

# Increasing Users' Privacy Awareness in the Internet of Things: Design Space and Sample Scenarios



Sarah Prange and Florian Alt

## 1 Introduction

In the era of ubiquitous computing [57], data collection and, as such, potential privacy intrusions are omnipresent. Computing devices do not only inflate users' everyday lives at home, but also in semi-public to public spaces. Examples include, but are not limited to, vacuum cleaning robots collecting floor maps of our homes, smart door locks providing access to our workspaces, digital ordering stations in restaurants, and security cameras in highly frequented places. In addition, the variety of devices and functionality, along with the concrete privacy implications, is huge. For instance, a particular smart TV might only provide access to online streaming services, while other smart TVs might additionally allow for voice interaction using built-in microphones.

As a result, it becomes increasingly challenging for users to stay aware of where their personal data are collected, and with whom it is shared. Moreover, not only device owners are affected, but also incidental users, even without explicit interaction [9].

In this chapter, we shed light on these challenges and illustrate current privacy awareness mechanisms (Sect. 2). However, existing mechanisms, such as, e.g., device indicators, tend to be overlooked [7, 44]. Other mechanisms, such as, e.g., labels on devices' packaging [17, 20, 30], mainly target those who purchase and

---

S. Prange (✉)  
University of the Bundeswehr, Munich, Germany

LMU Munich, Munich, Germany  
e-mail: [sarah.prange@unibw.de](mailto:sarah.prange@unibw.de)

F. Alt  
University of the Bundeswehr, Munich, Germany  
e-mail: [florian.alt@unibw.de](mailto:florian.alt@unibw.de)

set up the devices but are rarely available to other target groups such as visitors of the environment [39] or passers-by. At the same time, privacy awareness is a prerequisite for users to be able and act upon their privacy needs [9, 40, 41]. As such, increasing privacy awareness is a necessary first step.

To address this, we set out with a design space on how and in which contexts privacy-relevant information could be brought to users (Sect. 3). We illustrate three sample scenarios in which privacy-relevant information should be easily accessible for users, along with sample applications from our prior work (Sect. 4): providing privacy-relevant information on computing devices during purchase decisions, providing privacy-relevant information on demand, and providing privacy-relevant information within the environment. Note that the scenarios cover device purchase decisions as well as devices that are already installed and in use. The chapter is complemented with directions for future research (Sect. 5) and a summary (Sect. 6).

## 2 Background and Related Work

An increasing number of everyday objects are equipped with computing power and interconnected, commonly being referred to as the *Internet of Things (IoT)* [2, 4]. Think about, e.g., smart home appliances, but also smart cars, or surveillance systems in public spaces. While providing great benefits and features, these devices pose new threats to users' privacy [62].

In the following, we discuss the privacy challenges that arise from an IoT-infused world (Sect. 2.1) and current mechanisms aiming at increasing users' privacy awareness (Sect. 2.2).

### 2.1 Privacy Challenges

Privacy, which is individual control over when, where, and how personal data are being collected and shared [13], becomes increasingly challenging as sensing and computing technologies are seamlessly integrated into our daily lives [57]. The number of devices capable of collecting personal data is steadily rising, and sensing technology is placed in both private and public places.

The variety of devices is huge. For instance, smart vacuum cleaning robots scan floor maps of our homes to operate;<sup>1</sup> smart fridges reorder groceries; smart electricity meters monitor energy consumption and can thus infer users' activities [48]; smart voice assistants listen to our conversations [35]; cameras record and analyze

---

<sup>1</sup> <https://www.technologyreview.com/2017/07/25/150346/your-roomba-is-also-gathering-data-about-the-layout-of-your-home/>, last accessed August 31, 2022.

semi-public and public spaces for security purposes; smart door locks provide access to homes or offices via biometric features [42].

Also, devices come with various functionality and data collection capabilities, with different impacts on users' privacy. For instance, conversations—as potentially captured by a smart speaker—might be, from a privacy perspective, of different values as compared to grocery orders by a smart fridge. As a consequence, it is hard for users to correctly assess the privacy implications of specific devices, even if they have a general understanding of the technology [39].

