User-Driven Privacy Factors in Trigger-Action Apps: A Comparative Analysis with General IoT

Piero Romare[1]

Chalmers University of Technology
pieror@chalmers.se

Abstract. The growing adoption of Trigger-Action Platforms (TAPs) in the Internet of Things (IoT) paradigm has evolved users' ability to automate their digital environments. However, this automation also introduces potential threats to users' privacy. To enhance users' privacy decisions and develop effective permission management systems, it is crucial to understand users' comprehension of privacy factors in the IoT. This paper presents a literature review on privacy factors in the general IoT environment and compares them with users' priorities and preferences for privacy factors specific to TAPs. To this end, we earlier conducted three Focus Groups (FGs) to gather users' definitions and rankings of privacy factors in the TAPs context. Through the comparison with the general IoT literature, we highlight the similarities and differences in privacy factors between TAPs and traditional IoT applications. The outcomes of this study can inform the designers and developers with an emphasis on privacy-centric IoT TAPs.

1 Introduction

The increasing connectivity and automation facilitated by the Internet of Things (IoT) paradigm offer transformative capabilities across diverse domains such as smart homes, industrial automation, healthcare, and transportation. In particular, Trigger-Action Platforms (TAPs) like IFTTT, Zapier and Microsoft Power Automate have enabled end-users to automatize their own digital environment. Indeed, it is easier than ever to connect multiple services or devices in a workflow by utilizing the formula *"if-this-then-that"*. The opportunity of End-User Development (EUD) [57] allows for simple IoT programming of users' automated behaviour which can eventually save time in their digital activities [58]. While this technology offers a lot of benefits, it also creates potential threats to users' privacy. Despite the users' rights to privacy, a user-friendly and transparent system between the services and devices to which users can connect and automate their IoT apps, such as usable privacy tools [15,68], implemented with users' privacy requirements are still rarely considered. Enhancing the efficacy of users' informed privacy decisions is crucial in light of the growing automation of dataflows [8] within IoT applications and their active pervasiveness. It is essential to begin with an understanding of end users' comprehension of the privacy factors influencing their digital lives [42] to develop usable permission system

that facilitates the control of IoT apps, services, and devices. The protection of users' privacy should be emphasized in particular, in line with their preferences and expectations. In the pursuit of designing usable permission management systems, user-centric approaches that prioritize legal and users' privacy requirements are essential to ensure the effective integration of IoT TAPs technologies into users' digital ecosystems. To create IoT TAPs services and systems that protect privacy, system designers and developers need to comprehend which aspects can affect how individuals perceive their privacy in an IoT context. While there is already a body of research addressing privacy concerns in traditional IoT applications, IoT TAPs represent an evolution of the IoT landscape, introducing automation capabilities that extend beyond established paradigms. We are interested to investigate the following RQ:

– *RQ: What are the users' privacy concerns on the traditional IoT applications and how do they relate to and differ from the users' priorities for privacy factors concerning TAP?*

This paper explores the users' privacy needs and highlights the importance of addressing privacy concerns and preferences in Trigger-Action apps, a subset of the general IoT environment. In the broader context of IoT privacy, it has been shown that users find the protection settings complex since they lack privacy configurations awareness such as types of personal information collected and how data is shared [44]. Individual preferences and expectations as well as social norms play a role in users' level of comfort and acceptance of data collection [47]. To address our research question, we conducted three FGs in the context of TAPs and we compared the themes derived with the previous literature on general IoT.

Contributions To support the privacy by design development of IoT TAPs technology, our contributions are:

– a literature review on the general IoT privacy factors;
– presentation and ranking of privacy factors in the form of privacy preferences and concerns that are prioritized by users regarding IoT TAPs;
– comparison and discussion of how users' privacy factors on IoT TAPs go beyond and complement the privacy factors on general IoT.

Our focus is on supporting the end-users in their privacy permissions management in Trigger-Action applications. By recognizing the users' privacy concerns and preferences, we may build and deploy more reliable and trustworthy IoT systems that satisfy users' privacy expectations and needs.

Organization This paper is organized as follows: in Section 2 we introduce the context of IoT TAPs, in Section 3 we explore the literature review of the traditional IoT, and in Section 4 we present the participants' definitions of the most ranked privacy factors in each FGs. In Section 5 we compare and discuss the similarities and differences between IoT and IoT TAPs and we conclude the overview in Section 6.

2 Background on IoT Trigger-Action Platform

The role of an IoT Trigger-Action Platform (TAP) is to allow the end-users to interconnect more than one IoT device and/or service. Such platforms host the application where the users can design complex rules and processes that are customized to their own needs by specifying triggers that start specific actions. In IFTTT, the creation of the rules is based on a simple formula that is involved in the corresponding "if-this-then-that" transactions. In TAPs, the trigger holds a check on predetermined events (e.g., "if-this"), such as sensor data, user inputs, or time-based triggers. Then, in response to the trigger, the action has the role of carrying out predetermined tasks (e.g., "then-that"). The tasks could entail communicating with web services, controlling IoT devices, or starting events in other applications. This workflow can be illustrated briefly by the following example use case (see Figure 1): *if* new video recorded *then* upload on a social network. The user's personal data is shared between the smart glasses that send the trigger to the online social network that receives the action.

These workflows open a new set of privacy and security risks since the users' integration of heterogeneous systems and services such as third parties that perform actions involving personal user data [39]. Privacy leakages can happen due to improper configurations of the rules such as integrity and secrecy violations [59]. Moreover, even physical safety is at risk (i.e., creating unsafe conditions by turning off the heat in winter), as potential adverse effects can arise from this workflow [10].

3 Literature Review

We conduct a literature review on scientific articles reporting user studies exploring privacy factors in the IoT context. We believe that an extensive investigation of the privacy factors in the traditional IoT context would provide the baseline to confirm previous and elicit new concerns that are more related to IoT TAPs.

