attitudes regarding the sensitivity of fingerprint data.

   Based on the results of Paper VII, we conclude that the misconception of the privacy of fingerprint recognition is not the result of faking fingerprint-scanning in the prototypes—that is clicking on an icon on the screen instead of using the fingerprint sensor on the mobile phone. Moreover, our results reveal that non-users of fingerprint recognition tend to be more anxious about third-party access than users are, and users tend to regard fingerprint pattern as more sensitive than non-users do. In addition, the results of Paper VII disclose that people who believe that fingerprint patterns are not very sensitive can have very different grounds for their judgement. The outcome of our investigation in Paper VII contributes to addressing RQ2.2 and unravels different users' attitudes towards the privacy and security of fingerprint recognition used to confirm consent on mobile devices. Although Paper VII does not provide concrete design guidelines for usable user interfaces that provide information concerning security and privacy of fingerprint sensors, the reported users' perceptions and attitudes enable system and UI designers

to accommodate the needs of different groups of people.

In Paper VIII, we investigate the experts' understanding of our dynamic consent forms and discuss the implications for future directions, which empirically contribute to addressing RQ2.2. Our evaluation indicates that not all experts easily understand our approach involving alternative paths for obtaining dynamic consent. However, the experts who understand how we implement the concept of dynamic consent appreciate the incremental consent requests. Our evaluation confirms that the dynamic way of requesting permissions from the data subject must be accompanied by actionable choices—that is meaningful ways to exercise intervenability rights and the privacy consequences of taking action. In Paper VIII, based on the feedback we received, we discuss that incremental consent requests have the potential to more accurately describe the context and increase user control if passably designed.

5.4 Design Guidelines

The design guidelines provided by this thesis comprise a set of design requirements and recommendations. Paper II provides design requirements for TETs that operate based on privacy notifications. Paper VI presents design recommendations on engaging users with policy information in consent forms via different types of interaction techniques. Our contributions in the form of design guidelines can be categorised under empirical contributions, as they are based on and are supported by the results of systematically analysing data collected through the conduct of empirical research methodologies. Nonetheless, the guidelines arguably go beyond the empirical results as they are not achieved purely based on analysing the data collected in empirical studies.

In Paper II, we present a set of validated design requirements for privacy notifications which inform users about how their personal data are processed and guide the privacy decisions they make regarding how to intervene in the processing of their data. The final set of requirements presented in Paper II contributes to addressing RQ1 and reflects the four interaction phases conceptualised in [78] for privacy notifications: configuration, delivery, presentation, and intervention. However, our time and resource constraints make it hard to conduct longitudinal studies and simulate the real-world environment to investigate the delivery of notifications. Therefore, we exclude validating the delivery requirements and focus on investigating how the presentation of notifications can facilitate intervenability. The configuration requirements indicate the ability of users to configure and control the behaviour of a TET running based on privacy notifications. The presentation requirements specify how information should be presented to users using privacy notifications. Finally, the intervention requirements support users in terms of reacting to a privacy notification by exercising the rights of the data subject.

Based on the results of the experimental usability studies in Paper VI, we derive a few design recommendations on how to utilise the interaction techniques studied in Paper VI to engage users with policy information in consent forms. We recommend designers to carefully select interaction techniques to engage users with policy information considering the context of use and the potential biases that the use of different techniques may create in user attention to different aspects of policy information in a consent form. Paper VI suggests that uniform consent forms with identical layouts across different services could train users to attend to the right pieces of information. The design recommendations in Paper VI partially address RQ2.1.

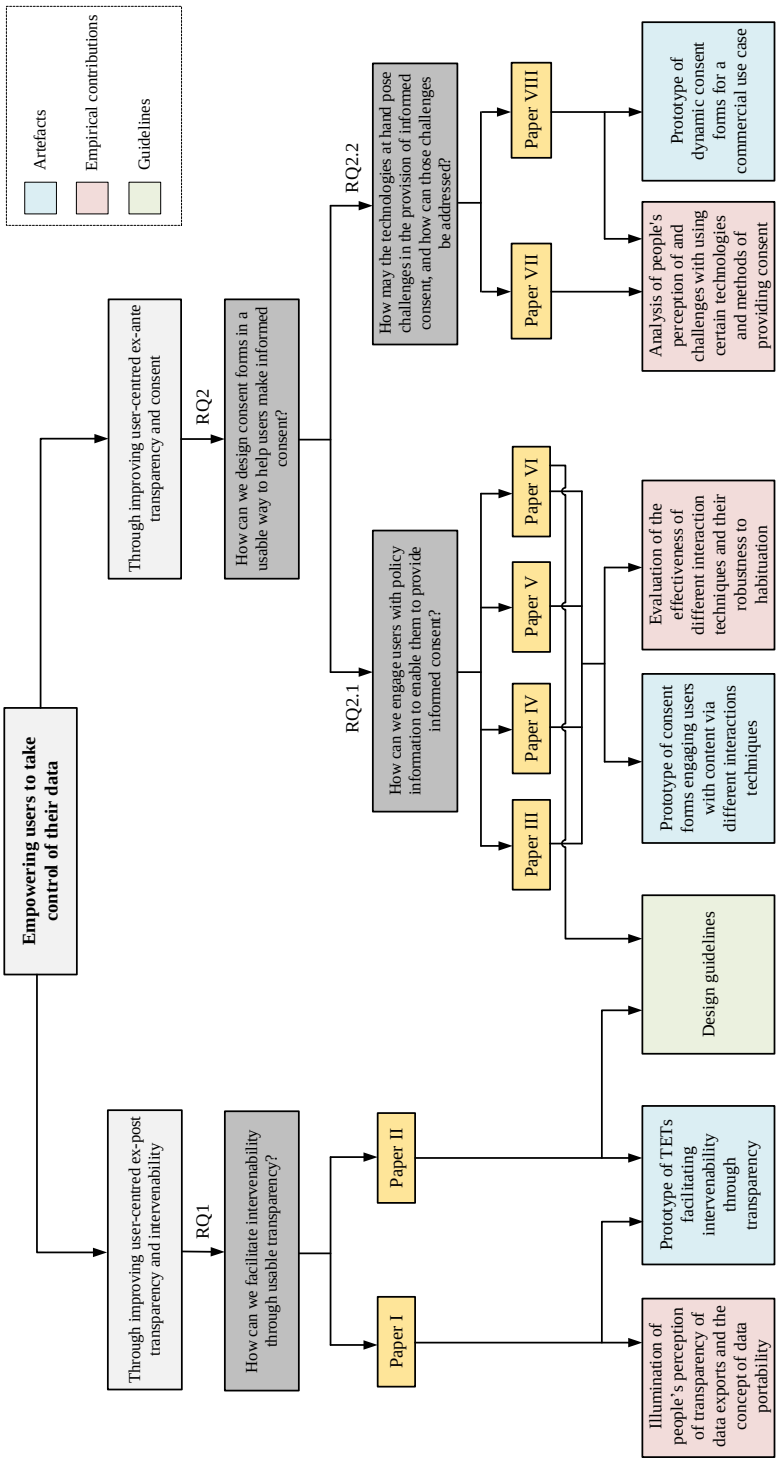

Figure 2: A summary of the contributions of this thesis.

6 Related Work

In this section, we complement the description of the related work in the appended papers with updated information. We concisely describe the studies related to enhancing ex-post transparency facilitating intervenability and the studies on improving ex-ante transparency and consent forms facilitating making informed consent. This section also briefly shows how this thesis advances the state of the art.

