Thesis for The Degree of Licentiate of Philosophy

A User-Centric Approach to Usable Privacy for IoT Trigger-Action Platforms

Piero Romare

CHALMERS

Division of Computing Science
Department of Computer Science & Engineering
Chalmers University of Technology
Gothenburg, Sweden, 2025

A User-Centric Approach to Usable Privacy for IoT Trigger-Action Platforms

Piero Romare

Department of Computer Science & Engineering
Division of Computing Science
Chalmers University of Technology
Gothenburg, Sweden

This thesis has been prepared using LaTeX.
Printed by Chalmers Reproservice,
Gothenburg, Sweden 2025.

Abstract

This licentiate thesis analyzes the diversity of Internet of Things (IoT) Trigger-Action Platforms (TAPs) users' privacy concerns and preferences for proposing privacy profiles as a basis for usable privacy management. IoT TAPs host applications created by users or service providers based on automated interactions between IoT devices and online services. Despite the benefits of TAPs, their automation capabilities raise privacy concerns, as they necessitate the collection and sharing of personal data. The research presented in this thesis is the first step for a human-centred design for a usable privacy permission system for IoT TAPs.

The research, grounded in a triangulation approach, combines qualitative insights from focus groups with a large-scale quantitative survey (N=301) and expert reviews. Initial focus groups explored user-defined privacy factors concerning TAPs, revealing concerns, especially regarding transparency, control, confidentiality and trust. These qualitative findings were then used to find differences and similarities between IoT TAP and general IoT for investigating specific privacy factors for IoT TAPs that go beyond those that users have for general IoT, such as their reliance on automation and the integration of trigger-action functionalities. Second, these findings provided input for the development and validation of a comprehensive questionnaire to measure users' privacy concerns and data sharing preferences in various TAP scenarios. The quantitative study based on the questionnaire identified three clusters: High Privacy, Medium Privacy, and Basic Privacy which were each characterized by data sharing preferences. This clustering forms the basis for proposing privacy profiles that can guide the design of more usable privacy management systems for TAPs. It supports a context-specific

approach to privacy management. The three studies provide directions to a recommendation system for enhancing privacy within the evolving context of IoT TAPs, towards personalized privacy assistants.

Keywords: Internet of Things, Trigger-Action Platform, Human-Computer Interaction, Privacy Concerns, Privacy Preferences, User-Centric Design

Acknowledgments

To my family, thank you for always believing in me, encouraging me to pursue my studies, and motivating me throughout this journey.

I would also like to extend my deepest gratitude to my supervisors, prof. Simone Fischer-Hübner, Dr. Farzaneh Karegar and prof. Morten Fjeld, for their guidance, insights, and support during these years. Your constructive feedback and expertise have been invaluable, and your belief in my abilities has been inspiring. I am incredibly grateful to have had the opportunity to work with you.

This work was partially supported by the Wallenberg AI, Autonomous Systems and Software Program (WASP) funded by the Knut and Alice Wallenberg Foundation.

Contents

Introduction

This licentiate thesis explores user privacy concerns, requirements and preferences in Internet of Things (IoT) Trigger-Action Platforms (TAPs) applications, which automate digital tasks based on defined events named triggers. IoT applications are based on the communication link between different devices and services that are online and connected. Some of the most popular platforms that can host these IoT applications are Trigger-Action Platforms. These help the users to create such kind of interconnection between smart devices or online services, even from different IoT manufacturers, avoiding the lack of standardization that often is encountered. Indeed, the improved interoperability as well as the new functionalities offered from these platforms available on the market have reached millions of users.

Even though platforms offer convenience, they also introduce privacy and security risks. For example, IoT TAPs like IFTTT and Zapier pose privacy concerns due to overprivileged access rights and excessive permission requests [1]. While these TAPs provide user-friendly interfaces [2] that allow end users to create their own automation, users are often unaware of the risks associated with these applications [3]. Indeed, such applications may lead to significant harms, including behavioural data leaks, potential embarrassment, physical or property damage, service disruptions, or malware distribution [4]. Thousands of applications on these TAPs can collect and share users' data with third parties to execute automation, often transmitting personal information with insufficient transparency and control over data sharing. TAPs allow users to set permissions, but the granularity of these options is usually limited [5], granting better usability, but opening potential security issues [6].

The interconnected nature of TAPs further complicates data management. Indeed, the volume of entities collecting, storing, and processing user data was predicted to exceed users' management capacities [7]. This complexity can lead to unintentional data leakage or unauthorized access, as the potentially huge volume of connections obscures the risks [8]. Each device or application added to a TAP application may introduce new data flow, without clear user notifications or consent after the adoption. While models such as SafeTAP help the users to identify potential conflicts between the rules that the applications employed [9], it is still an open question how the users can manage their privacy while using the automations. They are concerned about the exposure of their personal data, and they want to have personal control over their information. As emphasized in [10], addressing security and privacy challenges in IoT environments requires the development of usable systems that empower end-users to manage these concerns effectively. Understanding user needs is critical to designing effective, user-friendly privacy controls [11]. There is a gap between users' knowledge, attitudes, and behaviours about permissions and privacy settings since they are frequently ignored or misunderstood [12]. One promising approach to support users in managing data sharing among IoT TAP applications is to create privacy profiles that can include privacy preferences [13]. These profiles can be seen as a shortcut to assist the users with pre-defined settings [14], and they can pick up the profiles that best suit them [15].