3.1 Procedure and Approach

We executed our papers gathering using the following query:

> *(privacy) AND (IoT OR Internet of Things) AND (factor OR preference OR expectation OR concern OR attitude) AND (focus group OR interview OR survey OR questionnaire OR user study)*

We interacted with the web interface of ACM, Scopus, and the API of Semantic Scholar for posing the search query. Overall, 376 papers were retrieved from such scientific databases and we analyzed the title and the abstract of each paper. After the exclusion criteria mentioned below were applied, a total of 53 papers were selected for our goal. Then, we looked in detail at the context, the

factors, the participants, and the research methods to characterise with further information the analysis. Beyond our query, the exclusion criteria were:

- literature review, book chapter, and poster;
- evaluation of a specific application or framework (i.e., dashboard).

The decision to exclude papers focused on evaluating specific applications or frameworks is driven by the fact that these studies often examine contexts characterized by unique features, functionality, and user interfaces, which can particularly be designed just for these particular scenarios. The details about the papers retrieved from scientific databases are the following: Scopus [1] resulted in 262 candidates and 40 of them were selected. ACM [2] resulted in four candidates and one was selected and two of them were duplicates. Semantic Scholar API [3] resulted in 110 candidates and 12 were selected and two of them were duplicates. The API of Semantic Scholar provides parameters that are not included in the web interface, such as applying the query in the abstract. The total percentage of the papers selected is 14%. One challenge during the paper selection phase was the overlap of the taxonomy of a survey intended as a questionnaire and as a literature review. For our scope, we refer to a survey as a questionnaire.

3.2 Categorization of papers

Contexts and Participants: We observed a recurring pattern in the selected papers, indicating a shared context that can be extrapolated to smart home environments, general IoT settings, and healthcare IoT applications. Furthermore, in the selected user studies pertaining to our research query, we identified three primary groups of participants. These groups can be categorized as the Owners of IoT devices, Experts in the field, and potential End-Users. In Section 5 we refer to End-Users as potential End-Users that can include Owners or not Owners of an IoT device. Certain studies included participants who belonged to more categories (e.g., these categories are not mutually exclusive).

Research Method and Privacy Preferences: The research methods of the articles that we selected for this literature review involved questionnaires and qualitative methods such as focus groups, semi-structural interviews, and in-lab and field studies. Questionnaire has been widely used as a quantitative research method. We organize the presentation of the factors exploited in the papers selected for this literature review by distinguishing quantitative and qualitative methods. In the Appendix, in Tables 4 and 5, we describe the privacy factors considering the dimensions or constructs in the questionnaires, in Table 6 the themes and codes in the focus groups as well as in the interviews, and in Table 3 when the paper referring to mixed-methods. In these tables in the Appendix 7 we mapped the privacy factors reported in the papers selected with our findings in Section 4.

[1] https://www.scopus.com/search/form.uri?display=advanced
[2] https://dl.acm.org/action/doSearch
[3] https://api.semanticscholar.org/api-docs/

4 Focus Groups

We conducted three FGs to explore the privacy factors related to the users' concerns and preferences for using IoT TAPs [54]. We recruited 15 participants for our three FGs on the university campus and via personal networks, who were not limited to university staff members and students. The recruitment message gave a brief introduction to TAP platforms and described the study as an investigation of consumers' views and opinions of IoT application scenarios involving IoT Trigger-Action Platforms.

In summary, we organized each FG session consisting of three parts:

1. a prologue session where participants were welcomed, demographic questions were asked, and their consent was obtained.
2. Following an introductory session, a subsequent general discussion pertaining to TAPs was conducted, which was then followed by a focused discussion exploring various TAP scenarios.
3. The FG concluded with the participants' description of privacy factors and a sorting task based on these.

For the purpose of this work, we discuss in detail the sorting task (see also Section 4.1). The listing of such factors happened after general and scenario-based discussions around users' opinions, preferences, and concerns about TAPs and three specific related scenarios (an example is in Appendix 7). These scenarios were designed to illustrate different features of IoT apps and involved trigger-action recipes with at least two entities, including an IoT device, to highlight possible privacy concerns and ensure the validity of IoT app settings with data flow between entities. We agreed with the participants about terms and definitions of perceived privacy concerns and preferences extracted and we asked for potential improvements to such a list in a collaborative way. Before the conclusion, we got the ranks of the sorting task and the explanations from the participants of reason in the choice of the first ranked factor.

Fig. 1. When a new video is recorded with smart glasses then upload on social media.

4.1 Definitions and ranking of privacy factors in TAPs

To enrich our literature review, we merged the research findings with the attitudinal priorities of users in the context of IoT TAPs and related previous works. To achieve this objective, we present the participants' description of privacy factors that happened after the scenario-based discussion to ensure comprehensiveness and design privacy-enhancing approaches. We asked the participants to summarize and list the factors that arose in the discussion and named by the moderators. Consider that the following privacy factors were described immediately after the discussions from the notes of the moderators. Furthermore, we asked the participants to rank the factors based on how much of an impact each element had on the utilization of the Trigger-Action applications. This sorting task activity should not be interpreted quantitatively [19] due to both the small number of participants and the differences in the number of factors and meaning achieved from the FGs (e.g., a definition discussed in the FG1 may not be discussed in the FG2). In Table 1 we list the set of the top-ranked privacy factors and the description given in a collaborative manner among the participants. Six participants were concerned most with the control of the automation of the Trigger-Action applications in order to review what was going to be shared. Trust was selected as the first-ranked privacy factor by three participants as an aspect that influences confidence in the adoption and usage of IoT devices and the relative manufacturers. Two participants selected data sensitivity by referring to sensitive and personal information as well as financial or health data that have various challenges and then perceptions of individuals' privacy.

Table 1. Full list of participants' top-ranked factor and its description

FGs	Participants	Privacy Factors	Participants Quotes
1	P1	Level of Experience	The knowledge of what is possible, in the IoT has influence in the privacy preferences.
1	P2	Data Controller	Entity in charge of controlling data. In Europe your data controller must comply with the GDPR.
1	P3, P5	Data Sensitivity	How sensitive is the activity? Because maybe this activity could involve more or less sensitive data.
1	P4	Security of the workflow	The whole workflow must be sure that everything is in the device, like end to end for example.
2	P6, P7, P8, P9, P10	Control before the final action	That's quite a goal to be in control. First I want to see and then being able to take action.
2	P11	Trust in the device	You buy the device and you need to trust what is in and how it works.
3	P12	User Consent	People acceptance, or what allow your data participations.
3	P13, P15	Trust	it's more like in a general sense. Do you trust some companies or not? It's binary.
3	P14	Control before the final action	I would like to press the button It's me that decide when I share.