6.1 Improving Ex-ante Transparency and Informed Consent

As concisely outlined in Section 2.4, researchers have proposed different solutions to solve the current issues with consent and privacy notices. One approach to solving the problems related to privacy notices and consent forms is to make incremental improvements to the corresponding user interfaces, for example, by modifying the information provided to users and how to provide the information. The modifications aim to help users pay attention to the content, which may consequently help them become informed and make better decisions. Recent studies on cookie consents show that the design elements used in consent dialogues affect consent choices [83] and may deceive users into agreeing to more data processing purposes than the purposes they initially intended to agree [69]. Researchers have proposed privacy nutrition labels [63], multi-layered short notices summarising key data practices [9, 11, 42], personalised privacy notices [49, 125], polymorphic notice design [3, 4], visual attractors [20], privacy icons and images [30, 53], and comic-based interfaces to convey policy information [113]. However, the proposed methods all come with their own hurdles. For example, providing information in a compact form may impair transparency [74]. Moreover, the meaning of privacy icons may not be easily and uniquely understandable by all people due to cultural differences [53].

To solve the problems related to privacy notices, a few researchers adopted another approach and studied improvements to how users interact with the content of notices—for example, by actively involving them with the content using checkboxes [122] and swiping action [20]. Literature that does not focus on privacy also supports the idea that different interaction techniques can influence the number of user actions and user memory of the content [112]. The emphasis on informed consent in the GDPR [114] which should be given by clear affirmative actions also augments the importance of investigating how different interaction design solutions serving as affirmative actions in consent forms are effective in helping users pay attention.

In this thesis, we adopt the second approach towards contributing to solving the problems of consent. In Papers III–VI, the effectiveness of consent forms in the context of IdPs is improved by adjusting the active and conscious role of users in interacting with consent forms. Papers III–VI, contrary to previous studies in the context of IdPs, investigate the effects of actively involving users in consent forms along with fulfilling legal requirements. Apart from the

reported effectiveness of the proposed solutions on improving users' awareness of data sharing, Papers III–VI present the effects on the time to finish the relevant users' tasks and their satisfaction.

We complement Table 1 of Paper V, which depicts an overview of research on engaging user attention with content through different interaction techniques, by adding Paper VI to the comparison presented in Table 2. The interaction techniques utilised in this thesis originate from reviewing the literature on privacy and security notices (e.g. [20, 112]). Table 2 reports the results of studies in Paper VI before the habituation trial. Paper VI complements the previous works outlined in Table 2 by using both direct and indirect measures of user attention and investigating if and how the effectiveness of different design solutions changes under repeated exposure to consent forms. In Paper VI, we take certain steps to avoid having the same limitations found in the existing literature on habituation to privacy and security notifications [20, 60].

Javed et al. [60] and Bravo-Lillo et al. [20] use the rejection of disclosing sensitive information as a manifestation of not getting habituated to notices. Nonetheless, the information researchers consider as sensitive may not be regarded as sensitive by users. Moreover, in both studies conducted in [20, 60] users are continuously and uninterruptedly exposed to notices without having a primary task, which is not consistent with what happens in real-world situations. Participants in Paper VI have some primary tasks to do during the habituation trial—rating a photo after accepting a dialogue better simulates real situations.

In the following account, we briefly describe the studies conducted in the first three rows of Table 2. Bravo-Lillo et al. [20] investigate the effects of visual attractors for computer security warnings on user attention to the essential information, the salient field, for making decisions. The visual attractors compromise purely visual and inhibitive attractors, such as swiping and type actions that actively engage users with the salient field. The salient field includes either a suspicious or a benign installation request. The effectiveness of attractors on user attention is measured by the rate of reduction in installation for suspicious scenarios relative to benign scenarios. However, the rate of cancelling suspicious dialogues is affected by other factors such as lack of willingness to fulfil the request in the dialogue or lack of vulnerability feeling. If users could detect that the suspicious request was fake and safe they might not take it seriously. The results reveal that warnings with inhibitive attractors are more time-consuming to handle for participants, although they lead to a higher reduction in installation rates [20].

In the context of permission dialogues of IdPs, Wang et al. [122] suggest enabling users to control their data by deselecting what they do not want to share using checkboxes. Wang et al. [122] provide pre-selected checkboxes for requested personal data and the possibility to opt out of the optional ones in their proposed interfaces. Pre-selected checkboxes do not require a clear affirmative action and, thus, do not constitute a valid consent (Recital 32, GDPR). Wang et al. observe that people who use the checkbox-enabled interfaces release significantly less information overall and utilise granular

choices to opt out from specific data collection compared to the participants who use control permission dialogues that lack any options. However, Wang et al. do not measure if their proposed new interfaces increase user attention to what a user shared.

Sundar et al. [112] compare six different types of interaction techniques—namely click-to-download, dragging, hovering, sliding, zooming in and out, and flipping—in the context of informational websites on desktop. Their results support the theoretical assumptions of the model of interactivity effects [111]; certain interaction techniques—for example, sliding—are better than others to affect learning outcomes such as content recall positively.

6.2 Usable Ex-post Transparency Facilitating Intervenability

The latest stand-alone version of the Data Track tool, described and studied in Paper I, and the TET that runs on the basis of privacy notifications in Paper II are just two examples among many other ex-post TETs designed, implemented, and occasionally evaluated in various research. Murmann and Fischer-Hübner [80] reviewed 24 ex-post TETs which at least present implementation in a prototypical stage or an evaluated mockup. Only five of the ex-post TETs reviewed in [80], including the Data Track tool in Paper I, either—in theory—provide the opportunity for users to exercise (some) intervenability rights [5, 17] or provide functionalities which have the potentials to facilitate intervenability [61, 89]. For example, Kani-Zabihi et al. [61] introduce "Privacy Enquiry", a communication channel to the data controller, which functions as an online chat to allow users to express privacy concerns promptly. However, it is susceptible if this mechanism could also be used by data subjects to issue a request to exercise their intervenability rights.

The implementations of the privacy dashboards presented by Bier et al. [17] and Angulo et al. [5] work similarly with regard to how disclosed personal data are visualised. Data Track presented by Angulo et al. [5] and PrivacyInsight presented by Bier et al. [17], display derived data when technically feasible. Moreover, these two works discuss GDPR legal privacy rights and enable data subjects to exercise their legal rights to rectify and erase data. Subsequently, Raschke et al. [94] implement and evaluate a privacy dashboard that acts as an interface between the data subject and the controller which theoretically facilitates the execution of certain intervenability rights similar to two earlier proposed privacy dashboards presented in [5, 17]. Raschke et al. [94] apply a generalised version of the data taxonomy provided by [105] in their visualisation and offer separated views for each data category. Their expert evaluation with three participants reveals that the current version of their dashboard and the classification of data types do indeed help people find out what information is collected about them; however, their evaluation also indicates that their data classification needs to be refined based on comprehensive user studies.

Murmann and Fischer-Hübner discuss that although intervenability goes beyond transparency, TETs should inform and guide data subjects in exercising their intervenability rights [80]. However, only a few TETs currently available

Table 2: Overview of research on interaction techniques to engage user attention with content [Adapted table from Paper V].