Moreover, IoT devices are usually shared among multiple users, and the ecosystem of stakeholders is complex [23, 27, 61]. It not only includes device owners as those who set up and primarily use devices, but also secondary users such as, e.g., co-inhabitants of a smart home [9, 23, 24, 34], guests in a rental apartment [9, 38, 40], or passers-by in semi-public and public spaces [9, 46]. Manufacturers of devices, as well as providers of single services, are also relevant parties. This makes it unclear as to who is responsible for even providing privacy-relevant information and to whom.

Lastly, it is unclear what information is relevant to users in which context, for them to be able to make informed privacy decisions.

## 2.2 *Privacy Awareness Mechanisms*

An increasing number of devices in our environments are capable of collecting personal data about us with built-in sensors. This may happen inconspicuously and without direct interaction [9]. Even worse, users are oftentimes unaware of this, let alone the privacy implications of this data collection [3, 9, 34, 62].

Users, however, want to be informed about data being collected about them and shared with device providers [18, 28, 43, 52]. Moreover, awareness of privacy implications is a prerequisite for users to be able and preserve their privacy, and to decide with whom they are willing to share their personal data [9, 40, 41]. As such, there is a need to design suitable mechanisms that help increase privacy awareness [52, 58] among all affected individuals [9, 60].

Prior work suggested mechanisms that provide *general* privacy information (to, e.g., support purchase decisions) and information on *installed devices* (i.e., that are already in use and collecting data).

### **General Privacy Information**

Prior to data collection, providers of devices and services must provide privacy-relevant information. The default approach to this is privacy notices [11, 21], a textual description of which data are collected and how it is processed. These policies, however, tend to be long, are hard to understand for users, and thus are oftentimes not read thoroughly [56].

Research tried to address this challenge and make privacy-relevant information more accessible to users, to ultimately increase their awareness. Ebert et al. found that more concise and salient privacy notices can successfully increase users' privacy awareness [15]. Others suggested ways to make privacy policies more appealing and understandable. *Polisis* is a framework for automated analysis of privacy policies, to, e.g., assign icons [25]. Building upon this framework, the *PriBot* is a chat agent that provides privacy-relevant information and can answer users' questions [26]. Kitkowska et al. suggested visual and appealing designs for privacy policies and showed that these can successfully spark users' curiosity and ultimately create an understanding of privacy policies [31]. Another opportunity is the use of icons based on a risk assessment [16]. Mozilla's "Privacy not included guide" provides an emoji-based scale, assessing the privacy implications of computing devices ranging from "not creepy" to "super creepy," based on crowd-sourced data.<sup>2</sup>

**Privacy Labels** To particularly target purchase decisions of computing devices, Kelley et al. introduced the "privacy label", which acts similar to nutrition labels for groceries but includes information on data collection and sharing of a device. They found this representation to be easier and more comprehensible than privacy policies based on natural language [30]. Such privacy labels also make privacy information more accessible and can thus inform purchase decisions, avoiding concerns rising later on [20]. Moreover, Emami-Naeini et al. showed that critical information should be included in a primary layer (e.g., directly on a device's packaging), while details can be moved to additional sources (such as, e.g., a website) and linked on the label [17]. These types of labels became obligatory for IoT devices in several countries (e.g., UK,<sup>3</sup> Singapore<sup>4</sup>), and for applications on Apple's iOS.<sup>5</sup>

### Privacy Information on Installed Devices

Many devices that collect data communicate their status through *device indicators* while being in use. For example, webcams indicate via small LEDs whether they are currently on. Amazon's Alexa provides feedback on its recording status via a light ring (e.g., red refers to "muted") [8, 35]. Research also suggested alternatives such as, e.g., physical webcam indicators in the form of a flower [33] or an eye that mimics gaze (i.e., recording) direction [53].

<sup>2</sup> <https://foundation.mozilla.org/en/privacynotincluded/>, last accessed September 1, 2020.

<sup>3</sup> <https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/consultation-on-the-governments-regulatory-proposals-regarding-consumer-internet-of-things-iot-security#designing-a-security-label>, last accessed September 1, 2020.

<sup>4</sup> <https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about-cls>, last accessed June 17, 2022.

<sup>5</sup> <https://mashable.com/article/apple-privacy-nutrition-labels-ios14/?euope=true>, last accessed September 1, 2020.