5 Discussion

In this Section, we discuss the papers selected for this literature review to compare the privacy factors in the traditional IoT with our findings presented in Section 4 and IoT TAPs previous works for addressing our research question. We organize the following paragraphs by dividing questionnaires and interviews as delineated in Section 3. We summarize the comparison in Table 2.

General IoT Privacy Factors - Questionnaire: In the realm of smart home environments, the assessment of user acceptability depends on the principles of contextual integrity concerning the flow of information. This entails an examination of information flows, encompassing the sender, recipient, attributes, subject, and transmission principles [7]. The intention to embrace IoT technology is fundamentally influenced by perceived utility, ease of use, and privacy risk perception [16]. Additionally, the decision to replace older smart devices with newer ones demonstrates a substantial correlation with perceived utility [36]. In conjunction with perceived utility, trust in IoT devices emerges as another pivotal determinant in their adoption and usage within domestic settings [26]. An inherent optimism bias may mitigate concerns related to data practices, as individuals often hold misconceptions regarding data collection, sharing, protection, and storage when compared to actual practices [2]. Moreover, the lack of awareness, unfamiliarity, and complexity of IoT systems influence the consumers' decisions regarding device purchase [63]. The resistance to IoT adoption is accentuated by apprehensions surrounding adverse consequences, particularly within the framework of perceived risk models. Factors encompassing privacy and psychological risks show a positive correlation with resistance to IoT device adoption [24]. Anxiety resulting from potential security vulnerabilities and their associated repercussions further diminishes the inclination to use such devices [9]. Additionally, concerns regarding data sharing with third parties and data retention impact the consumers' intent to purchase IoT devices [18]. The adoption of IoT devices exhibits country variations, across the United States, Europe, and India, where a key influencer in these adoption disparities is the level of trust in governmental bodies [32]. Additionally, concerns related to transparency and user consent are shared across these regions, with similar findings concerning trust in companies reported in the UK [31]. Indeed, in a survey with over 2000 participants explored the end-users' willingness to share personal data to the IoT services [56] it has been found the importance of building trust in those services. Enhanced transparency and effective data control mechanisms positively impact data sharing practices [67,62]. Furthermore, parental apprehensions regarding their children's privacy revolve around surveillance by IoT companies, as evidenced in [40]. Older adults, who stand to benefit from IoT-enabled living support, encounter adoption barriers caused by technological proficiency and physical limitations [60,50]. An exploration of healthcare IoT device adoption, as detailed in [3], underscores the role of social influence as a positive factor, while a lack of control over personal data emerges as an obstacle. A scenario of crime prevention and healthcare was compared on the perceptions of privacy

and security risks and third-party seal shape the security risk perception when it concerns the healthcare preventive scenario [6]. The usage of smart devices extends beyond owners, and an additional vulnerable population comprises bystanders. Special attention is directed toward safeguarding their privacy and ensuring adequate information dissemination [41,5].

General IoT Privacy Factors - Interviews and Focus Group: the data ownership is a prominent privacy concern in IoT devices [45]. This issue is further exacerbated by the absence of robust regulatory frameworks within the domain of diabetes-related IoT devices, a concern elucidated through interviews conducted with healthcare experts, patients, and industry stakeholders [12]. There is an identified expectation on the idea of the Privacy by Design for IoT to guide the benefits and risks for the users [38]. Notably, this call for regulation is amplified by the phenomenon where users place their trust in IoT manufacturers to safeguard their privacy, yet rarely engage in verification of the implementation of such protective measures [69]. In the Australian context, experts emphasize robust regulation because of their concerns about vulnerable communities and the implications related the IoT devices [23]. In a smart campus, the students are concerned as well for the vulnerable communities, the relative inequalities, and the potential data breaches and third-party data sharing [11]. User control and reduced cognitive load, facilitated by privacy assistants, have been met with positive responses, as revealed in end-user interviews [14]. Informed decision-making with respect to IoT device purchases is encouraged through the solicitation of privacy information priorities from experts, with a particular focus on security mechanisms and data handling practices [17]. The lack of awareness regarding privacy issues is a salient concern among smart home end-users, many of whom possess a limited comprehension of associated security risks. Such awareness typically materializes following discussions with peers, exposure to news articles, or observations of unexpected device behaviors [66,19]. Longitudinal interviews conducted within home IoT environments have identified perceived benefits and data sensitivity as key factors influencing users' privacy considerations [1]. Furthermore, through the execution of four focus groups involving both end-users and IoT experts, four overarching themes pertaining to privacy concerns have been identified. These themes encompass data collection practices, the security of IoT devices, data storage mechanisms, and the subsequent utilization of collected data [49].

Privacy Factors in TAPs In our previous work, we conducted four focus groups [54]. The thematic analysis resulted in 9 themes that correspond to privacy factors such as transparency, control, trust, privacy of bystanders, risks, data minimization, confidentiality, privacy/security trade-off, potential misuse, and unexpected purposes or consequences. Similarly, in two FGs conducted earlier by Liu et al. related to smart speakers a task for the participants was to provide their concerns about privacy factors using a 10-Likert scale [37] including the collection of personal information, location, behavioral information and the consequent potential surveillance that includes unfair processing, excessive user profiling and

third-parties sharing. Using implicit and explicit security and privacy priming strategies on 20 trigger-action rules, it was shown that perceived benefits and trust beliefs in online companies are two predictors of riskier rule selection [46]. Contextual factors such as trigger and action locations, when the application runs, the online services involved, who can use and who is around were used to understand the impact on concerns such as leakage of sensitive data and unauthorized access [55]. Individuals' privacy preferences were studied using vignettes. The data type, retention time, third-party sharing, perceived benefit and the location of the data collection are privacy factors that affect the concerns. Indeed, their qualitative analysis confirms that users are uncomfortable when the data collection involves biometric data and occurs in private spaces [48]. In [13] participants were exposed to secrecy or integrity risks of TAP applets and provided experiences about accidental sharing of private information, including incidental users, and about safety and security risks that belong to the control of their devices or the execution of the applications.