Study	Context	Type	Measurement method for user attention	Results		
				Effectiveness: User attention	Efficiency: Time	Satisfaction: SUS score
[20]: Swipe & Type inhibitive attractors	Security warnings: Desktop	Online exp.	Rate of reduced installations in suspicious relative to benign scenarios	Inhibitive attractors resulted in a higher reduction in the installation rates.	Inhibitive attractors take more time.	—
[122]: Pre-selected checkboxes	Permission dialogue for IdP consent: Desktop	Online exp.	Counted data items released & opt-out actions	Users of checkbox-enabled interfaces release less information & opt out from some data collection.	—	—
[112]: Click, Slide, Zoom, Hover, Drag, & Flip	Informational website: Desktop	Lab. exp.	Recall of website information	Improved content recall depending on interaction technique.	—	User assessment & power usage correlated in various methods.
Paper III: Checkbox, Confirmation screen plus checkbox	Permission dialogue for IdP consent: Mobile	Lab. exp.	Recall of personal information shared	Confirmation screen helps improve information recall.	Reports Mean time to handle checkbox interfaces. Implies longer time for confirmation & checkboxes.	Good SUS scores for both types of interfaces.
Paper IV: DAD & pre-selected checkboxes	Permission dialogue for IdP consent: Desktop	Lab. exp.	Recall of personal information shared	DAD helps users recall information they share and reduces their uncertainty.	DAD interfaces are more time-consuming.	DAD interfaces have lower SUS values, within the acceptable range.
Paper V: Checkbox, Swipe, DAD	Permission dialogue for IdP consent: Mobile	Lab. exp.	Recall of personal information shared	DAD and Swipe give slightly better Recall values.	Checkboxes take slightly less time than Swipe or DAD. Swipe & DAD have almost the same completion time.	All earn good SUS scores: DAD scores highest SUS; Swipe scores lowest.
Paper VI: Checkbox, Swipe, DAD, Control group lacking active selection	Permission dialogue for IdP consent: Desktop	Lab. exp.	Recall of personal information shared, notice adherence, and eye-tracking	DAD gives significantly better Recall values compared to control group, no evidence of a difference between the other pairs.	The type of user engagement did not affect the time. But a lack of active user engagement significantly decreased the time.	Control group received the highest SUS (though no significant effect of the type of consent forms on SUS scores).

provide access to functionality to analyse the data and related information for exercising intervenability rights [80]. Even researchers who explicitly discuss the intervenability rights of erasure and rectification in their proposed TETs do not argue about the practical limits of ex-post TETs in terms of how far they can actively support data subjects and the technical and legal challenges of developing intervenability functions in their TETs.

In this thesis, the version of the Data Track tool in Paper I, to the best of our knowledge, is the first TET that attempts to visualise data exports in a usable way and facilitates the right to data portability by visualising data exports. Users can import their data exports requested from a service provider to the Data Track, visualise their data in different usable views, edit their data, and then transfer them to other services, if feasible in practice. However, the Data Track tool in Paper I does not discuss the solutions for visualising and exploring combined data exports from multiple services which have its own challenges. Recently, Schufrin et al. [106] presented the TransparencyVis tool, which is a web-based prototype to unify and visualise data exports from different online services.

A few authors have investigated the problems that users face when they attempt to delete data [45, 93], opt out from unsolicited advertisements [45], or manage cookie consents [117]. Nonetheless, Paper II, for the first time discusses users' expectations of how they would like to be guided and exercise their rights in a TET and the corresponding implications on the design and implementation of TETs. The TET in Paper II is a proof of concept of how users can be guided in exercising their intervenability rights through privacy notifications. In Paper II, we discuss that users will be able to experience usable transparency and intervenability if service providers and TETs go hand in hand. Nevertheless, ultimately, it is the service provider who can heed the user's choice.

7 Summary of Appended Papers

Paper I – Visualizing Exports of Personal Data by Exercising the Right of Data Portability in the Data Track—Are People Ready for This?

A transparency-enhancing tool called Data Track has been developed at Karlstad University. This paper reports on a user study that investigates the perception of a new function visualising exports of personal big data for the data subjects, which we added to the latest stand-alone version of the tool. To analyse the users' perception of Data Track and its transparency features as well as the concepts of data export and data portability, we conduct a qualitative user study in which users experience the latest stand-alone version of the tool. We observe that although users have little interest in the visualisation of derived data activities revealed in the Google location file, they are interested in other kinds of derived data, such as movement and travel patterns, usage patterns for different service providers, statistical data based on their behaviours, and information about to whom their data are disclosed, how their data are exchanged, and how

they might receive related advertisements. Moreover, we confirm that it is confusing for users to differentiate between locally and remotely stored and controlled data. Finally, despite being concerned regarding the security of the data exported to their machines, for exercising the right to data portability under the GDPR, most participants prefer to first export and edit their data before uploading them to another service provider. Users appreciate Data Track for being of aid in this context. Users would like to be in control when exercising the right to data portability. In other words, they do not prioritise the convenience of having their data transmitted directly from one controller to another one if it is technically feasible. In the future, we would like to extend the tool to visualise data exports of other service providers and to expand its functionality to support users in all the steps involved in exercising their right to data portability.

Paper II – From Design Requirements to Effective Privacy Notifications: Empowering mHealth Users to Make Informed Decisions

Currently, only few usable tools exist to provide users of online data services with the transparency of how their personal data have been processed and advise them regarding making informed decisions of how to intervene based on the information obtained. Privacy notifications can facilitate said functionality for the usage context of personal health tracking by accommodating user needs for the ecosystem of mobile phones. To address the lack of concrete design requirements for implementing usable tools, we elicit a set of design requirements from the literature, implement a prototype, and conduct a qualitative, iterative lab study to evaluate the efficacy of the requirements immanent in the prototype. The study targets active, former, and prospective users of mhealth services ($n = 16$), and elicits qualitative feedback to evaluate the prototype in three iterations. This iterative process yields a proof of concept in the form of a prototypical implementation of a TET which shows how privacy notifications can be implemented suitably as well as a set of revised design requirements that reflect the results of the evaluation. The concept of privacy notifications and the overall functionality of the prototype are received positively. However, the test subjects prefer additional empowerment in terms of being able to take immediate actions. The findings obtained during the evaluation of the prototype lead us to believe that privacy notifications have the potential to provide users of mobile devices with customised, situational awareness of matters concerning the processing of their data and enable them to make informed follow-up decisions to improve their privacy. Moreover, the set of evaluated design requirements can provide designers with the principles necessary to leverage privacy notifications to implement respective functionality.

Paper III – User Evaluations of an App Interface for Cloud-based Identity Management

CREDENTIAL is an EU-funded Horizon 2020 project that involves developing, testing, and presenting cloud-based services to manage digital identity

information and personal data with a higher level of security than existing technology. The CREDENTIAL Wallet is the central component of the tools developed in this project, and it supports users with its functionalities in a mobile application acting as an identity provider and a data access manager. The user interfaces of this app can be used to evaluate general questions concerning people's understanding of and preferences for providing consent and their appreciation of more privacy-friendly single sign-on solutions than what is currently offered to the general public. In this paper, we conduct usability studies for the prototype of the CREDENTIAL mobile app as an identity provider. The goal of the conducted studies is twofold: to assess i) users' consciousness of data disclosures and flow of data in authorisation dialogues (consent forms), and ii) users' understanding of authenticating to service providers and authorising service providers to access personal data in the context of identity providers accessible via mobile apps. The study encompasses a set of three user tests made of the core functions of authorisation and authentication. Results show that using a person's fingerprint for giving consent is easy, but most participants do not have a correct view of which entities may have access to their fingerprint data. Familiarity with identity apps appears to aggravate misunderstanding. In addition, the results reveal that it is not easy for our participants to recall the details of personal data releases and settings for disclosure options. An evaluation with a confirmation screen suggests that the confirmation screen slightly improves recall rates and can be a default option in authorisation dialogues. Our participants voice a desire to have control of their data and express a wish to be able to manually select mandatory information, which can be a means of slowing users down and cause them to reflect more. However, effective ways of unobtrusively slowing users down to reflect more are subject to future work.