This thesis builds on existing knowledge of IoT privacy which focuses specifically on TAPs for creating privacy profiles that might help users control their privacy. To design more effective and usable privacy management systems for TAPs, we conducted an exploratory study, a literature review and a confirmatory study. Indeed, the collection of research draws from three main studies that form the triangulation among three different Human-Computer Interaction (HCI) research methods. The first study offers qualitative insights from three focus groups discussions with in total 15 participants. This research identified nine key privacy themes, including transparency, control, trust, data minimization, risks, and the privacy of bystanders—those indirectly affected by the automated actions of others. In particular, transparency, trust and control are generally important privacy factors for IoT environments. The importance of these factors becomes clear when considering the automation of data sharing with third parties (data recipients) and automating actions taken by these third parties. This underscores the need for more usable and transparent privacy controls. The second study, a literature review of privacy concerns in IoT, further examines these themes by comparing user-driven privacy concerns in general IoT settings to those

specific to TAPs. This review highlighted how privacy concerns in smart homes, healthcare, and general IoT environments often overlap with TAPs, but also differ in relevant ways, especially regarding the tension between automation and user control. By this, it elicits what privacy factors are especially important for IoT TAPs. The third study uses a quantitative approach to explore privacy management in TAPs. Based on a survey of 301 participants, the study identified three privacy clusters—Basic, Medium, and High Privacy—representing varying attitudes toward data sharing. These profiles provide a foundation for designing more user-centric privacy management tools. A recurring theme across all three studies proposed in this thesis is the lack of user awareness regarding potential privacy risks, which emphasizes the need for better transparency and education about data collection and sharing practices. By integrating insights from qualitative and quantitative studies, and a literature review, this thesis contributes to the design of a privacy management system that supports user control and transparency in IoT TAPs considering privacy concerns and preferences.

Background

This section briefly discusses the evolution of privacy and provides background information about IoT automation and TAPs, which provide the context for this thesis.

The Evolution of Privacy: From the Right to be Alone to Comprehensive Data Protection

Historically, privacy has been defined with properties and statements that change together with technological progress or, in other words, the computational power [16].

A common highlighted property of privacy is that it is an individual concept and a fundamental right including the right to be let alone as defined in the societal context by Warren and Brandeis [17]. In the 19th century, they suggested that a new legal right to privacy was required since the rules that were in place were insufficient to safeguard individual privacy against the new advances in photography technology and journalism practices.

One of the biggest influences came in the 1960s with Westin's Privacy Theory triggered by the rise of information systems and databases. Westin defined privacy as the self-determination of an individual or groups of when, how and to what extent information is communicated to others. This definition placed more emphasis on control over personal information than on secrecy or being left alone since it covers disclosure, maintenance, and

dissemination. Furthermore, he included empirical research on his theory by deriving three personas: privacy fundamentalist, pragmatist and unconcerned [18]

A few years later, in 1975, Altman defined the privacy regulation theory as the selective control of access to the self as a dynamic boundary regulation [19] in a way that excessive privacy could lead to disconnect from society, while insufficient privacy could change the way individuals act.

Another key point in the history of privacy was from Solove during the 21st century, when he defined four privacy-related problems that may harm individuals: information collection, information processing, information dissemination and invasions [20].

Nissenbaum proposed the concept of contextual integrity, which maintains that privacy is preserved when the flow of information is appropriate to specific social domains and aligns with established norms [21]. Her contextual privacy framework to investigate social norms considers five main variables regarding how information is shared considering specific contexts. Those contexts are often formalized with these five variables: data subject, sender, receiver, attribute and transmission principle. Consequently, the concept of privacy has evolved from the initial notion of the "right to be let alone" to a more comprehensive understanding that includes the control and management of personal information and its context of use. This shift has been driven by technological innovations that have improved access to information and real-time communication, enhancing the ability of governments, companies, and individuals to conduct surveillance and intercept data.

In 1948, the Universal Declaration of Human Rights recognized privacy as a fundamental right in Article 12, stating that no one should be "subjected to arbitrary interference with [their] privacy"[1]. The first data protection law was introduced in 1970 in the German state of Hessen[2].

Recognizing technological advancements and the need to harmonize data protection laws across Europe, the EU Data Protection Directive 95/46/EC was adopted in 1995. This directive established principles such as purpose limitation, restrictions on the use of sensitive personal data, consent as a common legal basis for data processing, and a general prohibition (with exceptions) on personal data transfers to non-European countries lacking adequate data protection [3].

In 2016, the General Data Protection Regulation (GDPR) was approved

[1] https://www.un.org/en/about-us/universal-declaration-of-human-rights

[2] https://starweb.hessen.de/cache/PLPR/06/0/00080.pdf#page=59

[3] https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

by the European Parliament and came into effect in 2018. Unlike a directive, the GDPR is directly applicable in all EU member states. It enforces strict regulations on the use of personal and sensitive data, aiming to protect individual privacy in an era of pervasive data collection and monitoring. Key innovations include the requirement for Data Protection by Design and Default (Article 25) and strengthened rights and controls for data subjects.

Internet of Things Trigger-Action Platforms and its Automation

Internet-connected devices and online services have transformed many aspects of our lives, enabling automation by connecting these devices and services through integrated software. This automation often follows Event-Condition-Action (ECA) or Trigger-Action recipes and is applied in a range of contexts. For example, in an industrial context, Amazon EC2's auto-scaling feature utilizes Event-Condition-Action (ECA) recipes [22]:

> when average CPU utilization goes over 60% → event
> if maximum number of servers not reached → condition
> add a server → action

The event defines the trigger, the condition is the requirement that needs to be satisfied to execute the specified action, and the action establishes the actions to be performed [23]. For end-users, the term End User Development (EUD) refers to the process of creating recipes to automate their smart environments by linking smart home devices or wearables with online services or other devices. These recipes are typically created using simplified code, often following an "if-then" structure, combined with intuitive interfaces and hosting platforms. As a result, thousands of applications have become available, empowering users to customize their environments with ease. TAPs host these applications, which are built as event-driven programs consisting of at least one trigger and one action. IoT TAPs, such as IFTTT, Zapier, Make, and Microsoft Power Automate, operate similarly to app stores with millions of users. They function as connectors or "webhooks", facilitating communication between devices and online services.