Comparing IoT and TAPs privacy factors: Our sorting task analysis, as illustrated in Table 1, underscores the critical roles of that control and transparency are crucial in supervising the automation process. As our participants' priorities show, this encompasses and extends to (pre)control before the final action (from P6 FG2: "first I want to see and then being able to take action") and transparency of the data controller (from P2 FG1: "the entity in charge of controlling data") in dealings with third parties, where third-party integration significantly enhances the capabilities of TAPs. Users can actively select and integrate specific triggers and actions offered by third-party services to construct their automation workflows. However, in the broader IoT, third parties and in TAPs cases also third parties performing the triggered actions may not always be visible or directly accessible to users. The escalating complexity and volume of self-executing data exchanged among an increasing number of recipients continue to expand, along with the functionalities of these systems, users are confronted with the challenge of maintaining a comprehensive overview of data flows and processes. In the traditional IoT context, the concepts of data storage and retention time predominantly relate to the management of sharing settings, while in TAPs, since the potential secrecy and integrity violations in TAP applications, users should be given the ability to control and minimize the data to be shared by selecting when, where, or what should trigger the execution of automated workflows using conditional and contextual access and withhold sharing for a time period. These factors are intrinsically held to granting users granular control over both data sharing and app configuration settings. Due to misconfigured settings accidental data sharing and reliability concerns can occur, and in TAPs, the amount of interconnections between services and devices increases the likelihood of accidental data sharing and unexpected device behaviour.
A common priority relates to the crucial importance of trust in IoT devices, IoT manufacturers, and the regulations and certifications established by governments. This priority is rooted in the imperative need to address concerns related to surveillance, customer monitoring and profiling also in relation with

the bystanders, incidental or secondary users. Previous studies have shown that end users often prioritize the benefits offered by IoT technologies over privacy risks [61,52,53,25]. However, there is a common demand for security countermeasures against hackers and data leakage, and users express a desire for updates and standardization within the IoT environment.
In Table 2, the factors mapped are not precisely identical and should be interpreted with caution. The column representing IoT TAPs Privacy Factors is structured based on themes and codes derived from the analysis in our focus groups [54].

Table 2. Mapping from traditional IoT to Trigger-Action IoT

Authors	IoT Privacy Factors	IoT TAPs Privacy Factors
[2,18,34,5,56,27,1,66]	Data Storage, Retention Time	Data Minimization: conditional and contextual access; minimize data to be shared.
[3,23,60,41]	Social Norms	Potential Misuse and Unexpected Consequences or Purpose: social stigma; Privacy of Bystanders: Consequences for vulnerable populations.
[16,36,61,52,53,25,30] [60,50,66,26]	Perceived Usefulness Perceived Ease of Use Lack of Awareness, Unfamiliarity, Complexity	Privacy/Security trade-off: convenience and usability.
[62,67,60,51,62] [32,31,9,33]	Control and Consent	Control: control before the final action, granular control in the data sharing, granular control in the configuration.
[19,25,26,11]	Unexpected device behavior	Potential Misuse and Unexpected Consequences or Purpose: reliability concerns for automated trigger, accidental data sharing, sensitivity due to unspecified context, unexpected data tracking/sharing/processing.
[18,6,45,11,3,26,40,43] [32,60]	Third-Parties and Transparency	Transparency: transparency of data recipients, general overview
[41,5,64]	Privacy of the Bystanders	Privacy of the Bystanders: transparency and consent for bystanders
[12,38,17,22]	Lack of Regulations	Trust: assurance guarantees
[26,31,56,69,53,32,40,63]	Trust in the IoT device	Trust in the IoT device, Surveillance
[63,16,53,41,56,31,61,65,23]	Security risks	Security risks: hackers, data leaks.

6 Conclusion

In this paper, we have undertaken a comparative analysis of privacy factors within the context of Trigger-Action Apps (TAPs) in IoT and the traditional IoT paradigm. The privacy concerns specific to TAPs were derived from insights

gathered through three focused group discussions, and the prioritization of these concerns was determined by participants in our prior study [54]. Simultaneously, we conducted a comprehensive literature analysis to identify privacy factors in the broader IoT landscape. Our research underscores the critical privacy factors essential for management and protection in the IoT TAPs. These factors encompass the main characteristic of TAPs which is automation with the imperative need for user control and transparency to oversee the automation process effectively. Moreover, it emphasizes the necessity for granular control over data sharing and app configuration to enable users to maintain the integrity of their data. Furthermore, our findings stress the importance of minimizing unintentional data sharing and reliability concerns, thereby enhancing the overall security of IoT systems. Lastly, trust in IoT devices, manufacturers, and regulatory frameworks emerges as a crucial component in safeguarding user privacy. To support the privacy by design development of IoT technology, we want to emphasize the importance of supporting the end-users in their privacy permissions management in Trigger-Action applications. By recognizing the potential obstacles and threats, as well as the privacy factors that matter to the users, we may build and deploy more reliable and trustworthy IoT systems that satisfy users' privacy expectations and needs.

Acknowledgements: This work was partially supported by the Wallenberg AI, Autonomous Systems and Software Program (WASP) funded by the Knut and Alice Wallenberg Foundation. I would like to thank my supervisor Simone Fischer-Hübner and my co-supervisor Farzaneh Karegar for their helpful feedback and advice who together with Victor Morel also helped with conducting the focus groups and thematic analysis.