Paper IV – Helping John to Make Informed Decisions on Using Social Login

Users need to make two privacy-related decisions when subscribing to a new web service: i) whether to use an existing SSO account of an identity provider and ii) the information the identity provider is allowed to share with the service provider. From a privacy perspective, the use of existing social network-based SSO solutions (i.e. social login) is not recommended. However, this recommendation is accompanied by drawbacks regarding security, usability, and functionality. Thus, in principle, it should be up to the user to consider all advantages and disadvantages of using SSO and to consent to requested permissions, provided that the user is well informed. Another issue with existing social login sign-up interfaces is that they are often not compliant with legal privacy requirements of informed consent and "Privacy by Default". Accordingly, our research focuses on enabling users to make informed decisions and provide consent in this context. To this end, we identify users' problems and usability issues from the literature and through an expert cognitive walkthrough, and we elicit end-user and legal privacy requirements for UIs that enable users

to provide informed consent. We utilise this input to develop a tutorial for informing users about the pros and cons of sign-up methods. We also use this input to design SSO sign-up UIs for enabling informed consent, following the approaches of human-centred and privacy by design by addressing user requirements and legal privacy requirements from the beginning and throughout the UI development cycle. We test both the tutorial and the UIs in a between-subject laboratory study with 80 participants. The results indicate that the tutorial notably helps users improve their knowledge about the advantages of options they have for sign-up; however, more investigations are required to ideally communicate the advantages and disadvantages of services that may threaten users' privacy. For our newly developed UIs, informed consent is enforced with the help of the active involvement of users via DAD and the question-and-answer method. The results reveal that the new UIs are significantly more effective in helping users to provide informed consent than the current authorisation dialogues of the social network. In conclusion, affirmative actions such as DAD that require users to carefully check opt-in choices to be made as well as interactive knowledge testing and feedback are examples of effective HCI concepts for UIs that enable users to provide informed consent.

Paper V – An Evaluation of Three Designs to Engage Users when Providing Their Consent on Smartphones

In this paper, we contribute to decreasing the gap between requirements of informed consent and the design of user interfaces for consent dialogues. We investigate three interactive techniques—namely DAD, checkbox, and swiping—that actively involve users in the process of providing consent via permission dialogues of IdPs on mobile devices. The interaction techniques may differ in terms of how users perceive them and the cognitive efforts they require. Therefore, the interactive techniques utilised in this paper, which facilitate users to select personal information actively, are compared in terms of their usability and effectiveness to help users be more attentive and aware of their data flow. We report on three user studies with 60 participants in total ($n = 3 \times 20$), each conducted to test a specific interactive design option. The results reveal that checkboxes, while speedy, do not engage users as much as DAD or swiping. Different interface designs have an impact on perceived usability. Younger adults are, in general, faster in handling the permission dialogues and providing their consent than mature adults (over 30). However, the fact that we are unable to demonstrate a relationship between the time for the task and participants' information recall rates prompts further investigation; does spending more time on a design also imply more attention to essential items on the dialogues? In such studies, direct methods to measure attention, like eye-tracking, must be used.

Paper VI – The Dilemma of User Engagement in Privacy Notices: Effects of Interaction Modes and Habituation on User Attention

Privacy notices and consent forms are the means of conveying privacy policy information to users. Valid consent needs to be confirmed by a clear affirmative action (Art. 4 (11), GDPR). Despite previous research, it is not yet clear whether user engagement with consent forms via different types of interactions for confirming consent plays a significant role in effectively drawing user attention to the content, even after repeated exposure. We investigate, in a laboratory study, how different types of interactions which engage users with consent form contents differ in terms of their effectiveness, efficiency, and user satisfaction. Moreover, we examine if and how habituation affects user attention, satisfaction, and the time they spend on providing their consent. We conduct a controlled experiment with 80 participants in four different groups where people are either engaged actively with policy information via DAD, swipe, or checkboxes or are not actively engaged with the content (as the control condition) in a first-exposure phase and a habituation phase. We measure user attention to consent forms along multiple dimensions, including direct, objective measurements and indirect, self-reported measures. Our results show that the different types of interactions may affect user attention to certain aspects of policy information. In particular, the DAD action results in significantly more user attention to the data items compared to other groups. However, with repeated exposure to consent forms, the difference disappears. It appears that during the habituation trial, users learn how to manage their time and resources to respond to the consent requests more effectively and efficiently. Thus, uniform consent forms with identical layouts across different services could train users to attend to the right pieces of information. We conclude that user engagement with policy content needs to be designed with care so that attention to substantial policy information is increased and not negatively affected. Based on our results, we also derive a few design recommendations in this paper.

Paper VII – Fingerprint Recognition on Mobile Devices: Widely Deployed, Rarely Understood

Misunderstanding of who has access to authentication tokens affects obtaining and withdrawing consent, particularly in the context of IdPs. In this paper, we conduct an online study—an Internet-based survey with 100 participants—to investigate individuals' perception of privacy of fingerprint recognition on mobile devices and the sensitivity of fingerprint data. Our work contributes to the body of knowledge by reporting and discussing i) people's perception of entities which have access to and control of authentication tokens (i.e. fingerprint biometric data and PIN codes) in the context of IdPs, ii) the differences in attitudes towards privacy and sensitivity of fingerprint data among people who use the fingerprint technology on their devices and others, and iii) people's subjective opinions about the degree of sensitivity of fingerprint data and their justifications of their answers. This study also reveals that when we do not aim

to measure the exact characteristics of user interaction with fingerprint sensors, we can use a simplified prototype in which clicking on an icon on the screen serves as a proxy for fingerprint recognition on mobile devices. In addition, our results show that self-estimation of knowledge in Computer Security is not a good indicator of respondents' understanding of fingerprint security and privacy. Our results obtained from investigating users' perception of access to and storage of fingerprint data as sensitive data (i.e. the perception of privacy) and users' opinions regarding its security can help system and UI designers address user problems in this context.

Paper VIII – Opportunities and Challenges of Dynamic Consent in Commercial Big Data Analytics

In the context of big data analytics, the dynamic demands of online data services are changing the scenarios related to the processing of personal data. Such changes may pose challenges with regard to legal requirements such as transparency and consent and, therefore, call for novel methods to address the legal and conceptual issues that arise in its course. We define the concept of "dynamic consent" as a means to meet the challenge of acquiring consent in a commercial use case that faces a change for repurposing the processing of personal data to implement new data services. We present a prototypical implementation that facilitates incremental consent forms based on dynamic consent. We report the results gained via two focus groups which we used to evaluate our design, and we derive implications for future directions of research from our findings. Our expert evaluations show that not all experts easily understand our approach involving alternative paths for obtaining dynamic consent. Nonetheless, those that understand how the concept of dynamic consent is used in our scenario also appreciate the approach of incremental consent requests. This dynamic way of collecting or altering user permissions should come along with meaningful ways to exercise the intervenability rights. In particular, the UIs of dynamic consent should provide users with direct access to functions for easily revoking a previously given consent, when a request to extend this consent appears dynamically. Future directions for the design of dynamic consent should address these results of our expert evaluations.

8 Conclusion and Future Work

Aiming to increase individuals' control of their data, the GDPR enhances the transparency requirements for data collection practices and empowers data subjects with certain rights. Despite these enhanced rights of the data subject, users have little or no control over who uses their data and for what purposes, which consequently imperils the privacy of their personal information. Therefore, apart from aiming for legal compliance, HCI implications of the legal privacy rights and requirements must be considered to make them effective in terms of enabling users to maintain control of their data in practice. Consequently, this

thesis investigated how to design usable tools and solutions which improve user-centred transparency, intervenability, and consent.