To help users *detect* devices in their environment, Song et al. suggested attaching visual or auditory cues to devices [51]. *Lumos* is an augmented reality interface that can be employed on users' personal devices and help them detect hidden IoT devices in their environment [50]. Sami et al. used smartphones emitting laser signals to detect hidden cameras via the reflection of the laser [49]. Funk et al. guided users to smart objects using smart glasses [22]. Thakkar et al. suggested four different privacy awareness mechanisms for the smart home context: a physical data dashboard, a mobile application, ambient colored light, and voice messages on privacy via a smart speaker. These mechanisms aim at targeting device owners, but also potential bystanders, with detailed information being preferred by both target groups [54].

### 2.3 Summary and Limitations

In times where data collection is ubiquitously present, it becomes increasingly hard for users to even be aware of potential privacy intrusions and ultimately be able to protect their privacy. Research tried to tackle these challenges by designing mechanisms that target users' *privacy awareness*. However, current privacy awareness mechanisms are only effective to a limited extent. Users might overlook or not realize or understand the meaning of privacy indicators [7, 44]. Moreover, information on devices is oftentimes only available for those who purchase and configure devices, but not for potential *bystanders* (e.g., guests in a smart environment), who might likewise be affected. As a result, especially bystanders are uncertain about device states [1].

In addition, the exact device position and/or area of operation is oftentimes unclear, let alone the concrete privacy implications of certain devices and data being collected. The increasing number of devices being installed further exacerbates this issue. This calls for further research on *privacy awareness mechanisms* that target *device owners* and *bystanders* alike.

## 3 Design Space

Users' privacy perceptions are influenced by many factors, including, e.g., the environment in which data are collected in and type of data that is collected. We argue that this information is privacy-relevant and should be made available to users, to increase privacy awareness. Based on these factors, we derive a design space for privacy awareness mechanisms for the IoT. In the following, we discuss contextual factors that impact users' privacy perceptions, as well as types of information that are ultimately privacy-relevant and how this information could be provided.

### 3.1 Contextual Factors

Individual privacy perceptions and (dis)comfort with personal data being recorded are highly impacted by contextual factors, as highlighted in our previous work [46]:

**Social Aspects and Trust:** Users consider trust and relationships when deciding with whom to share their personal data [19, 36, 59, 60]. For instance, users rely on friends' opinions regarding data sharing [19] and consider *who* is collecting their data [36] as well as who is the owner of a particular device [40].

**Environment:** Also, users' current environment impacts their concerns. As such, data collection in *private* spaces (e.g., the home) is less acceptable as compared to data collection in other spaces, such as restaurants (*semi-public*) or *public* spaces [18, 37]. It is also important to users whether they are familiar with the environment [46]. In unfamiliar settings, users are particularly concerned about (hidden) data collection, especially when they consider the space private at the same time, as is the case for, e.g., rental apartments [38, 46, 51].

### 3.2 Privacy-Relevant Information

Privacy-relevant information can comprise various content and be made available to users in various ways.

#### Content

Depending on users' current context, various information could become relevant for users to decide whether or not they are willing to share their personal data:

**Type of Sensor(s):** The type of sensors—and, respectively, the type of data being collected—impacts users' privacy perceptions. For instance, cameras and microphones (i.e., video and audio recordings) are usually considered particularly sensitive [32].

**Tracking Space:** The area of data collection can further help users assess privacy intrusions, particularly bystanders who are not familiar with the space devices are in [9].

**Device Owner:** The relationship to the device owner crucially impacts users' willingness to be recorded by devices [9, 19, 36, 41, 59, 60]. For instance, users are more comfortable with devices being placed in trusted environments (e.g., in friends' homes) [39, 40, 46] as compared to devices being installed by (unknown) hosts of rental apartments [9, 38].

**Purpose:** Users are more likely to accept data collection if it suits their own needs and purpose. For instance, for health-related purposes, even long-term data tracking is acceptable [5]. This particularly holds true for personal physiological

data [45]. In contrast, video and audio recordings are less acceptable, regardless of the purpose [37].