References

1. Abbott, J., Dev, J., Kim, D., Gopavaram, S., Iyer, M., Sadam, S., Mare, S., Ringenberg, T., Andalibi, V., Camp, L.J.: Privacy Lessons Learnt from Deploying an IoT Ecosystem in the Home. In: EuroUSEC 2022 (2022)
2. Al-Ameen, M.N., Chauhan, A., Ahsan, M.A.M., Kocabas, H.: A look into user's privacy perceptions and data practices of IoT devices. IJICS (2021)
3. Alaiad, A., Zhou, L.: Patients' Adoption of WSN-Based Smart Home Healthcare Systems: An Integrated Model of Facilitators and Barriers. ProComm (2017)
4. Alraja, M.: Frontline healthcare providers' behavioural intention to Internet of Things (IoT)-enabled healthcare applications: A gender-based, cross-generational study. Technological Forecasting and Social Change (2022)
5. Alshehri, A., Spielman, J., Prasad, A., Yue, C.: Exploring the Privacy Concerns of Bystanders in Smart Homes from the Perspectives of Both Owners and Bystanders. Proceedings on Privacy Enhancing Technologies (2022)
6. Ando, R., Shima, S., Takemura, T.: Analysis of Privacy and Security Affecting the Intention of Use in Personal Data Collection in an IoT Environment (2016)
7. Apthorpe, N., Shvartzshnaider, Y., Mathur, A., Reisman, D., Feamster, N.: Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. IMWUT (2018)

8. Brandtzaeg, P.B., Pultier, A., Moen, G.M.: Losing control to data-hungry apps: A mixed-methods approach to mobile app privacy. Soc. Sci. Comput. Rev. (2019)
9. Cannizzaro, S., Procter, R., Ma, S., Maple, C.: Trust in the smart home: Findings from a nationally representative survey in the UK. PLOS ONE (2020)
10. Celik, Z.B., McDaniel, P., Tan, G.: Soteria: Automated IoT safety and security analysis. In: USENIX ATC 18 (2018)
11. Cheong, P.H., Nyaupane, P.: Smart campus communication, IoT, and data governance: Understanding student tensions and imaginaries. Big Data Soc (2022)
12. Cleveland, S.M., Haddara, M.: Internet of Things for diabetics: Identifying adoption issues. Internet of Things (2023)
13. Cobb, C., Surbatovich, M., Kawakami, A., Sharif, M., Bauer, L., Das, A., Jia, L.: How risky are real users' IFTTT applets? In: Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020) (2020)
14. Colnago, J., Feng, Y., Palanivel, T., Pearman, S., Ung, M., Acquisti, A., Cranor, L.F., Sadeh, N.: Informing the Design of a Personalized Privacy Assistant for the Internet of Things. In: CHI (2020)
15. Corcella, L., Manca, M., Paternò, F., Santoro, C.: A visual tool for analysing iot trigger/action programming. In: HCSE (2018)
16. Dong, X., Chang, Y., Wang, Y., Yan, J.: Understanding usage of Internet of Things (IOT) systems in China. Information Technology & People (2017)
17. Emami-Naeini, P., Agarwal, Y., Cranor, L.F., Hibshi, H.: Ask the Experts: What Should Be on an IoT Privacy and Security Label? In: S&P (2020)
18. Emami-Naeini, P., Dheenadhayalan, J., Agarwal, Y., Cranor, L.F.: Which Privacy and Security Attributes Most Impact Consumers' Risk Perception and Willingness to Purchase IoT Devices? In: S&P (2021)
19. Emami-Naeini, P., Dixon, H., Agarwal, Y., Cranor, L.F.: Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. In: CHI (2019)
20. Foltz, C.B., Foltz, L.: Mobile users' information privacy concerns instrument and IoT. Information & Computer Security (2020)
21. George, J.F., Chen, R., Yuan, L.: Intent to purchase IoT home security devices: Fear vs privacy. PLOS ONE (2021)
22. Gopalakrishna, N.K., Anandayuvaraj, D., Detti, A., Bland, F.L., Rahaman, S., Davis, J.C.: "If security is required". In: Proceedings of the 4th International Workshop on Software Engineering Research and Practice for the IoT (2022)
23. Harkin, D., Mann, M., Warren, I.: Consumer IoT and its under-regulation: Findings from an Australian study. Policy & Internet (2022)
24. Hong, A., Nam, C., Kim, S.: What will be the possible barriers to consumers' adoption of smart home services? Telecommunications Policy (2020)
25. Hsu, C.L., Lin, J.C.C.: An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives. Computers in Human Behavior (2016)
26. Jaspers, E.D.T., Pearson, E.: Consumers' acceptance of domestic Internet-of-Things: The role of trust and privacy concerns. Journal of Business Research (2022)
27. Jeon, H., Lee, C.: Internet of Things Technology: Balancing privacy concerns with convenience. Telematics and Informatics (2022)
28. Kim, D., Park, K., Park, Y., Ahn, J.H.: Willingness to provide personal information: Perspective of privacy calculus in IoT services. Comput. Hum. Behav. (2019)
29. Kim, S., Yoon, J.: An Exploratory Study on Consumer's Needs on Smart Home in Korea. In: Design, User Experience, and Usability: Technological Contexts (2016)
30. Kowatsch, T., Maass, W.: Critical Privacy Factors of Internet of Things Services: An Empirical Investigation with Domain Experts. In: LNBIP (2012)