First, to facilitate intervenability through improving user-centred ex-post transparency and address RQ1, we designed, implemented, and tested two ex-post TETs. Moreover, we provided a set of validated design requirements for implementing TETs that run on the basis of privacy notifications. We revealed that users appreciated the functionality and transparency provided by our proposed TETs. However, our research unravelled a few challenges that need to be addressed should intervenability be facilitated through usable transparency provided by client-side ex-post TETs.

Based on the commonality of the results achieved with regard to users' attitudes, understanding, and concerns related to the functionality and information provided by our proposed TETs, we conclude that users of client-side TETs will not always be able to differentiate between the tool itself and the data service for which it provides transparency. They appreciate simplicity and efficiency but not at the expense of lack of control of their data. Users want comprehensible and straightforward, yet complete, information while exercising their rights. They expect to have additional empowerment in terms of taking immediate actions provided in TETs. In addition, easy and simple ways of exercising intervenability rights must simultaneously assure them regarding the effectiveness and efficacy of taking action. Finally, users prefer to use a tool that enables them to visualise and review their data exports instead of immediate and direct transfer of their data between services when exercising their right to data portability.

However, satisfying user expectations and the practicability of providing ex-post TETs which respect user needs require to solve the technical and legal issues regarding the collaboration among various stakeholders, including TETs and data services. Future research on improving ex-post transparency and intervenability must cater to the user problems, needs, and expectations concerning the ex-post TETs revealed in this thesis.

Second, to improve user-centred ex-ante transparency and consent and address RQ2, we designed usable consent forms in the context of identity providers which actively engaged users with policy information and evaluated their effectiveness on drawing user attention, their efficiency, and user satisfaction. Moreover, we examined if the potential short-term benefits arising from engaging users with the content were robust to habituation. Actively engaging users with policy information through different interaction techniques, although more time-consuming, is effective in drawing their attention compared to situations where users can easily click to continue. Repeated exposure to consent forms negates the short-term benefits of engaging users with policy information. Nonetheless, consistent consent forms with identical layouts across services could train users to pay attention to the appropriate pieces of information.

Engaging users with policy information in consent forms needs to be carefully designed. The design must not cause insufficient or less attention to any policy information that allows users to understand the consequences of

data processing. Interactivity compromises the processing of non-interactive content. Moreover, different types of actions cause inconsistent attention to the policy information involved. For example, the DAD action results in more user attention to the policy items that must be dragged than the policy items to which dragged items are dropped.

We conclude that designers should consider the context of use when selecting a suitable interaction technique to engage users with policy information. For example, checkboxes suffice for both fulfilling the legal requirements and drawing user attention in frequently-appearing consent forms such as (blocking) cookie consent notices. Our results concerning the effectiveness of user engagement with policy information are valid so long as users have to interact with content and there are no dark patterns involved. Interface designs that seek to lead users into desired behaviours through malicious interaction flows are referred to as "dark patterns" [43]. For example, the dark patterns of not showing a *reject all* button on the first page next to the *accept all* button and not showing granular control at the first layer make it more likely for users to accept cookies [83].

To further contribute to improving consent, we investigated how certain technologies could affect the provision of informed consent and studied the effectiveness of our proposed design for adapted consent based on the peculiarities of the technology at hand. Particularly, we designed and evaluated a prototype that facilitated incremental consent forms based on dynamic consent for repurposing new types of data derived in big data analytics. Users who understand how we implement the concept of dynamic consent appreciate the incremental consent requests which have the potential to describe the context more accurately and increase user control of their data if suitably designed. Further, we investigated different people's understanding of privacy of fingerprint recognition in the context of IdPs and their attitudes regarding the sensitivity of the fingerprint data, which could affect obtaining informed consent from users as well as consent withdrawal. The user expectations and issues revealed in our evaluations must be addressed in the future design of adapted consent dependent on the technologies at hand.

With technological advancements such as the emergence of new big data analytics and algorithmic decision-making and the demand for privacy-preserving data processing, the current practices of obtaining consent based on data protection rules and regulations face new challenges. For example, with the ever-growing application of neural networks, how can service providers achieve specific and informed consent from their customers when the process itself is not transparent or the data processing purposes are impossible to predict and explain? Thus, current practices must be adapted to the demand and traits of the technologies at hand. Future research should focus on finding solutions for providing usable transparency for privacy-preserving neural networks and obtaining informed consent from users in this context.

The stricter requirements of consent in the GDPR—for example, the need for explicit consent in certain circumstances—call for more investigation to find usable solutions which can assure the enhancement of user autonomy and

control. The result in this thesis revealed that even with active engagement with policy information, users missed the salient fields and gave their consent, which could have severe consequences for the privacy of their personal information. Thus, future research should investigate affirmative actions for providing explicit consent. Users may associate using digital signatures to confirm consent with legal commitments. Nonetheless, future research should investigate if this brings more attention to policy information.

Acknowledgement of Prior Work

PhD dissertation in Computer Science at Karlstad University usually involves two phases. The PhD dissertation, the outcome of the second phase, is based on the licentiate dissertation published at the end of the first phase. This thesis is based on and recognises the work previously published as the author's licentiate thesis [62].

References

[1] Lag (2003:460) om etikprövning av forskning som avser människor, 2003.

[2] I. Adjerid, A. Acquisti, L. Brandimarte, and G. Loewenstein. Sleights of privacy: Framing, disclosures, and the limits of transparency. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, pages 9:1–9:11. ACM, 2013.

[3] B. B. Anderson, J. L. Jenkins, A. Vance, C. B. Kirwan, and D. Eargle. Your memory is working against you: How eye tracking and memory explain habituation to security warnings. *Decision Support Systems*, 92:3 – 13, 2016.

[4] B. B. Anderson, A. Vance, C. B. Kirwan, J. L. Jenkins, and D. Eargle. From warning to wallpaper: Why the brain habituates to security warnings and what can be done about it. *Journal of Management Information Systems*, 33(3):713–743, 2016.

[5] J. Angulo, S. Fischer-Hübner, T. Pulls, and E. Wästlund. Usable transparency with the Data Track: A tool for visualizing data disclosures. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*, CHI EA '15, pages 1803–1808. ACM, 2015.

[6] C. A. Ardagna, L. Bussard, S. De Capitani di Vimercati, G. Neven, E. Pedrini, S. Paraboschi, F. Preiss, P. Samarati, S. Trabelsi, and M. Verdicchio. Primelife policy language. In *W3C Workshop on Access Control Application Scenarios*. W3C, 2009.

[7] H. Arendt. *The Human Condition*. University of Chicago Press, 1958.

[8] Art. 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent, Adopted on 13 July 2011.

[9] Art. 29 Data Protection Working Party. Opinion 10/2004 on more harmonised information provisions, Adopted on 25 November 2004.

[10] Art. 29 Data Protection Working Party. Guidelines on consent under Regulation 2016/679, Adopted on November 2017.

[11] Art. 29 Data Protection Working Party. Guidelines on transparency under Regulation 2016/679, Revised and adopted on 11 April 2018.

[12] Art. 29 Data Protection Working Party. Guidelines on the right to data portability, Revised and adopted on 5 April 2017.

[13] A. Bangor, P. Kortum, and J. Miller. Determining what individual SUS scores mean: Adding an adjective rating scale. *Journal of Usability Studies*, 4(3):114–123, 2009.

[14] A. Bangor, P. T. Kortum, and J. T. Miller. An empirical evaluation of the system usability scale. *International Journal of Human–Computer Interaction*, 24(6):574–594, 2008.

[15] L. Barkhuus and J. A. Rode. From mice to men – 24 years of evaluation in CHI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, volume 10 of *CHI '07*. ACM, 2007.