For example, in a smart home context, an IoT TAP application available on IFTTT [4] which follows the "if-then" is:

[4] https://ifttt.com/applets/yurpy75a

> if you exit an area → trigger
> turn off lights → action

Another example related to wearables is illustrated in Figure 1. This functionality enables users to automate devices and services based on personal needs without requiring specific coding expertise. On IFTTT, users simply drag and drop their chosen triggers and actions within the web interface (see Figure 2). TAP applications facilitate connections between devices or services whenever a specific event triggers an action. While this offers convenience, it also introduces new privacy challenges, particularly when personal or sensitive data is transferred between trigger and action services.

Additionally, during the initial setup, users are redirected to the service's OAuth access token page to grant IFTTT permission to access their accounts [5]. This token is then used to authenticate API calls to connected services or retrieve trigger data during the application's execution. Although the token streamlines permission management by eliminating additional steps, it is overprivileged and coarse-grained, granting more permissions than are strictly necessary [24].

In this thesis, we propose an approach for improving the usability of fine-grained permission control management systems.

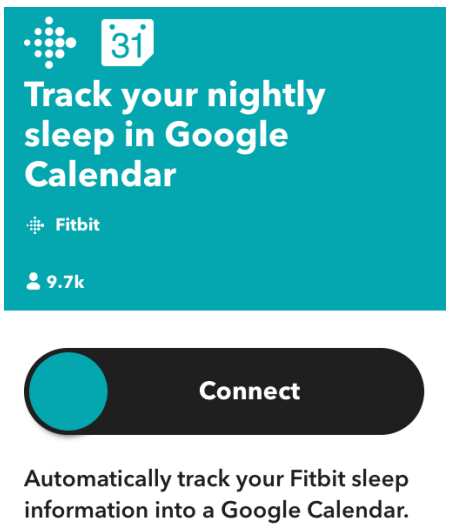

Figure 1: IFTTT as store to download pre-created app

Figure 2: IFTTT interface for creating automations

[5] https://ifttt.com/docs/api_reference

Related Work

In this section, we briefly present and discuss the related work of this thesis providing an overview of the two existing user studies about privacy in IFTTT as well as research on usable privacy controls for IoT, based on privacy clustering and profiles of preferences.

Empirical Studies of Privacy in IoT TAP

In recent years, IoT has enabled new possibilities for connecting various devices, which can significantly amplify data exposure through interconnectivity. This has raised critical questions about user privacy, including how users perceive privacy, how they can be informed about privacy risks, and how they can maintain control and manage their privacy in IoT environments. In the context of IoT TAP, researchers have investigated the nature of privacy risks in IoT TAP applications and how these risks are understood and perceived by users.

Cobb et al. [25] examine the real-world security and privacy risks of IFTTT applets by analysing 732 applets from 28 participants. They combine automated information-flow analysis with qualitative analysis of applet titles and survey responses to assess the likelihood of harm. This research reveals that far fewer applets than previously thought [4] pose significant risks in practice. While many applets technically exhibit secrecy or integrity violations, these rarely translate into actual harm due to contextual factors like applet configuration and the user's intent.

Saeidi et al. [3] investigate how users assess the risks associated with IFTTT applets that connect smart home devices and services. It explores users' concerns about using these applets and highlights how these concerns are influenced by contextual factors such as device location and data sensitivity. The findings reveal that nudging participants to consider various scenarios encourages them to think more carefully about potential risks, ultimately increasing their overall level of concern.

To the best of our knowledge, no existing studies have explored individuals' privacy concerns and preferences in the context of IoT TAP. This thesis aims to address this gap by eliciting individuals' privacy concerns, requirements, and data-sharing preferences in this context.

Towards Usable IoT Privacy Controls

The literature reveals empirical insights into user acceptance and interaction with IoT privacy control systems, indicating that complexity and usability challenges are significant barriers.

Research consistently finds that user privacy preferences are highly context-dependent. A privacy recommendation system that employs data-driven insights to adapt to various IoT environments was developed, taking into account personalized privacy profiles for users [26]. This approach has been extended to different contexts, including general public IoT systems and specific environments like households [27]. These studies highlight the potential of machine learning techniques to improve IoT privacy controls by better aligning them with individual user preferences.

Increased user awareness and educational interventions have been shown to improve user engagement with privacy control systems. Previous studies indicate that when users are better informed in terms of privacy implications, they tend to make more cautious and confident privacy decisions, highlighting the need for systems that promote privacy awareness [28, 29, 30]. These insights are essential for developing feedback mechanisms that build user trust and encourage informed decision-making [31].

Another important theme is the trade-off between privacy and convenience for users. While IoT devices provide significant convenience, this often comes at the potential cost of user privacy and the need to trust device manufacturers [32]. A Personalized Privacy Assistant (PPA) could support users in making informed decisions and reduce cognitive overload, helping them manage these trade-offs effectively [33]. These tools offer users insights into effective privacy practices and help them adjust settings to align with their individual preferences, often using machine learning [34]. The varying perceptions of PPA autonomy underscore the need to balance users' desire for control with concerns about cognitive overload [35].

Additionally, to understand user decision-making regarding IoT privacy configurations, data-driven strategies can guide the design of intelligent interfaces that simplify and improve the usability of privacy management [36]. Supervised [37] and unsupervised [38] learning algorithms can assist users in making privacy decisions, for example, by creating personalized privacy profiles [27]. Experts suggest implementing usable privacy solutions that include the diversity of contexts, such as wearable devices, smart homes, and public IoT systems, to address privacy concerns within IoT ecosystems [39]. These approaches, including tangible interfaces [40], show promise in improving user engagement and satisfaction in managing their privacy [41].

Our work extends previous work by investigating privacy profiles of preferences of users, as a basis for usable and fine-grained privacy controls for IoT TAP users when they have been informed about the privacy implications of using IoT TAP apps for a selected range of scenarios and contexts.

Research Questions

The overall objective that this thesis addresses is to elicit and then analyze the diversity of IoT TAP users' privacy concerns and preferences for proposing privacy profiles as a basis for usable privacy management. Thus, the Research Questions (RQs) that this thesis answers are the following:

- **RQ1**: What are the privacy factors that play a role in users' concerns and preferences for using IoT and in particular IoT TAPs?
- **RQ2**: What privacy clusters and profiles can be identified to support a usable permission management system, reflecting the concerns, requirements and data-sharing preferences of users primed with privacy risks on IoT TAP?