### Availability and Output

The privacy-relevant information could be made available to users in various ways. For instance, information could be provided in relation to the environment, e.g., on a personal device such as a smartphone or tablet [50], or using contextual images [51]. Another opportunity is to provide information only on specific devices similar to, e.g., the privacy labels [17, 30].

Accordingly, privacy-relevant information is available at different times. For instance, information that is bound to the device's packaging [17, 30] is available to support purchase decisions. Hence, users would need to *actively search* for and inform themselves about devices to receive this information. Information that is provided independently on a personal device, however, would be *always available* to users as they are moving around. Lastly, privacy mechanisms can act in various degrees of proactivity (e.g., low, medium, high in the context of smart homes [29]). Privacy-relevant information could thus be provided *actively*, e.g., through *push notifications* on personal devices, e.g., when entering an unfamiliar area with data collection being in place.

## 4 Sample Scenarios

To further emphasize the relevance of increasing privacy awareness in the IoT, we illustrate three concrete scenarios in the following, along with sample applications. In particular, privacy awareness can and should be increased, in various ways, in the following cases: (1) supporting decisions for purchasing IoT devices with privacy-relevant information (*PriCheck* [55]); (2) allowing users to consult privacy-relevant information on demand (e.g., using their mobile phones, *PriView (mobile)* [46]); (3) providing privacy-relevant information and guidance within the environment (e.g., by means of augmented reality, *PriView (HMD)* [46]). For an overview of relevant design space dimensions per scenario, refer to Table 1.

### 4.1 Privacy-Relevant Information for Purchase Decisions

Prior work already identified device purchases as a relevant starting point and suggested means to support users' decision-making with privacy-relevant information, e.g., by labels on devices' packaging [17, 20, 30]. However, devices are also oftentimes purchased online, where users are not in the hands of the actual device

**Table 1** Scenarios vs. Design Space: We see several scenarios in which privacy-relevant information is needed (left, Sect. 4), and how the design space dimensions would come into play in each scenario (right, Sect. 3)

Scenario	Context	Privacy-Relevant Information	
		Content (Visualization)	Availability and Output
Purchase Decisions	active search for (new) devices	device, sensors, data policies, security standards	on-demand, browser extension
On-Demand Information	active search for installed devices in arbitrary environments	device position (all); sensors, tracking space, recording state, device owner (some)	on-demand or push, mobile application
In Situ Information	information in arbitrary environments	device position (all); sensors, tracking space, recording state, device owner (some); or simple general warning	always-on or push, head-mounted display



**Fig. 1** *PriCheck* is a browser extension supporting purchase decisions with privacy-relevant information on smart devices. Figure from [55]

packaging. Users who *actively* search for devices should have access to privacy-relevant information during purchase decisions. As such, a promising approach is to provide privacy-relevant information in the form of a *browser extension*, to be easily accessible for users when forming a decision. A sample browser extension with privacy-relevant information is the *Privacy Bird* that notifies users if a website’s privacy policy violates their preferences [12]. This could be similarly applied to online purchase decisions as well.

*PriCheck* as suggested by Volk et al. [55] provides privacy-relevant information, comparable to the privacy labels [17, 20, 30], in the form of a browser extension in an online shop (see Fig. 1). In particular, it shows the name of the device along with built-in sensors and functionality visualized as icons (black refers to “included”), data protection quality, security standards, and availability of data protection information. The extension also allows to compare two devices (see Fig. 1, center) and to highlight mismatches with pre-configured privacy preferences (see Fig. 1, right). In an exploratory study ( $N = 11$ ), participants comparing devices in a mock online shop using *PriCheck* appreciated the usability of the extension as



well as the information provided and agreed that it helped them considering privacy-relevant information for their decisions [55].