[16] K. Bernsmed and S. Fischer-Hübner. User interface prototypes. A4Cloud Deliverable D:D-5.4. Technical report, A4Cloud EU project, September 2015.

[17] C. Bier, K. Kühne, and J. Beyerer. PrivacyInsight: the next generation privacy dashboard. In S. Schiffner, J. Serna, D. Ikonomou, and K. Rannenberg, editors, *Privacy Technologies and Policy*, pages 135–152. Springer, 2016.

[18] R. Böhme and S. Köpsell. Trained to accept?: a field experiment on consent dialogs. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2403–2406. ACM, 2010.

[19] L. Bortolotti and M. Mameli. Deception in psychology: moral costs and benefits of unsought self-knowledge. *Accountability in Research*, 13(3):259–275, 2006.

[20] C. Bravo-Lillo, S. Komanduri, L. F. Cranor, R. W. Reeder, M. Sleeper, J. Downs, and S. Schechter. Your attention please: Designing security-decision UIs to make genuine risks harder to ignore. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13. ACM, 2013.

[21] J. Brooke et al. SUS– a quick and dirty usability scale. *Usability Evaluation in Industry*, 189(194):4–7, 1996.

[22] B. Brown, M. Chui, and J. Manyika. Are you ready for the era of 'big data'. *McKinsey Quarterly*, 4(2011):24–35, 2011.

[23] M. Buchenau and J. F. Suri. Experience prototyping. In *Proceedings of the 3rd Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques*, DIS '00, pages 424–433. ACM, 2000.

[24] A. Carey. The group effect in focus groups: Planning, implementing and interpreting focus group research. In J. M. Morse, editor, *Critical Issues in Qualitative Research Methods*, pages 225–241. Sage Publications, 1994.

[25] E. Carolan. The continuing problems with online consent under the EU's emerging data protection principles. *Computer Law & Security Review*, 32(3):462–473, 2016.

[26] F. H. Cate. The limits of notice and choice. *IEEE Security Privacy*, 8(2):59–62, 2010.

[27] A. Cavoukian. Privacy by design: The 7 foundational principles – Implementation and mapping of fair information practices. *Information and Privacy Commissioner of Ontario, Canada*, 5, 2009.

[28] J. E. Cohen. Turning privacy inside out. *Theoretical inquiries in law*, 20(1):1–32, 2019.

[29] L. F. Cranor. P3P: making privacy policies more useful. *IEEE Security & Privacy*, 99(6):50–55, 2003.

[30] L. F. Cranor, P. Guduru, and M. Arjula. User interfaces for privacy agents. *ACM TOCHI*, 13(2):135–178, 2006.

[31] B. Custers, S. van Der Hof, B. Schermer, S. Appleby-Arnold, and N. Brockdorff. Informed consent in social media use – the gap between user expectations and EU personal data protection law. *SCRIPTed*, 10:435, 2013.

[32] R. A. Dahl. The concept of power. *Behavioral science*, 2(3):201–215, 1957.

[33] M. Degeling, C. Utz, C. Lentzsch, et al. We value your privacy ... now take some cookies. *Informatik Spektrum*, 42:345–346, 2019.

[34] Z. Efroni, J. Metzger, L. Mischau, and M. Schirmbeck. Privacy icons: A risk-based approach to visualisation of data processing. *European Data Protection Law Review*, 5(3):352–366, 2019.

[35] Eropean Data Protection Board. Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), 12 November 2019.

[36] R. R. Faden and T. L. Beauchamp. *A history and theory of informed consent*. Oxford University Press, 1986.

[37] S. Fischer-Hübner, J. Angulo, F. Karegar, and T. Pulls. Transparency, privacy and trust – technology for tracking and controlling my data disclosures: Does this work? In S. M. Habib, J. Vassileva, S. Mauw, and M. Mühlhäuser, editors, *Trust Management X*, pages 3–14. Springer, 2016.

[38] F. J. Fowler Jr. *Survey research methods*. SAGE Publications, 2013.

[39] B. Friedman, E. Felten, and L. I. Millett. Informed consent online: a conceptual model and design principles. *University of Washington Computer Science & Engineering Technical Report 00–12–2*, 2000.

[40] B. Friedman, P. H. Khan Jr, and D. C. Howe. Trust online. *Communications of the ACM*, 43(12):34–40, 2000.

[41] A. Giannopoulou. Algorithmic systems: The consent is in the detail? *Internet Policy Review*, 9(1), 2020.

[42] J. Gluck, F. Schaub, A. Friedman, H. Habib, N. Sadeh, L. F. Cranor, and Y. Agarwal. How short is too short? implications of length and framing on the effectiveness of privacy notices. In *Twelfth Symposium on Usable Privacy and Security*, SOUPS '16, pages 321–340. USENIX Association, 2016.

[43] C. M. Gray, Y. Kou, B. Battles, J. Hoggatt, and A. L. Toombs. The dark (patterns) side of UX design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, page 1–14. ACM, 2018.

[44] G. Guest, A. Bunce, and L. Johnson. How many interviews are enough? an experiment with data saturation and variability. *Field Methods*, 18(1):59–82, 2006.

[45] H. Habib, S. Pearman, J. Wang, Y. Zou, A. Acquisti, L. F. Cranor, N. Sadeh, and F. Schaub. "it's a scavenger hunt": Usability of websites' opt-out and data deletion choices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–12. ACM, 2020.

[46] M. Hansen. Marrying transparency tools with user-controlled identity management. In S. Fischer-Hübner, P. Duquenoy, A. Zuccato, and L. Martucci, editors, *The Future of Identity in the Information Society*, pages 199–220. Springer, 2008.

[47] M. Hansen. Top 10 mistakes in system design from a privacy perspective and privacy protection goals. In J. Camenisch, B. Crispo, S. Fischer-Hübner, R. Leenes, and G. Russello, editors, *Privacy and Identity Management for Life*, pages 14–31. Springer, 2012.

[48] M. Hansen, M. Jensen, and M. Rost. Protection goals for privacy engineering. In *2015 IEEE Security and Privacy Workshops*, pages 159–166, 2015.

[49] M. Harbach, M. Hettig, S. Weber, and M. Smith. Using personal examples to improve risk communication for security & privacy decisions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, page 2647–2656. ACM, 2014.

[50] H. Hedbom. A survey on transparency tools for enhancing privacy. In V. Matyáš, S. Fischer-Hübner, D. Cvrček, and P. Švenda, editors, *The Future of Identity in the Information Society*, pages 67–82. Springer, 2009.

[51] A. R. Herzog and J. G. Bachman. Effects of questionnaire length on response quality. *Public Opinion Quarterly*, 45(4):549–559, 1981.

[52] M. Hildebrandt. Profiling and ami. In K. Rannenberg, D. Royer, and A. Deuker, editors, *The Future of Identity in the Information Society*, pages 273–310. Springer, 2009.

[53] L.-E. Holtz, H. Zwingelberg, and M. Hansen. *Privacy policy icons*, pages 279–285. Springer, 2011.

[54] F. Hörandner, S. Krenn, A. Migliavacca, F. Thiemer, and B. Zwattendorfer. CREDENTIAL: a framework for privacy-preserving cloud-based data sharing. In *11th International Conference on Availability, Reliability and Security (ARES)*, pages 742–749. IEEE, 2016.

[55] K. Hornbæk. Current practice in measuring usability: challenges to usability studies and research. *International Journal of Human-Computer Studies*, 64(2):79–102, 2006.

[56] K. Hornbæk. Some whys and hows of experiments in human–computer interaction. *Found. Trends Hum.-Comput. Interact.*, 5(4):299–373, June 2013.

[57] D. Huth. A pattern catalog for GDPR compliant data protection. In *PoEM Doctoral Consortium*, pages 34–40, 2017.