31. Kulyk, O., Milanovic, K., Pitt, J.: Does My Smart Device Provider Care About My Privacy? Investigating Trust Factors and User Attitudes in IoT Systems. In: Proceedings of the 11th NordiCHI (2020)
32. Lafontaine, E., Sabir, A., Das, A.: Understanding People's Attitude and Concerns towards Adopting IoT Devices. In: Extended Abstracts of the 2021 CHI (2021)
33. Lee, A.R.: Investigating the Personalization–Privacy Paradox in Internet of Things (IoT) Based on Dual-Factor Theory: Moderating Effects of Type of IoT Service and User Value. Sustainability (2021)
34. Lee, H., Kobsa, A.: Privacy preference modeling and prediction in a simulated campuswide IoT environment. In: PerCom (2017)
35. Lee, S., Suk, J., Ha, H.R., Song, X.X., Deng, Y.: Consumer's Information Privacy and Security Concerns and Use of Intelligent Technology. In: AISC (2020)
36. Lenz, J., Bozakov, Z., Wendzel, S., Vrhovec, S.: Why people replace their aging smart devices: {A} push–pull–mooring perspective. Computers & Security (2023)
37. Liu, Y.l., Huang, L., Yan, W., Wang, X., Zhang, R.: Privacy in AI and the IoT: The privacy concerns of smart speaker users and the Personal Information Protection Law in China. Telecommunications Policy (2022)
38. Luthfi, A., Emigawaty, E.: Towards Privacy by Design on the Internet of Things (IoT) Use: A Qualitative Descriptive Study. IJHISI (2022)
39. Mahadewa, K., Zhang, Y., Bai, G., Bu, L., Zuo, Z., Fernando, D., Liang, Z., Dong, J.S.: Identifying privacy weaknesses from multi-party trigger-action integration platforms. In: 30th ACM SIGSOFT (2021)
40. Mann, M., Wilson, M., Warren, I.: Smart Parenting? The Internet of Things, Children's Privacy, and Data Justice. Int. J. Child. Rights (2022)
41. Marky, K., Gerber, N., Pelzer, M.G., Khamis, M., Mühlhäuser, M.: "You offer privacy like you offer tea": Investigating Mechanisms for Improving Guest Privacy in IoT-Equipped Households. Proceedings on Privacy Enhancing Technologies (2022)
42. Marreiros, H., Gomer, R.C., Vlassopoulos, M., Tonin, M., m.c. schraefel: Exploring user perceptions of online privacy disclosures. In: IADIS (2015)
43. Maus, B., Olsson, C.M., Salvi, D.: Privacy Personas for IoT-Based Health Research: A Privacy Calculus Approach. Frontiers in Digital Health (2021)
44. Menard, P., Bott, G.J.: Analyzing IOT users' mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment. Comput Secur (2020)
45. Montanari, A., Mashhadi, A., Mathur, A., Kawsar, F.: Understanding the Privacy Design Space for Personal Connected Objects. In: eWiC (2016)
46. Morgan, P.L., Collins, E.I., Spiliotopoulos, T., Greeno, D.J., Jones, D.M.: Reducing risk to security and privacy in the selection of trigger-action rules: Implicit vs. explicit priming for domestic smart devices. International Journal of Human-Computer Studies (2022)
47. Naeini, P.E., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L.F., Sadeh, N.M.: Privacy expectations and preferences in an iot world. In: SOUPS (2017)
48. Naeini, P.E., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L.F., Sadeh, N.M.: Privacy expectations and preferences in an iot world. In: Symposium On Usable Privacy and Security (2017)
49. Padyab, A., Ståhlbröst, A.: Exploring the dimensions of individual privacy concerns in relation to the Internet of Things use situations. Digit. Policy Regul. Gov. (2018)
50. Pal, D., Papasratorn, B., Chutimaskul, W., Funilkul, S.: Embracing the Smart-Home Revolution in Asia by the Elderly: An End-User Negative Perception Modeling (2019), iEEE Access

51. Ponciano, L., Barbosa, P., Brasileiro, F., Brito, A., Andrade, N.: Designing for Pragmatists and Fundamentalists. In: IHC (2017)
52. Psychoula, I., Singh, D., Chen, L., Chen, F., Holzinger, A., Ning, H.: Users' Privacy Concerns in IoT Based Applications. In: SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI (2018)
53. Railean, A., Reinhardt, D.: Life-Long Privacy in the IoT? Measuring Privacy Attitudes Throughout the Life-Cycle of IoT Devices. In: IFIP Advances in Information and Communication Technology (2018)
54. Romare, P., Morel, V., Karegar, F., Fischer-Hübner, S.: 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) (2023)
55. Saeidi, M., Calvert, M., Au, A., Sarma, A., Bobba, R.B.: If this context then that concern: Exploring users' concerns with IFTTT applets. CoRR (2020)
56. Sah, J., Jun, S.: The Role of Consumers' Privacy Awareness in the Privacy Calculus for IoT Services. International Journal of Human–Computer Interaction (2023)
57. dos Santos, M.A., Villela, M.L.B.: Characterizing end-user development solutions: A systematic literature review. In: Interacción (2019)
58. Spahn, M., Dörner, C., Wulf, V.: End user development: Approaches towards a flexible software design. In: European Conference on Information Systems (2008)
59. Surbatovich, M., Aljuraidan, J., Bauer, L., Das, A., Jia, L.: Some recipes can do more than spoil your appetite: Analyzing the security and privacy risks of ifttt recipes. In: Proceedings of the 26th International Conference on WWW (2017)
60. Wang, S., Bolling, K., Mao, W., Reichstadt, J., Jeste, D., Kim, H.C., Nebeker, C.: Technology to Support Aging in Place: Older Adults' Perspectives. Healthcare (2019)
61. Wang, X., McGill, T.J., Klobas, J.E.: I Want It Anyway: Consumer Perceptions of Smart Home Devices. Journal of Computer Information Systems (2018)
62. Wickramasinghe, C.I., Reinhardt, D.: A Survey-Based Exploration of Users' Awareness and Their Willingness to Protect Their Data with Smart Objects. In: Privacy and Identity Management. Data for Better Living: AI and Privacy (2020)
63. Williams, M., Nurse, J.R.C., Creese, S.: Privacy is the Boring Bit: User Perceptions and Behaviour in the Internet-of-Things. In: PST (2017)
64. Yao, Y., Basdeo, J.R., Mcdonough, O.R., Wang, Y.: Privacy Perceptions and Designs of Bystanders in Smart Homes. Proc. ACM Hum. Comput. Interact. (2019)
65. Yildirim, H., Ali-Eldin, A.M.T.: A model for predicting user intention to use wearable IoT devices at the workplace. J. King Saud Univ. Comput. Inf. Sci. (2019)
66. Zeng, E., Mare, S., Roesner, F.: End user security & privacy concerns with smart homes. In: USENIX (2017)
67. Zhang, Y., Wang, D., Mu, J., Yang, Z.: Effects of Transparency of Service Design on User Attitude Toward 'Exchanging Information for Service'. In: CCIS (2019)
68. Zhao, V., Zhang, L., Wang, B., Lu, S., Ur, B.: Visualizing differences to improve end-user understanding of trigger-action programs. CHI EA '20 (2020)
69. Zheng, S., Apthorpe, N., Chetty, M., Feamster, N.: User Perceptions of Smart Home IoT Privacy. Proc. ACM Hum. Comput. Interact. (2018)