#### Supporting Purchase Decisions with *PriCheck*

To summarize, *PriCheck* [55] supports users as follows:



**Context**

online purchase of smart devices, *active search*



**Device(s)**

search for *one (new) device* at a time, and *comparison* between two devices



**User(s)**

one user who is about to become the *owner*



**Content**

built-in sensors and functionality, data protection quality and security standards, availability of data protection information



**Availability**

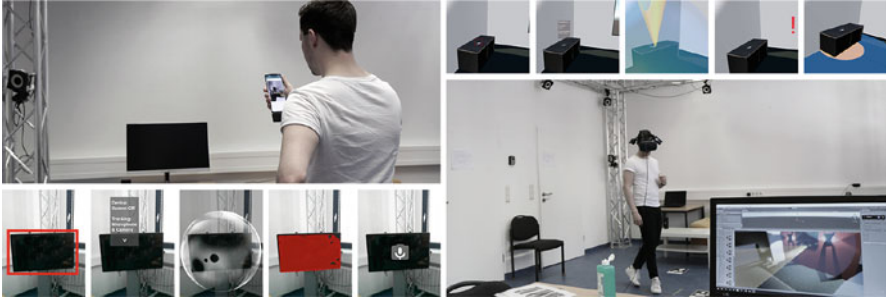
*on-demand*, but within the situation (online shop)

## 4.2 Carrying and Consulting Privacy-Relevant Information on Demand


Users might also want to *actively search* for devices that are already installed and in use. Indicators in the form of, e.g., LEDs or beep sounds [51], can help users discover devices, yet yield little additional information. Other mechanisms, such as the IoT assistant,<sup>6</sup> list devices in users' vicinity and allow to communicate privacy choices but do not cover other information such as the exact device position in users' environment.






*PriView*, employed as a mobile application using a thermal camera dongle [46], allows users to actively scan the environment for devices (see Fig. 2 left, top). In several visualizations, it shows: device position (red frame), textual information, tracking space (bubble), device state (segmentation via the thermal camera), or built-in sensors (Fig. 2 left, bottom). This can particularly help users in unfamiliar environments that are considered private (e.g., a rental apartment), to detect devices they are uncomfortable with. Participants in an exploratory user study ( $N = 21$ ) appreciated the innovative and easy-to-use mobile application. They also liked *PriView* being available on their personal mobile devices, while also having the possibility to put it away anytime [46].

<sup>6</sup> <https://play.google.com/store/apps/details?id=io.iotprivacy.iotassistant&hl=de&gl=US>, last accessed May 26, 2022.



**Fig. 2** *PriView* is a concept for privacy visualizations meant to increase users’ awareness. *PriView* can, e.g., be employed as a mobile application for scanning the environment on demand (left) or in a head-mounted display (HMD), enabling to provide privacy-relevant information in the environment (right). Figure from [46]

 **Privacy-Relevant Information on Demand with *PriView* (mobile)**  
 To summarize, *PriView (mobile)* [46] supports users as follows:

	<b>Context</b>	<i>active</i> device search, scanning the (unfamiliar/untrusted) environment
	<b>Device(s)</b>	potentially multiple devices that are already <i>installed</i> and in use
	<b>User(s)</b>	primary users as well as bystanders, potentially unknown device owners
	<b>Content</b>	device position (all visualizations); built-in sensors, textual information (including device owner), tracking space, recording state
	<b>Availability</b>	on-demand, push notifications possible

### 4.3 Providing Privacy-Relevant Information and Guidance In Situ

To provide users with privacy-relevant information in arbitrary environments, augmented reality (AR) can serve as a means for in situ information and guidance. For instance, *PriView* employed in a head-mounted display (HMD) provides users with visualizations of potential privacy intrusions within the environment [46]. Similar to the mobile application, it shows: device position (red frame), textual information, tracking space in 3D, a general warning icon, and tracking space on the floor (Fig. 2 right). This can particularly help users in arbitrary environments to

increase privacy awareness, particularly when they are new to a place. Participants of our study ( $N = 21$ ) liked the visualizations being available in situ using the HMD. They wished for more details in spaces they considered private (e.g., a rental apartment), while simpler indications were sufficient in places where data collection is obvious (e.g., security cameras at a train station) [46].



#### **In Situ Privacy-Relevant Information with *PriView* (HMD)**

To summarize, *PriView* (HMD) [46] supports users as follows:



**Context**

information within the (unfamiliar/untrusted) environment



**Device(s)**

potentially multiple devices that are already *installed* and in use



**User(s)**

primary users as well as bystanders, potentially unknown device owners



**Content**

device position (all visualizations); built-in sensors, textual information (including device owner), tracking space, recording state



**Availability**

always-on, push notifications possible

## **5 Directions for Future Research**

In the following, we illustrate and discuss interesting directions for future research that arise from privacy awareness challenges and mechanisms within the IoT.