Research Methods

The research methods used to address the research questions and to understand and get insights from individuals follow the so-called triangulation [42]. Triangulation is an HCI specific term that employs mixed-method research designs. A qualitative research method aims to explore participants' understandings and perceptions of a specific topic through in-depth engagement with a small sample. The expert evaluation, conducted through a literature review of scientific articles published by individuals with specialized knowledge in the field, looks to assess the relevance and depth of existing findings. In contrast, a quantitative research method relies on a larger sample size to enable the generalization of results to broader populations. In our context, we refer to triangulation because, in the three papers that this thesis presents, we adopted qualitative, expert reviews and quantitative methods. Such a procedure is employed to give more consistent and complete results to overcome or minimise the insufficient certainty that occasionally results from a single review method or approach. A single method may not consider relevant aspects while a convergence of results from different sources, across different data collection methods, can help to get a more robust and reliable understanding of the phenomena under study.

Paper I In the first study, we conducted **three focus groups** on privacy concerns and preferences towards IoT TAP with, respectively, **N=5, N=6, N=4**. Such a qualitative method employs participants' opinions about a topic with an open discussion driven by a moderator. The number of participants is often limited and should not count more than eight participants per

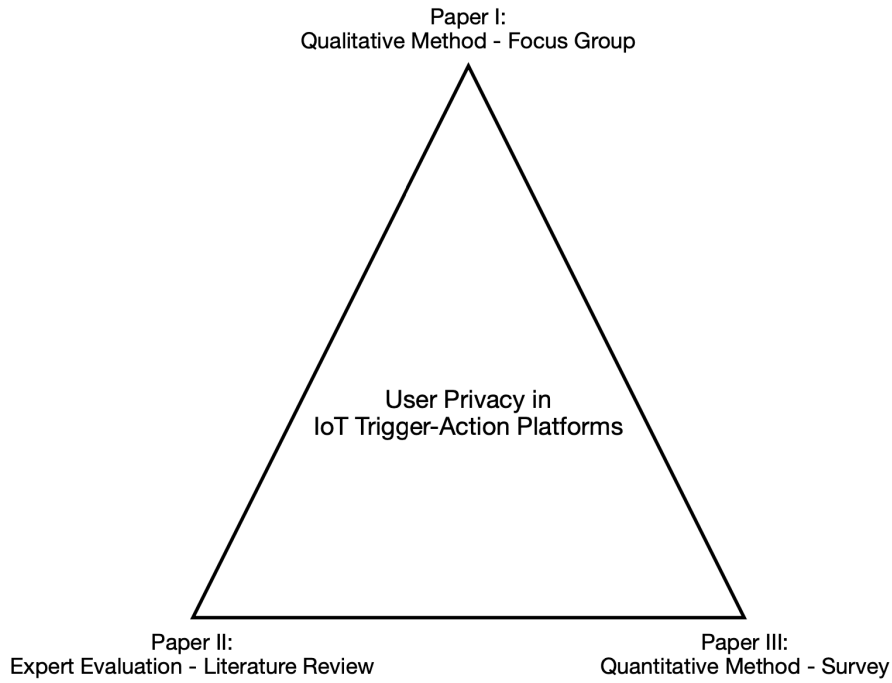

Figure 3: Triangulation on IoT TAP Users' Privacy Concerns, Requirements and Data-Sharing Preferences

group [43]. The funnel technique [44] is a relevant aspect of this method since it refers to guiding the participants from a broader topic (IoT TAP) to the detailed goal of the study (privacy in IoT TAP). In this way, the participants are not biased towards the expectations of the moderator and do not feel any performance pressure. Further, we introduced an artificial and gender-neutral person named Alex. Alex had the role of facilitating the process by preserving the participants' privacy since they were warmly recommended to refer to them when describing their thoughts and empathizing with the role of a user who in their everyday life used IoT TAP applications. We can divide all three focus groups into three sessions: 1) introduction and general discussion 2) focused discussion 3) summary and card sorting task. The parts one and two last 45 minutes, while the last one 15 minutes. A break was proposed between parts one and two. In the first part, we introduced the IoT and IoT TAP context with the help of some real examples of TAP applications. In the second part, the moderator redirected the conversation towards the benefits and the risks of using the TAP applications. This was done with the help of three scenarios which were three real IFTTT applica-

tions that involved personal data sharing. At the end, we revealed the topic of the conversation and summarized the notes taken. We asked the participants to add any other privacy concerns or preferences and rank them individually from the most to the least important. During the discussion, the conversations were recorded and saved on the university servers. Not limited, but especially after the break, the moderator took notes about quotations and sentences from the participants regarding the scope of the study. At the end, we thanked and rewarded the participants with a gift card from the university shop. The notes and the transcripts were then shared among the four authors of this paper who analyzed the text data using thematic analysis. All the authors compared their codes of the three focus groups and debated until code saturation was reached.

Paper II The second study is mostly a **literature review**. Thus, no research method was used that directly involved people besides the **card sorting task** collected from the focus groups of Paper I which included **N=15**. Considering the triangulation practice, this study can be interpreted as the expert reviews angle since it considers the previous knowledge on a similar topic. It is aimed at finding differences and similarities between user studies on the general IoT and the IoT TAP that go beyond those that users have for general IoT. A sample of 376 papers was retrieved by seeking for IoT privacy empirical studies (e.g., interviews, surveys, focus groups) that elicited factors, preferences, expectations, concerns and attitudes. After reading the abstracts of these 376, the 14% were finally selected. In particular, these papers are compared with the privacy factors that were high-ranking in the card sorting task utilized at the end of the focus groups conducted in Paper I to elicit IoT TAP specific privacy factors. The found literature was presented considering the privacy factors extracted, the research methods applied, the contexts (e.g., general IoT, healthcare IoT and smart home) and the type of participants recruited (owners of IoT devices, end-users, experts).