7 Appendix

Table 3. Summary of Privacy Factors in IoT context with mixed-methods

Authors	Contexts	Participants	Privacy Factors
Wang et al. [60]	Healthcare IoT	End-Users	Sensitivity of Data Types, Usability, Consequences for Vulnerable Populations, General Overview, Control, Trust, Lack in Standardization, Technology Knowledge
Zhang et al. [67]	General IoT	End-Users	Sensitivity of Data Types, Consent, Trust in Controller Process Recipient, Convenience
Psychoula et al. [52]	General IoT	End-Users	Customer Monitoring, Unexpected Data Tracking/Sharing, Sensitivity of Data Types, Trust, Hackers, Consent, Third-Parties, Privacy/Security Trade-off, Convenience, Reliability Concerns
Alaiad et al. [3]	Healthcare IoT	Owners of IoT Device, Experts	Confidentiality, Data Leaks, Customer Monitoring, Utility, Control, Unauthorized Access, Sensitivity of Data Types, Third-Parties
Gopalakrishna et al. [22]	General IoT	Experts	Standardization, Hackers, Encryption, Trustworthy Data, Assurance Guarantees
Al-Ameen et al. [2]	General IoT	End-Users	Sensitivity of Data Types, Third-Parties, Data Protection (Encryption of Communication, Encryption of data at rest), Conditional and Contextual Access, Storage Period
Williams et a. [63]	General IoT	End-Users	Granular Control in the Configuration, Customer Monitoring, Consent, Unexpected Data Tracking/Sharing, Surveillance, Third-Parties, Usability, Encryption, Trade-off Privacy/Security, Social Norms, Cognitive Load
Marky et al.[41]	Smart Home	Owners of IoT Device	Protecting Bystanders, Data Deletion, Transparency and Consent for Bystanders, Security Risks, Convenience, Usability, Intrusiveness, Control, General Overview, Social Norms, Sensitivity of Data Types, Data Leaks

Table 4. Summary of Privacy Factors in IoT context with questionnaires

Authors	Contexts	Participants	Privacy Factors
Railean et al. [53]	General IoT	End-Users	Hackers, Trust in IoT Device, Usability, Assurance Guarantees, Clear Privacy Policy, Convenience, Trust in Governments, Updates
Kowatsch et al. [30]	General IoT	Experts	Privacy Risk, Privacy Concerns, Trust in organization, Expected usefulness, Personal interest, Intention to use, Willingness to provide info
Ponciano et al. [51]	General IoT	End-Users	Collection of Personal Data, Data inference, Third-Parties, Trust in Governments Utility, Granular Control in Data Sharing
Lee [34]	General IoT	End-Users	Conditional and Contextual Access, Trust in Governments, Trust in IoT Manufacturer, Sensitivity of Data Types, Convenience
Dong et al [16]	General IoT	Owners of IoT Device, Experts	Utility, Security Risks, Convenience, Reliability, Data Leaks, Hackers
Hsu et al. [25]	General IoT	End-Users	Utility, Unexpected Data Tracking/Sharing, Trust in Controller Process Recipient, User Consent, Third-Parties, Reliability, Lack of Standardization
Ando et al. [6]	General IoT	End-Users	Usability, Third-Parties, Customer Monitoring, Assurance Guarantees, Unexpected Data Tracking/Sharing, Surveillance, User Control, Transparency of Data Recipients, General Overview
Alshehri et al. [5]	Smart Home	Owners of IoT Device	protecting Bystanders, Data disclosures Awareness to Bystanders, Sensitivity of Data Types, Consent for Bystanders Utility, Withhold Sharing for a Time period, consequences on Vulnerable population
Apthorpe et al. [7]	Smart Home	End-Users	Trust in Controller Process Recipient, Consent, Notification, Confidentiality, Retention Time, Third-Parties, sensibility of Data Types
Cannizzaro et al. [9]	Smart Home	End-Users	Intention to use, Trust in Security, Data Leaks, Unexpected Data Tracking/Sharing, Trust in IoT Manufacturer, Trust in ioT Device, Reliability Concerns
Wickramasinghe et al. [62]	General IoT	End-Users	Third-Parties, Unexpected Data Tracking/Sharing, Granular Control in the Data Sharing, Transparency, General Overview, Data Access, Consent, Data minimization
Lenz et al. [36]	Smart Home	Owners of IoT Device	Privacy Concern, Switching Costs, Perceived Usefulness, Ease of Use, Subjective Norm, Facilitating Conditions, Hedonic Motivation, Switching Intention
Sah et al. [56]	Smart Home	End-Users	Data Collection Data Storage, Data Controller, Retention Time, Purpose of Collection, Anonymity, Data Leaks, Misuse of Data, Third Parties, Data Deletion, Data Minimization, Security
Jeon et al. [27]	General IoT	End-Users	Hacker, Data Minimization, Data Deletion, Third-Parties
Jaspers et al. [26]	Smart Home	End-Users	Perceived Usefulness, Perceived Ease of Use, Third-Parties, Excessive Collection, Collection Unawared, Prior Knowledge, Subjective Norms, Trust
Mann et al. [40]	Smart Home	End-Users	Data Controller, Data Deletion, Safety, Consequences of Vulnerable populations, Data Storage, Surveillance Awareness, Consent
Alraja [4]	Healthcare IoT	End-Users	Privacy (Potential Misuse, Third-Parties, Attitude, Conditional and Contextual Access, Security, Safety of Execution, Trust, Risk perception, Perceived Behavioral Control, Behavioral Intention