### **5.1 Amount of Information**

An interesting question for future research is *how much information* on IoT devices users will need to make informed privacy decisions. Is a simple device indicator enough to increase awareness, or would users prefer a deeper understanding of data collection and policies?

Moreover, the preferred amount of information varies depending on the environment [46]. For instance, in environments with multiple devices, including such that are firmly installed as well as such carried by passers-by, there is a high potential for an awareness mechanism to cause visual overload. As such, the amount of information should most likely be reduced, with the opportunity to still receive details on demand.

## 5.2 Contextualize and Adapt

As a next step, privacy awareness mechanisms could automatically *adapt* to the context and/or their users. For instance, different scenarios (cf. Sect. 4) might require different support for users' privacy awareness. For purchasing a new device to install it within their own environment, users might need awareness as to how it can be configured in a privacy-preserving way. Being in unfamiliar environments with installed devices, however, rather calls for information on spaces being covered by data collection, for users to be able to avoid these as they wish. Also, for scenarios that users encounter more often (e.g., visiting a certain place), awareness cannot be assumed at first but might increase over time as a mechanism is being used in this scenario. Moreover, an awareness mechanism could also adapt to users' prior knowledge (e.g., reduce information that users already received earlier) or technical expertise (e.g., use simpler versions for lay users, while providing more details for advanced users).

## 5.3 Enabling Control

While awareness is a prerequisite for users to be able to make informed privacy decisions [9, 40, 41], it is only a first step. In particular, users need to be given means to execute (or: enforce) these decisions on nearby devices. For instance, *PARA* is an augmented reality interface that provides privacy controls and allows users to filter data being collected about them [6]. Mobile applications, such as, e.g., the *IoT assistant*,<sup>6</sup> likewise allow users to control nearby devices but require to do so for each and every device or sensor separately, increasing complexity as the number of devices rises. The *PriKey* tries to tackle this challenge by summarizing privacy decisions per sensor in a tangible device [47]. *Personalized privacy assistants* [10, 14] can recommend privacy settings or even act autonomously based on users' privacy preferences or desired standards. This approach, however, needs to find a balance between awareness and control [10]. Future research should further look into how to build upon users' awareness and enable privacy *control*, particularly for those who do not have access to a device's interface.

## 6 Summary and Conclusion

In this chapter, we highlight the need for *increasing users' privacy awareness* within the *Internet of Things (IoT)*. In particular, the increasing number of devices with increasing functionality and sensors makes it challenging for users to stay aware of their personal data being collected. We shed light on design opportunities for bringing privacy-relevant information to users, as well as sample scenarios and applications: supporting purchase decision with *PriCheck* [55], consulting privacy-relevant on demand using *PriView (mobile)* [46], and providing in situ information and guidance using *PriView (HMD)* [46]. Promising directions for future research

include investigating the necessary amount of information, adapting privacy awareness mechanisms to context, and enabling privacy control as a necessary next step.