Paper III The third study is an online questionnaire/survey divided into two parts. This quantitative research method completes the triangulation.

For the first part, we designed a **questionnaire** by considering an existing privacy protection framework named 6-axis protection goals [45]. We conducted a literature review regarding existing questions related to privacy concerns and requirements. We adapted eleven items under the three dimensions (Confidentiality, Control and Transparency) selected from the framework. We collected data from $N = 301$ participants. To facilitate the participants' understanding of the topic, we exposed the participants to the same

questionnaire repeated in four scenarios. These four scenarios were selected through a procedure similar to the Delphi method, under a 25-minute **semi-structured interview with six experts** individually. Six experts helped us to identify the privacy risks associated with prefiltered scenarios that involved personal data. The participants of our questionnaire were then exposed to the scenarios and primed with the risks. The answers were made possible through a 5-Likert scale, from "strongly disagree" to "strongly agree". The scenarios and the questions were shuffled randomly.

In the second part, we designed a full **factorial vignette experiment** considering three data sharing preferences features: data categories, the purpose of collection, and data recipient type. The sub-levels for the three features were, in order, 4x3x3, so a total of 36 yes / no questions, one per combination.

The median time to complete the study was 10 minutes. Since substantial changes were made regarding the questions under the three dimensions, we demonstrated the questionnaire to be, in short, valid, reliable and with an excellent global fit. This has been done through Exploratory Factor Analysis and Multi Group Confirmatory Factor Analysis.

Research Contributions

Within the context of the IoT Trigger-Action Platform, this thesis handles the privacy concerns, requirements and preferences with human-in-the-loop:

- **Identification of Human Privacy Concerns and Preferences:** We derived insights about individuals' privacy concerns and preferences that can lay the foundations for the design of usable privacy permission management systems. This contribution is given by the findings from **Paper I** that answer the **RQ1**.

- **Elicitation of IoT TAP specific Privacy Factors beyond general IoT:** the results in **Paper I** and **Paper II** reveal a broadened comprehension of the privacy factors in IoT TAP by including the general IoT, thus integrating meaningful considerations to **RQ1**. We compared the privacy factors that matter for the individuals considering user studies in IoT and IoT TAPs showing what privacy factors relevant for IoT TAPs go beyond privacy factors for the traditional IoT. Considering the automated nature of IoT TAP, we provided directions towards usable privacy emphasizing the need for granular control over the data sharing, control and transparency to help the users to handle the increasing amount of interconnection and data recipients.

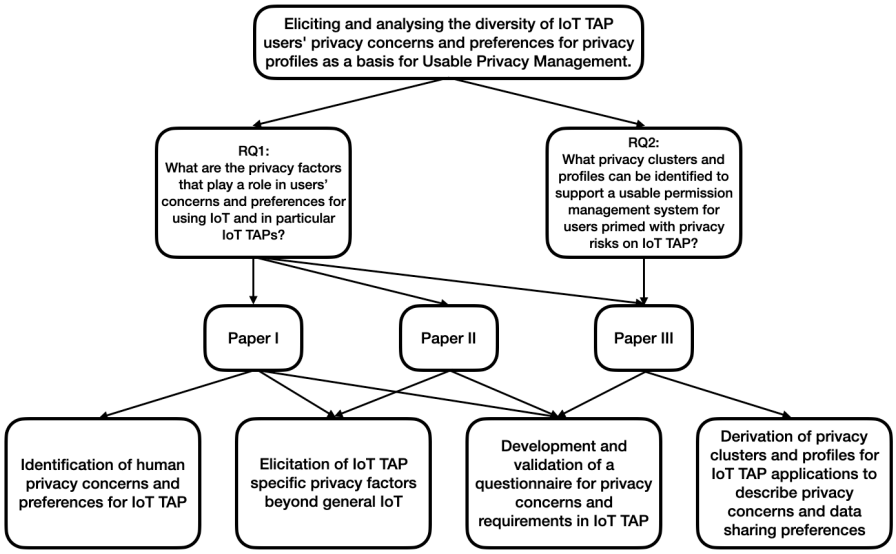

Figure 4: Thesis Overview

- **Development and Validation of a Novel Questionnaire:** We designed and validated a new questionnaire to reliably collect data, aimed at categorizing participants based on their concerns about transparency, control and confidentiality of personal data practices in IoT TAPs when they were also primed with potential privacy risks. This was applied across four distinct IoT TAP real applications. **Paper I, Paper II** and **Paper III** collectively illustrate the design of questions that effectively capture participants' privacy requirements and concerns, and they provide statistical evidence supporting the questionnaire as a tool capable of gathering data to answer the **RQ2**.

- **Derivation of Privacy Clusters and Profiles for IoT TAP Applications:** We identified clusters representing participants' privacy concerns and requirements, specifically within the context of IoT TAP scenarios where users were informed about privacy risks. Utilizing the data from our factorial vignette study, we demonstrated how the identified features aligned with the privacy clusters. These clusters were further characterized to form distinct privacy preference profiles. This contribution is demonstrated in **Paper III** and answers the **RQ2**.

Thesis structure

Paper 1: Tapping into Privacy: A Study of User Preferences and Concerns on Trigger-Action Platforms [46]

This paper investigates user privacy concerns and preferences within the context of Internet of Things (IoT) Trigger-Action Platforms (TAPs). These platforms enable users to connect various devices and services, automating actions based on predefined rules or "applets". For example, a user might create a rule that automatically turns on their smart lights when their smartwatch detects they are approaching home.

While offering convenience, TAPs require the collection and sharing of personal data, raising privacy concerns. To understand these concerns, we conducted focus groups, using a fictional persona, "Alex," to contextualize TAP usage. We presented participants with various scenarios, such as a smart fridge automatically adding items to a shopping list or smart glasses uploading videos to social media, prompting discussions on potential privacy risks.