Table 5. Summary of Privacy Factors in IoT context with questionnaires

Authors	Contexts	Participants	Privacy Factors
Maus et al. [43]	Healthcare IoT	Owners of IoT Device	Unauthorized Access to Sensitive Data, Perceived Benefits, Surveillance, Control, Transparency, Trust, Transparency of Data Recipients, Usability
Lee [33]	Smart Home	End-Users	Perceived Benefits, Data Leaks, Control unexpected Data Tracking/Sharing, Customer Monitoring, Trust in Control Process Recipient, Third-Parties
George et al. [21]	Smart Home	End-Users	Data Access, Privacy of Bystanders
Lafontaine et al. [32]	General IoT	End-Users	Trust in IoT Manufacturer, Trust in Governments, Hackers, Unexpected Data Tracking/Sharing (Consent), Perceived benefits, Security Risks
Emami-Naeini et al. [18]	Smart Home	End-Users	Third-Parties, Access Control, Sharing frequency, Data Retention, Data linkage, Data Inference, Security, Control, Trust in Recipient, Security update, Usability, Purpose of Collection
Kulyk et al. [31]	Smart Home	End-Uses	Usability, Confidentiality, Hackers, Encryption, Transparency, User Control, Unauthorised Data Access, Trustworthy safe service, Trust in Controller Process Recipient
Wang et al. [61]	Smart Home	End-Users	Perceived Benefits, Perceived Risk, Control, Confidentiality, Security Risk, Hackers, Utility
Foltz et al. [20]	General IoT	End-Users	Surveillance, Customer Monitoring, Unexpected Data Tracking/Sharing, Secondary use of information, Third-Parties
Hong et al. [24]	Smart Home	End-Users	Security Risk, Potential Misuse, Data Access, Data Leaks, Control
Lee et al. [35]	General IoT	End-Users	User Consent, Customer Monitoring, Data Leaks Unexpected Data Tracking/Sharing, Hackers, Reliability Concerns, Excessive Collection of Personal Information, Third-Parties, increased Vulnerability due to multiple connectivity, Reliability Concerns massive spread of damage due to increased connectivity, malware and ransomware
Yildirim et al. [65]	General IoT	End-Users	Improper Access, Secondary Use, Risks, Trust, Utility, Consent, Unexpected Data Tracking/Sharing, Encryption, Third-Parties, Customer Monitoring
Kim et al. [28]	General IoT	End-Users	Perceived Benefits, Third-Parties, Potential Misuse, Unexpected Data Tracking/Sharing, Hackers, Trust in Governments, Sensitivity of Data Types, number of IoT service, Usability
Pal et al. [50]	Smart Home	End-Users	Convenience, Reliability, Control, User Consent, Potential Misuse, Unexpected Data Tracking/Sharing, Trust in Governments, protecting Bystanders, Control, Reliability Concerns

Table 6. Summary of Privacy Factors in IoT context with qualitative methods

Authors	Contexts	Participants	Privacy Factors
Cleveland et al. [12]	Healthcare IoT	Experts, End-Users	User Awareness, Trust in IoT Manufacturers, Unexpected Data Tracking/Sharing, Sensitivity on Data Types
Abbott et al [1]	Smart Home	Owners of IoT Device	Utility, Usage Restricted, Easy Setup, Physical Safety, Data Access, Multi-Users, User Knowledge, Usability, Data Types
Liu et al. [37]	General IoT	Owners of IoT Device	Data Collection, Unreasonable Consent, Sensitive Personal Information, Opaque and Unfair Data Processing, Excessive User profiling, Third-Parties, Anonymization, Privacy/Security Trade-off, Data Security and Integrity, Low Readability
Harkin et al. [23]	General IoT	Expert	Consent, Data Security, Industry Standard, Vulnerable Communities, Surveillance, Privacy of Bystanders, Encryption, Trust
Cheong et al. [11]	General IoT	End-Users	Convenience, Unexpected consequences, benefits, Trust, Protection practices, Data Leaks, Surveillance, Reliability Concerns, Consent, Data Controller
Emami-Naeini et al. [17]	General IoT	Experts	Trust in the Device, Security updates, Sensitivity of Data Types, type of senses on the Device, Encryption of Data, Device Actuations, General Overview, Granular Control in the Data Sharing, Conditional and Contextual Access, Retention Time, Purpose of Data Collection, Data inference, Control, Data Access, Third-Parties
Colnago et al. [14]	General IoT	End-Users	Convenience, Data Security, Physical Safety Potential Misuse, Customer Monitoring, Trust in Governments Trust in Controller Process Recipient, Surveillance, Granular Control in the Configuration, General Overview, Withhold Sharing for a Time period, Utility
Yao et al. [64]	Smart Home	End-Users	Utility, Trust, Transparency and Consent for Bystanders, Withhold Time Sharing for a Time period, Control
Zeng et al. [66]	Smart Home	Owners of IoT Device	Physical Security, Hackers, Trust in IoT Manufacturer, Trust in Governments, Third-Parties, Encryption of Data at rest, Confidentiality, Trust in the Device, Conditional and Contextual Data Access, Surveillance, Potential Misuse, Reliability Concerns, Utility, Control, Privacy/Security Trade-off, Privacy of Bystanders
Padyab et al. [49]	General IoT	End-Users, Experts	Personally Identifiable information, Data Access, Potential Misuse, Sensitivity of Data Types, Third-Parties, Hackers, Trust in Governments location Device, Trust in IoT Manufacturer, Retention Time, Confidentiality, Data Aggregation, Consent, Sensitivity due to unspecified context, Reliability Concerns, Unexpected Data Tracking/Sharing
Kim et al. [29]	Smart Home	End-Users	Convenience, Trustworthy, Data Leaks, Automatic Control
Emami-Naeini et al. [19]	General IoT	Owners of IoT Device	Unexpected Data Tracking/Sharing, Control, Types Data collected, Retention Time, Purpose of Data Collection, Inferred Data, Hackers, Confidentiality, Encryption, Lack of Trust in IoT Manufacturer, Retention Time, Data deletion, Granular Control in the Configuration
Zheng et al. [69]	Smart Home	Owners of IoT Device	Convenience, Control, Hackers, Data Access, Confidentiality, Third-Parties, Transparency, Data selling, Data Collection from ISP, Trust in Governments, Trust in IoT manufacture
Montanari et al. [45]	General IoT	End-Users	Data Ownership, Data inference, Granular Control in Data Sharing, social stigma, Transparency of Data Recipients, Control, Retention Time, Self-Hosting
Luthfi et al. [38]	General IoT	End-Users	Unexpected Data Tracking/Sharing, Data Leaks, Encryption of communication Potential Misuse, Confidentiality, Transparency