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

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

[60] Y. Javed and M. Shehab. Look before you authorize: Using eye-tracking to enforce user attention towards application permissions. *Proceedings on Privacy Enhancing Technologies*, 2017(2):23–37, 2017.

[61] E. Kani-Zabihi and M. Helmhout. Increasing service users' privacy awareness by introducing on-line interactive privacy features. In P. Laud, editor, *Information Security Technology for Applications*, pages 131–148. Springer, 2012.

[62] F. Karegar. *Towards Improving Transparency, Intervenability, and Consent in HCI*. Licentiate thesis, Karlstad University, 2018.

[63] P. G. Kelley, L. Cesca, J. Bresee, and L. F. Cranor. Standardizing privacy notices: an online study of the nutrition label approach. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, pages 1573–1582. ACM, 2010.

[64] J. Kitzinger. Qualitative research: Introducing focus groups. *BMJ*, 311(7000):299–302, 1995.

[65] J. Lazar, J. H. Feng, and H. Hochheiser. *Research methods in human-computer interaction*. Morgan Kaufmann, 2017.

[66] T. Linden, R. Khandelwal, H. Harkous, and K. Fawaz. The privacy policy landscape after the GDPR. *Proceedings on Privacy Enhancing Technologies*, 2020(1):47 – 64, 2020.

[67] E. Luger, S. Moran, and T. Rodden. Consent for all: Revealing the hidden complexity of terms and conditions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '13, page 2687–2696. ACM, 2013.

[68] O. Lynskey. *The foundations of EU data protection law*. Oxford University Press, 2015.

[69] D. Machuletz and R. Böhme. Multiple purposes, multiple problems: A user study of consent dialogs after GDPR. *Proceedings on Privacy Enhancing Technologies*, 2020(2):481–498, 2020.

[70] J. A. MacIntosh. Focus groups in distance nursing education. *Journal of Advanced Nursing*, 18(12):1981–1985, 1993.

[71] I. S. MacKenzie. *Human-Computer Interaction: An Empirical Research Perspective*. Morgan Kaufmann, 2013.

[72] N. K. Malhotra, S. S. Kim, and J. Agarwal. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4):336–355, 2004.

[73] A. M. McDonald and L. F. Cranor. The cost of reading privacy policies. *ISJLP*, 4(3):543–568, 2008.

[74] A. M. Mcdonald, R. W. Reeder, P. G. Kelley, and L. F. Cranor. A comparative study of online privacy policies and formats. In *International Symposium on Privacy Enhancing Technologies Symposium*, pages 37–55. Springer, 2009.

[75] J. E. McGrath. Methodology matters: Doing research in the behavioral and social sciences. In *Readings in Human–Computer Interaction*, pages 152–169. Elsevier, 1995.

[76] L. I. Millett, B. Friedman, and E. Felten. Cookies and web browser design: Toward realizing informed consent online. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '01, pages 46–52. ACM, 2001.

[77] D. L. Morgan. Focus groups. *Annual review of sociology*, 22(1):129–152, 1996.

[78] P. Murmann. Eliciting design guidelines for privacy notifications in mhealth environments. *International Journal of Mobile Human Computer Interaction (IJMHCI)*, 11(4):66–83, 2019.

[79] P. Murmann. *Information at Your Fingertips : Facilitating Usable Transparency via Privacy Notifications*. PhD thesis, Karlstad University, 2020.

[80] P. Murmann and S. Fischer-Hübner. Tools for achieving usable ex-post transparency: A survey. *IEEE Access*, 5:22965–22991, 2017.

[81] J. Nielsen and R. Molich. Heuristic evaluation of user interfaces. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '90, page 249–256. ACM, 1990.

[82] B. Nissen, V. Neumann, M. Mikusz, R. Gianni, S. Clinch, C. Speed, and N. Davies. Should I agree? delegating consent decisions beyond the individual. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, page 1–13. ACM, 2019.

[83] M. Nouwens, I. Liccardi, M. Veale, D. Karger, and L. Kagal. Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. CHI '20, page 1–13. ACM, 2020.

[84] M. T. Orne. On the social psychology of the psychological experiment: With particular reference to demand characteristics and their implications. *American psychologist*, 17(11):776, 1962.

[85] Y. J. Park. Digital literacy and privacy behavior online. *Communication Research*, 40(2):215–236, 2013.

[86] A. S. Patrick and S. Kenny. From privacy legislation to interface design: Implementing information privacy in Human-Computer Interactions. In R. Dingledine, editor, *Privacy Enhancing Technologies*, pages 107–124. Springer, 2003.

[87] J. S. Pettersson, S. Fischer-Hübner, N. Danielsson, J. Nilsson, M. Bergmann, S. Clauss, T. Kriegelstein, and H. Krasemann. Making prime usable. In *Proceedings of the 2005 Symposium on Usable Privacy and Security*, SOUPS '05, page 53–64. ACM, 2005.

[88] I. Pollach. What's wrong with online privacy policies? *Communications of the ACM*, 50(9):103–108, 2007.

[89] 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. In B. Berendt, T. Engel, D. Ikonomou, D. Le Métayer, and S. Schiffner, editors, *Privacy Technologies and Policy*, pages 38–59. Springer, 2016.

[90] J. Preece, Y. Rogers, H. Sharp, D. Benyon, S. Holland, and T. Carey. *Human-Computer Interaction*, chapter 27, pages 537–565. Addison-Wesley Longman Ltd., 1994.

[91] S. Preibusch. Guide to measuring privacy concern: Review of survey and observational instruments. *Int. J. Hum.-Comput. Stud.*, 71(12):1133–1143, 2013.

[92] T. Pulls. *Preserving privacy in transparency logging*. PhD thesis, Karlstad University, 2015.

[93] K. M. Ramokapane, A. Rashid, and J. M. Such. "I feel stupid I can't delete...": A study of users' cloud deletion practices and coping strategies. In *Thirteenth Symposium on Usable Privacy and Security*, SOUPS '17, pages 241–256. USENIX Association, 2017.

[94] P. Raschke, A. Küpper, O. Drozd, and S. Kirrane. Designing a GDPR-compliant and usable privacy dashboard. In M. Hansen, E. Kosta, I. Nai-Fovino, and S. Fischer-Hübner, editors, *Privacy and Identity Management. The Smart Revolution: 12th IFIP WG 9.2, 9.5, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Ispra, Italy, September 4-8, 2017, Revised Selected Papers*, pages 221–236. Springer, 2018.

[95] R. Rosenthal. The volunteer subject. *Human relations*, 18(4):389–406, 1965.

[96] J. Rubin and D. Chisnell. *Handbook of usability testing: how to plan, design, and conduct effective tests*. John Wiley & Sons, 2008.

[97] S. Ruoti, B. Roberts, and K. Seamons. Authentication melee: A usability analysis of seven web authentication systems. In *Proceedings of the 24th International Conference on World Wide Web*, WWW '15, pages 916–926. International World Wide Web Conferences Steering Committee, 2015.

[98] L. Sanders. On modeling an evolving map of design practice and design research. *Interactions*, 15(6):13–17, Nov. 2008.

[99] J. Sauer, K. Seibel, and B. Rüttinger. The influence of user expertise and prototype fidelity in usability tests. *Applied Ergonomics*, 41(1):130–140, 2010.

[100] F. Schaub, R. Balebako, and L. F. Cranor. Designing effective privacy notices and controls. *IEEE Internet Computing*, 21(3):70–77, 2017.

[101] F. Schaub, R. Balebako, A. L. Durity, and L. F. Cranor. A design space for effective privacy notices. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security*, SOUPS '15, page 1–17. USENIX Association, 2015.