Through thematic analysis of the recorded and transcribed focus group discussions, we identified nine key themes. These themes indicate that users are concerned about the transparency and controllability of automated processes in IoT TAPs, as well as the potential risks these applications pose to their privacy and the privacy of others. They also express a desire for trust in the automation process, data minimisation strategies, and an understanding of the trade-offs between privacy and security. transparency, control, trust, privacy of bystanders, risks, data minimisation, confidentiality, privacy/security trade-offs, and potential misuse and unexpected consequences. These findings underscore the need for usable privacy controls that provide users with control over automation processes, data sharing, and transparency regarding data recipients and potential risks.

Statement of contributions In this paper, I designed the study together with the co-authors, wrote the script for conducting the focus groups, organized the settings, and moderated the discussions. The co-authors participated in some or all focus groups and took notes. All the authors analysed data using thematic analysis. I wrote the full paper excluding the second paragraph of the Introduction, and the second paragraph of section II.A and the Limitations that were written with Simone Fischer-Hübner, Farzaneh Karegar and Victor Morel. All the authors review the paper. The informed consent form and ethical approval application were written by Simone Fischer-Hübner.

Appeared in: 2023 20th Annual International Conference on Privacy, Security and Trust (PST). IEEE, 2023. doi: 10.1109/PST58708.2023.10320180.

Paper 2: User-Driven Privacy Factors in Trigger-Action Apps: A Comparative Analysis with General IoT [47]

This paper provides a comparison between general IoT and IoT Trigger-Action Platforms regarding users' privacy concerns. Human factors concerning IoT TAP were reproposed from Paper I and similarities and differences with general IoT were discussed.

Accidental data sharing risks are expanded in TAPs due to the intricate web of interconnected services. Misconfigured workflow rules, more likely with increasing complexity, can lead to unintended data disclosure. The nature of trust also differs. General IoT trust focuses on data security and manufacturer reputation. In TAPs, trust extends to platform providers and integrated third-party services, requiring confidence in responsible data handling across the entire workflow.

Data storage and retention concerns in general IoT centre on user control over sharing settings. In contrast, TAPs offer conditional and contextual access, enabling users to set precise conditions for data sharing within automated workflows. This granular control is required in TAPs and would allow more refined data flow management.

Finally, TAPs' emphasis on automation poses unique privacy challenges. Understanding complex connections within automated processes can be difficult, and users may lack control over their execution. User-friendly interfaces with clear data process overviews (i.e., dashboard) and granular control over automation are essential for addressing these challenges.

Statement of contributions In this paper, I am a single author. My supervisors (Simone Fischer-Hübner and Farzaneh Karegar) contributed with feedback and review comments.

Appeared in: Privacy and Identity Management. Sharing in a Digital World. Privacy and Identity 2023. IFIP Advances in Information and Communication Technology, vol 695. Springer, Cham. https://doi.org/10.1007/978-3-031-57978-3_16

Paper 3: Towards Usable Privacy Management for IoT TAPs: Deriving Privacy Clusters and Preference Profiles [48]

This research paper explores user privacy concerns and data-sharing preferences within IoT Trigger-Action Platforms (TAPs). We argued that existing privacy controls in TAPs are often too complex and fail to reflect users' diverse needs. To address this, the research seeks to develop more usable privacy management systems by identifying distinct privacy clusters based on shared user concerns and requirements and characterising these clusters into privacy profiles by examining data-sharing preferences. These profiles would be used to inform the design of privacy management systems that offer tailored privacy settings, potentially through "bundles" aligned with different privacy attitudes.

Users across all identified privacy clusters tend to be cautious about sharing data, emphasizing the need for Data Protection by Default principles in TAPs. The study also underscores the importance of transparency-enhancing tools (TETs) that provide users with clear and understandable information about data processing practices in TAPs. Such tools can empower users to make more informed decisions about data sharing and permissions.

Statement of contributions In this paper, I am the first author. I designed the study, conducted the semi-structured interviews with the experts to select the scenarios and privacy risks for the questionnaire, collected the data from the questionnaire, analysed the data, wrote the full paper and the discussion in collaboration with Simone Fischer-Hübner and Farzaneh Karegar. The questionnaire was designed with Farzaneh Karegar. The informed consent form and ethical approval application were written by Simone Fischer-Hübner.

Under submission.

Conclusion

This thesis explores the privacy concerns and preferences of users in the context of IoT TAPs, and is proposing privacy profiles as a foundation for usable privacy management. We identified nine key privacy themes, highlighting user concerns about transparency, control, trust, data minimisation, and risks associated with data sharing and automation in IoT TAPs. Furthermore, we compared these findings with general IoT privacy concerns, revealing the need for granular control over data sharing and transparency specific to the automated nature of TAPs. We concluded with a quantitative

approach to identify three distinct privacy clusters based on user concerns about transparency, control, and confidentiality, further characterising these clusters into privacy profiles based on data-sharing preferences. By combining insights from these three studies, this thesis aims to contribute to the design of a privacy management system that supports user control and transparency in IoT TAPs, considering the diversity of users' privacy concerns and preferences.

Bibliography

[1] Earlence Fernandes, Amir Rahmati, Jaeyeon Jung, and Atul Prakash. Decoupled-ifttt: Constraining privilege in trigger-action platforms for the internet of things. *CoRR*, abs/1707.00405, 2017. URL http://arxiv.org/abs/1707.00405.

[2] Danilo Caivano, Daniela Fogli, Rosa Lanzilotti, Antonio Piccinno, and Fabio Cassano. Supporting end users to control their smart home: design implications from a literature review and an empirical investigation. *Journal of Systems and Software*, 144:295–313, 2018. ISSN 0164-1212. doi: https://doi.org/10.1016/j.jss.2018.06.035. URL https://www.sciencedirect.com/science/article/pii/S0164121218301262.

[3] Mahsa Saeidi, McKenzie Calvert, Audrey W. Au, Anita Sarma, and Rakesh B. Bobba. If This *Context* Then That *Concern* : Exploring users' concerns with IFTTT applets. *Proceedings on Privacy Enhancing Technologies*, 2022(1):166–186, January 2022. ISSN 2299-0984. doi: 10.2478/popets-2022-0009. URL https://petsymposium.org/popets/2022/popets-2022-0009.php.