## References

1. Ahmad, I., Farzan, R., Kapadia, A., & Lee, A. J. (2020). Tangible privacy: Towards user-centric sensor designs for bystander privacy. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW2), 1–28.
2. Alaa, M., Zaidan, A., Zaidan, B., Talal, M., & Kiah, M. (2017). A review of smart home applications based on Internet of Things. *Journal of Network and Computer Applications*, 97, 48–65.
3. Ali, B., & Awad, A. I. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. *Sensors*, 18(3), 817.
4. Atzori, L., Iera, A., & Morabito, G. (2017). Understanding the Internet of Things: Definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Networks*, 56, 122–140.
5. Barua, D., Kay, J., & Paris, C. (2013). Viewing and controlling personal sensor data: What do users want? In S. Berkovsky & J. Freyne (Eds.), *Persuasive technology* (pp. 15–26). Springer.
6. Bermejo Fernandez, C., Lee, L. H., Nurmi, P., & Hui, P. (2021). *PARA: Privacy management and control in emerging IoT ecosystems using augmented reality* (pp. 478–486). Association for Computing Machinery.
7. Chow, R., Egelman, S., Kannavara, R., Lee, H., Misra, S., & Wang, E. (2015). HCI in business: A collaboration with academia in IoT privacy. In F. Fui-Hoon Nah & C.-H. Tan (Eds.), *HCI in business* (pp. 679–687). Springer.
8. Chung, H., Iorga, M., Voas, J., & Lee, S. (2017). Alexa, can I trust you? *Computer*, 50(9), 100–104.
9. Cobb, C., Bhagavatula, S., Garrett, K. A., Hoffman, A., Rao, V., & Bauer, L. (2021). “I would have to evaluate their objections”: Privacy tensions between smart home device owners and incidental users. *Proceedings on Privacy Enhancing Technologies*, 4, 54–75.
10. Colnago, J., Feng, Y., Palanivel, T., Pearman, S., Ung, M., Acquisti, A., Cranor, L. F., & Sadeh, N. (2020). 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 (pp. 1–13). Association for Computing Machinery.
11. Cranor, L. F. (2012). Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *Journal on Telecommunications and High Technology Law*, 10, 273.
12. Cranor, L. F., Guduru, P., & Arjula, M. (2006). User interfaces for privacy agents. *ACM Transactions on Computer-Human Interaction*, 13(2), 135–178.
13. Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, 10(1), 104–115.
14. Das, A., Degeling, M., Smullen, D., & Sadeh, N. (2018). Personalized privacy assistants for the Internet of Things: Providing users with notice and choice. *IEEE Pervasive Computing*, 17(3), 35–46.
15. Ebert, N., Alexander Ackermann, K., & Scheppeler, B. (2021). Bolder is better: Raising user awareness through salient and concise privacy notices. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21. Association for Computing Machinery.
16. Efroni, Z., Metzger, J., Mischau, L., & Schirmbeck, M. (2019). Privacy icons. *European Data Protection Law Review*, 5(3), 352–366.
17. Emami-Naeini, P., Agarwal, Y., Cranor, L. F., & Hibshi, H. (2020). Ask the experts: What should be on an IoT privacy and security label? In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 447–464). IEEE.
18. Emami-Naeini, P., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L., & Sadeh, N. (2017). Privacy expectations and preferences in an IoT world. In *Proceedings of the Symposium on Usable Privacy and Security*, SOUPS '17 (pp. 399–412). USENIX Association.