[102] B. W. Schermer. The limits of privacy in automated profiling and data mining. *Computer Law & Security Review*, 27(1):45–52, 2011.

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

[104] H. Schneider, M. Eiband, D. Ullrich, and A. Butz. Empowerment in HCI – a survey and framework. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, page 1–14. ACM, 2018.

[105] B. Schneier. A taxonomy of social networking data. *IEEE Security & Privacy*, 8(4):88–88, 2010.

[106] M. Schufrin, S. Lamarr Reynolds, A. Kuijper, and J. Kohlhammer. A visualization interface to improve the transparency of collected personal data on the internet. *arXiv preprint arXiv:2009.02998*, 2020.

[107] J. P. Simmons, L. D. Nelson, and U. Simonsohn. False-positive psychology: Undisclosed flexibility in data collection and analysis allows presenting anything as significant. *Psychological science*, 22(11):1359–1366, 2011.

[108] D. I. Sjøberg, J. E. Hannay, O. Hansen, V. B. Kampenes, A. Karahasanovic, N.-K. Liborg, and A. C. Rekdal. A survey of controlled experiments in software engineering. *IEEE transactions on software engineering*, 31(9):733–753, 2005.

[109] D. J. Solove. Conceptualizing privacy. *Calif. L. Rev.*, 90:1087, 2002.

[110] F. K. Stage and K. Manning. *Research in the college context: Approaches and methods*. Routledge, 2015.

[111] S. S. Sundar. Social psychology of interactivity in human-website interaction. In A. N. Joinson, K. Y. A. McKenna, T. Postmes, U.-D. Reips, and S. S. Sundar, editors, *The Oxford handbook of Internet psychology*, pages 89–104. Oxford University Press, 2007.

[112] S. S. Sundar, S. Bellur, J. Oh, Q. Xu, and H. Jia. User experience of on-screen interaction techniques: An experimental investigation of clicking, sliding, zooming, hovering, dragging, and flipping. *Human–Computer Interaction*, 29(2):109–152, 2014.

[113] M. Tabassum, A. Alqhatani, M. Aldossari, and H. Richter Lipford. Increasing user attention with a comic-based policy. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, page 1–6. ACM, 2018.

[114] The European Parliament and the Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union L. 119, 4.5.2016*, pages 1–88, 2016.

[115] P. Tsormpatzoudi, B. Berendt, and F. Coudert. Privacy by design: From research and policy to practice–the challenge of multi-disciplinarity. In *Annual Privacy Forum*, pages 199–212. Springer, 2015.

[116] T. S. Tullis and J. N. Stetson. A comparison of questionnaires for assessing website usability. In *Usability Professional Association Conference*, volume 1, pages 1–12, 2004.

[117] C. Utz, M. Degeling, S. Fahl, F. Schaub, and T. Holz. (Un)Informed consent: Studying GDPR consent notices in the field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, CCS '19, page 973–990. ACM, 2019.

[118] I. van Ooijen and H. U. Vrabec. Does the GDPR enhance consumers' control over personal data? an analysis from a behavioural perspective. *J Consum Policy*, 42:91–107, 2019.

[119] A. Vance, J. L. Jenkins, B. B. Anderson, D. K. Bjornn, and C. B. Kirwan. Tuning out security warnings: A longitudinal examination of habituation through fMRI, eye tracking, and field experiments. *MIS Q.*, 42(2):355–380, June 2018.

[120] Vetenskapsrådet. *Forskningsetiska principer inom humanistisk-samhällsvetenskaplig forskning*. Vetenskapsrådet, 2002.

[121] M. Walker, L. Takayama, and J. A. Landay. High-fidelity or low-fidelity, paper or computer? choosing attributes when testing web prototypes. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 46, pages 661–665. SAGE Publications, 2002.

[122] N. Wang, J. Grossklags, and H. Xu. An online experiment of privacy authorization dialogues for social applications. In *Proceedings of the 2013 Conference on Computer Supported Cooperative Work*, CSCW '13, pages 261–272. ACM, 2013.

[123] A. F. Westin. Privacy and freedom. *New York: Atheneum*, page 7, 1967.

[124] J. O. Wobbrock and J. A. Kientz. Research contributions in Human-Computer Interaction. *Interactions*, 23(3):38–44, 2016.

[125] M. S. Wogalter, V. C. Conzola, and T. L. Smith-Jackson. Research-based guidelines for warning design and evaluation. *Applied ergonomics*, 33(3):219–230, 2002.

[126] M. A. Zimmerman. Psychological empowerment: Issues and illustrations. *American Journal of Community Psychology*, 23(5):581–599, 1995.

[127] C. Zimmermann. A categorization of transparency-enhancing technologies. *arXiv preprint arXiv:1507.04914*, 2015.

[128] C. Zimmermann, R. Accorsi, and G. Müller. Privacy dashboards: reconciling data-driven business models and privacy. In *Ninth International Conference on Availability, Reliability and Security (ARES)*, pages 152–157. IEEE, 2014.

The Lord of Their Data Under the GDPR?

The challenges imposed by the ever-growing online data processing make it difficult for people to control their data, which inevitably imperils the privacy of their personal information. Thus, there is an increasing need for different societal, technological, and legal solutions that empower users to take control of their data. The intervenability rights and the enhanced transparency and consent requirements in the General Data Protection Regulation (GDPR) aim to enable users to gain control of their data. However, they will not be beneficial for users in practice without considering their Human-Computer Interaction (HCI) implications.

The objective of this thesis is to propose usable tools and solutions which improve user-centred transparency, intervenability, and consent, thereby empowering users to take control of their data and make informed decisions. To this end, we investigate how usable ex-post transparency can facilitate intervenability by implementing and testing transparency-enhancing tools that run on users' devices. Further, we analyse the effectiveness of engaging users with policy information through different types of interaction techniques on drawing user attention to consent form contents. We extend our investigation to the robustness of varying consent form designs to habituation. Moreover, we study how users perceive our design of adapted consent based on the demands and challenges of the technology at hand. The outcome of this thesis includes several artefacts, design guidelines, and empirical analyses.

ISBN 978-91-7867-170-0 (print)

ISBN 978-91-7867-169-4 (pdf)

ISSN 1403-8099

DOCTORAL THESIS | Karlstad University Studies | 2020:36

The Lord of Their Data Under the GDPR?

Empowering Users Through Usable Transparency, Intervenability, and Consent

The challenges imposed by the ever-growing online data processing make it difficult for people to control their data, which inevitably imperils the privacy of their personal information. Thus, there is an increasing need for different societal, technological, and legal solutions that empower users to take control of their data. The intervenability rights and the enhanced transparency and consent requirements in the General Data Protection Regulation (GDPR) aim to enable users to gain control of their data. However, they will not be beneficial for users in practice without considering their Human-Computer Interaction (HCI) implications.

The objective of this thesis is to propose usable tools and solutions which improve user-centred transparency, intervenability, and consent, thereby empowering users to take control of their data and make informed decisions. To this end, we investigate how usable ex-post transparency can facilitate intervenability by implementing and testing transparency-enhancing tools that run on users' devices. Further, we analyse the effectiveness of engaging users with policy information through different types of interaction techniques on drawing user attention to consent form contents. We extend our investigation to the robustness of varying consent form designs to habituation. Moreover, we study how users perceive our design of adapted consent based on the demands and challenges of the technology at hand. The outcome of this thesis includes several artefacts, design guidelines, and empirical analyses.

ISBN 978-91-7867-170-0 (print) | ISBN 978-91-7867-169-4 (pdf)

DOCTORAL THESIS | Karlstad University Studies | 2020:36