[4] Milijana Surbatovich, Jassim Aljuraidan, Lujo Bauer, Anupam Das, and Limin Jia. Some recipes can do more than spoil your appetite: Analyzing the security and privacy risks of ifttt recipes. In *WWW '17*, page 1501–1510, Republic and Canton of Geneva, CHE, 2017. International World Wide Web Conferences Steering Committee. ISBN 9781450349130. doi: 10.1145/3038912.3052709. URL https://doi.org/10.1145/3038912.3052709.

[5] Musard Balliu, Iulia Bastys, and Andrei Sabelfeld. Securing iot apps. *IEEE Security & Privacy*, 17(5):22–29, 2019.

[6] Xianghang Mi, Feng Qian, Ying Zhang, and XiaoFeng Wang. An empirical characterization of ifttt: ecosystem, usage, and performance. In *Proceedings of the 2017 Internet Measurement Conference*, IMC '17, page

398–404, New York, NY, USA, 2017. Association for Computing Machinery. ISBN 9781450351188. doi: 10.1145/3131365.3131369. URL https://doi.org/10.1145/3131365.3131369.

[7] Carlo Maria Medaglia and Alexandru Serbanati. An overview of privacy and security issues in the internet of things. In Daniel Giusto, Antonio Iera, Giacomo Morabito, and Luigi Atzori, editors, *The Internet of Things*, pages 389–395, New York, NY, 2010. Springer New York. ISBN 978-1-4419-1674-7.

[8] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, and Klaus Wehrle. Privacy in the internet of things: threats and challenges. *Security and Communication Networks*, 7(12):2728–2742, 2014.

[9] McKenna McCall, Faysal Hossain Shezan, Abhishek Bichhawat, Camille Cobb, Limin Jia, Yuan Tian, Cooper Grace, and Mitchell Yang. Safetap: An efficient incremental analyzer for trigger-action programs. 2021.

[10] Fabio Paternò and Carmen Santoro. End-user development for personalizing applications, things, and robots. *International Journal of Human-Computer Studies*, 131:120–130, 2019. ISSN 1071-5819. doi: https://doi.org/10.1016/j.ijhcs.2019.06.002. URL https://www.sciencedirect.com/science/article/pii/S1071581919300722. 50 years of the International Journal of Human-Computer Studies. Reflections on the past, present and future of human-centred technologies.

[11] Andreas Jacobsson and Paul Davidsson. Towards a model of privacy and security for smart homes. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, pages 727–732. IEEE, 2015.

[12] Nourah Alshomrani, Steven Furnell, and Ying He. Assessing user understanding, perception and behaviour with privacy and permission settings. In Abbas Moallem, editor, *HCI for Cybersecurity, Privacy and Trust*, pages 557–575, Cham, 2023. Springer Nature Switzerland. ISBN 978-3-031-35822-7.

[13] Jialiu Lin, Bin Liu, Norman Sadeh, and Jason I Hong. Modeling {Users'} mobile app privacy preferences: Restoring usability in a sea of permission settings. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 199–212, 2014.

[14] Odnan Ref Sanchez, Ilaria Torre, Yangyang He, and Bart P. Knijnenburg. A recommendation approach for user privacy preferences in the fitness

domain. *User Modeling and User-Adapted Interaction*, 30(3):513–565, July 2020. ISSN 0924-1868. doi: 10.1007/s11257-019-09246-3. URL https://doi.org/10.1007/s11257-019-09246-3.

[15] Paritosh Bahirat, Yangyang He, Abhilash Menon, and Bart Knijnenburg. A data-driven approach to developing iot privacy-setting interfaces. In *Proceedings of the 23rd International Conference on Intelligent User Interfaces*, IUI '18, page 165–176, New York, NY, USA, 2018. Association for Computing Machinery. ISBN 9781450349451. doi: 10.1145/3172944.3172982. URL https://doi.org/10.1145/3172944.3172982.

[16] H Flaherty David. Protecting privacy in surveillance societies. *The Federal Republic of Germany, Sweden, France, Canada, and the United States, North Carolina*, 1989.

[17] S Warren and Louis D Brandeis. The right to privacy. *Harvard Law Review*, 15(5), 1890.

[18] Alan F Westin. Privacy and freedom. *Washington and Lee Law Review*, 25(1):166, 1968.

[19] Irwin Altman. The environment and social behavior: privacy, personal space, territory, and crowding. *ERIC*, 1975.

[20] Daniel J Solove. *Understanding privacy*. Harvard university press, 2010.

[21] Helen Nissenbaum. Privacy as contextual integrity. *Wash. L. Rev.*, 79: 119, 2004.

[22] Hamoun Ghanbari, Bradley Simmons, Marin Litoiu, and Gabriel Iszlai. Exploring alternative approaches to implement an elasticity policy. In *2011 IEEE 4th International Conference on Cloud Computing*, pages 716–723, 2011. doi: 10.1109/CLOUD.2011.101.

[23] Z. Milosevic, W. Chen, A. Berry, and F.A. Rabhi. Chapter 2 - real-time analytics. In Rajkumar Buyya, Rodrigo N. Calheiros, and Amir Vahid Dastjerdi, editors, *Big Data*, pages 39–61. Morgan Kaufmann, 2016. ISBN 978-0-12-805394-2. doi: https://doi.org/10.1016/B978-0-12-805394-2.00002-7. URL https://www.sciencedirect.com/science/article/pii/B9780128053942000027.

[24] Earlence Fernandes, Amir Rahmati, Jaeyeon Jung, and Atul Prakash. Decentralized action integrity for trigger-action iot platforms. 01 2018. doi: 10.14722/ndss.2018.23121.

[25] Camille Cobb, Milijana Surbatovich, Anna Kawakami, Mahmood Sharif, and Lujo Bauer. How Risky Are Real Users' IFTTT Applets? page 25.

[26] Paritosh Bahirat, Yangyang He, Abhilash Menon, and Bart Knijnenburg. A data-driven approach to developing iot privacy-setting interfaces. In *Proceedings of the 23rd International Conference on Intelligent User Interfaces*, IUI '18, page 165–176, New York, NY, USA, 2018. Association for Computing Machinery. ISBN 9781450349451. doi: 10.1145/3172944.3172982. URL https://doi.org/10.1145/3172944.3172982.

[27] Yangyang He, Paritosh Bahirat, Bart P. Knijnenburg, and Abhilash Menon. A data-driven approach to designing for privacy in household iot. *ACM Trans. Interact. Intell. Syst.*, 10(1), September 2019. ISSN 2160-6455. doi: 10.1145/3241378. URL https://doi.org/10.1145/3241378.

[28] Marc Dupuis and Mercy Ebenezer. Help wanted: Consumer privacy behavior and smart home internet of things (iot) devices. In *Proceedings of the 19th Annual SIG Conference on Information Technology Education*, SIGITE '18, page 117–122, New York, NY, USA, 2018. Association for Computing Machinery. ISBN 9781450359542. doi: 10.1145/3241815.3241869. URL https://doi.org/10.1145/3241815.3241869.

[29] Maria Chaparro Osman, Tricia Prior, Summer Rebensky, Andrew Nakushian, and Meredith Carroll. Influencing iot device user privacy behaviors: An empirical study. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 66(1):2078–2082, 2022. doi: 10.1177/1071181322661239. URL https://doi.org/10.1177/1071181322661239.

[30] Tomasz Kosinski. Design challenges of privacy controls for iot systems. 2019. URL https://research.chalmers.se/en/publication/511728.

[31] Hosub Lee and Alfred Kobsa. Confident privacy decision-making in iot environments. *ACM Trans. Comput.-Hum. Interact.*, 27(1), December 2019. ISSN 1073-0516. doi: 10.1145/3364223. URL https://doi.org/10.1145/3364223.

[32] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. User perceptions of smart home iot privacy. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW), November 2018. doi: 10.1145/3274469. URL https://doi.org/10.1145/3274469.

[33] Hosub Lee and Alfred Kobsa. Privacy preference modeling and prediction in a simulated campuswide iot environment. In *2017 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pages 276–285, 2017. doi: 10.1109/PERCOM.2017.7917874.

[34] Anupam Das, Martin Degeling, Daniel Smullen, and Norman Sadeh. Personalized privacy assistants for the internet of things: Providing users with notice and choice. *IEEE Pervasive Computing*, 17(3):35–46, 2018. doi: 10.1109/MPRV.2018.03367733.

[35] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. Informing the design of a personalized privacy assistant for the internet of things. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–13, New York, NY, USA, 2020. Association for Computing Machinery. ISBN 9781450367080. doi: 10.1145/3313831.3376389. URL https://doi.org/10.1145/3313831.3376389.

[36] Yangyang He. Recommending privacy settings for internet-of-things, 2019. URL https://tigerprints.clemson.edu/all_dissertations/2528. All Dissertations. 2528.

[37] Norman Sadeh, Jason Hong, Lorrie Cranor, Ian Fette, Patrick Kelley, Madhu Prabaker, and Jinghai Rao. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and ubiquitous computing*, 13:401–412, 2009.

[38] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun Aerin Zhang, Norman Sadeh, Yuvraj Agarwal, and Alessandro Acquisti. Follow my recommendations: A personalized privacy assistant for mobile app permissions. In *Twelfth symposium on usable privacy and security (SOUPS 2016)*, pages 27–41, 2016.

[39] Heather Richter Lipford, Madiha Tabassum, Paritosh Bahirat, Yaxing Yao, and Bart P Knijnenburg. Privacy and the internet of things. *Modern Socio-Technical Perspectives on Privacy*, 233, 2022.

[40] Bayan Al Muhander, Omer Rana, and Charith Perera. Privify: Designing tangible interfaces for configuring iot privacy preferences, 2024. URL https://arxiv.org/abs/2406.05459.

[41] Leena Alghamdi, Ashwaq Alsoubai, Mamtaj Akter, Faisal Alghamdi, and Pamela Wisniewski. A user study to evaluate a web-based prototype for smart home internet of things device management, 2022. URL `https://arxiv.org/abs/2204.07751`.

[42] Chauncey E Wilson. Triangulation: the explicit use of multiple methods, measures, and approaches for determining core issues in product development. *Interactions*, 13(6):46–ff, 2006.

[43] Richard A Krueger and Mary Anne Casey. *Designing and conducting focus group interviews*, volume 18. Citeseer, 2002.

[44] Vincent R. Waldron. Interviewing for knowledge. *IEEE Transactions on Professional Communication*, PC-29(2):31–34, 1986. doi: 10.1109/TPC.1986.6449030.

[45] Marit Hansen, Meiko Jensen, and Martin Rost. Protection goals for privacy engineering. In *2015 IEEE Security and Privacy Workshops*, pages 159–166, New York, NY, USA, 2015. IEEE. doi: 10.1109/SPW.2015.13.

[46] Piero Romare, Victor Morel, Farzaneh Karegar, and Simone Fischer-Hübner. Tapping into Privacy: A Study of User Preferences and Concerns on Trigger-Action Platforms. In *2023 20th Annual International Conference on Privacy, Security and Trust (PST)*, pages 1–12, 2023.

[47] Piero Romare. User-Driven Privacy Factors in Trigger-Action Apps: A Comparative Analysis with General IoT. In *Privacy and Identity Management. Sharing in a Digital World. Privacy and Identity 2023. IFIP Advances in Information and Communication Technology, vol 695.*, pages 244–264, 2024.

[48] Piero Romare, Farzaneh Karegar, and Simone Fischer-Hübner. Towards Usable Privacy Management for IoT TAPs: Deriving Privacy Clusters and Preference Profiles. In *Under Submission.*