19. Emami Naeini, P., Degeling, M., Bauer, L., Chow, R., Cranor, L. F., Haghghat, M. R., & Patterson, H. (2018). The influence of friends and experts on privacy decision making in IoT scenarios. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW), 1–26.
20. Emami-Naeini, P., Dixon, H., Agarwal, Y., & Cranor, L. F. (2019). Exploring how privacy and security factor into IoT device purchase behavior. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, CHI '19 (pp. 534:1–534:12). ACM.
21. Feng, Y., Yao, Y., & Sadeh, N. (2021). A design space for privacy choices: Towards meaningful privacy control in the Internet of Things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21. Association for Computing Machinery.
22. Funk, M., Boldt, R., Pfleging, B., Pfeiffer, M., Henze, N., & Schmidt, A. (2014). Representing indoor location of objects on wearable computers with head-mounted displays. In *Proceedings of the 5th Augmented Human International Conference*, AH '14. Association for Computing Machinery.
23. Garg, R., & Moreno, C. (2019). Understanding motivators, constraints, and practices of sharing Internet of Things. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 3(2), 1–21.
24. Geeng, C., & Roesner, F. (2019). Who's in control? Interactions in multi-user smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19 (pp. 1–13). ACM.
25. Harkous, H., Fawaz, K., Leuret, R., Schaub, F., Shin, K. G., & Aberer, K. (2018). Polisix: Automated analysis and presentation of privacy policies using deep learning. In *27th USENIX Security Symposium (USENIX Security 18)* (pp. 531–548). USENIX Association.
26. Harkous, H., Fawaz, K., Shin, K. G., & Aberer, K. (2016). PriBots: Conversational privacy with chatbots. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association.
27. He, W., Golla, M., Padhi, R., Ofek, J., Dürmuth, M., Fernandes, E., & Ur, B. (2018). Rethinking access control and authentication for the home Internet of Things (IoT). In *27th USENIX Security Symposium (USENIX Security 18)* (pp. 255–272). USENIX Association.
28. Jakobi, T., Ogonowski, C., Castelli, N., Stevens, G., & Wulf, V. (2017). The catch(es) with smart home: Experiences of a living lab field study. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, CHI '17 (pp. 1620–1633). ACM.
29. Jin, H., Guo, B., Roychoudhury, R., Yao, Y., Kumar, S., Agarwal, Y., & Hong, J. I. (2022). Exploring the needs of users for supporting privacy-protective behaviors in smart homes. In *CHI Conference on Human Factors in Computing Systems*, CHI '22. Association for Computing Machinery.
30. Kelley, P. G., Bresee, J., Cranor, L. F., & Reeder, R. W. (2009). A “nutrition label” for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, SOUPS '09. Association for Computing Machinery.
31. Kitkowska, A., Warner, M., Shulman, Y., Wästlund, E., & Martucci, L. A. (2020). Enhancing privacy through the visual design of privacy notices: Exploring the interplay of curiosity, control and affect. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)* (pp. 437–456). USENIX Association.
32. Klasnja, P., Consolvo, S., Choudhury, T., Beckwith, R., & Hightower, J. (2009). Exploring privacy concerns about personal sensing. In H. Tokuda, M. Beigl, A. Friday, A. J. B. Brush, & Y. Tobe (Eds.), *Pervasive computing* (pp. 176–183). Springer.
33. Koelle, M., Wolf, K., & Boll, S. (2018). Beyond led status lights—design requirements of privacy notices for body-worn cameras. In *Proceedings of the Twelfth International Conference on Tangible, Embedded, and Embodied Interaction*, TEI '18 (pp. 177–187). Association for Computing Machinery.
34. Koshy, V., Park, J. S. S., Cheng, T.-C., & Karahalios, K. (2021). “We just use what they give us”: Understanding passenger user perspectives in smart homes. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21. Association for Computing Machinery.
35. Lau, J., Zimmerman, B., & Schaub, F. (2018). Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM Conference on Human-Computer Interaction*, 2(CSCW), 102.

36. Lederer, S., Mankoff, J., & Dey, A. K. (2003). Who wants to know what when? Privacy preference determinants in ubiquitous computing. In *CHI '03 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '03 (pp. 724–725). Association for Computing Machinery.
37. Lee, H., & Kobsa, A. (2016). Understanding user privacy in Internet of Things environments. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)* (pp. 407–412). IEEE.
38. Mare, S., Roesner, F., & Kohno, T. (2020). Smart devices in Airbnbs: Considering privacy and security for both guests and hosts. *Proceedings on Privacy Enhancing Technologies*, 2020(2), 436–458.
39. Marky, K., Prange, S., & Alt, F. (2021). Roles matter! understanding differences in the privacy mental models of smart home visitors and inhabitants. In *Proceedings of the 20th International Conference on Mobile and Ubiquitous Multimedia*, MUM'21. ACM.
40. Marky, K., Prange, S., Krell, F., Mühlhäuser, M., & Alt, F. (2020). “You just can't know about everything”: Privacy perceptions of smart home visitors. In *19th International Conference on Mobile and Ubiquitous Multimedia* (pp. 83–95). Association for Computing Machinery.
41. Marky, K., Voit, A., Stöver, A., Kunze, K., Schröder, S., & Mühlhäuser, M. (2020). “I don't know how to protect myself”: Understanding privacy perceptions resulting from the presence of bystanders in smart environments. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*, NordiCHI '20. Association for Computing Machinery.
42. Mecke, L., Pfeuffer, K., Prange, S., & Alt, F. (2018). Open sesame! user perception of physical, biometric, and behavioural authentication concepts to open doors. In *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia*, MUM 2018 (pp. 153–159). Association for Computing Machinery.
43. Mikusz, M., Houben, S., Davies, N., Moessner, K., & Langheinrich, M. (2018). Raising awareness of IoT sensor deployments. In *Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT*. IET.
44. Portnoff, R. S., Lee, L. N., Egelman, S., Mishra, P., Leung, D., & Wagner, D. (2015). Somebody's watching me? Assessing the effectiveness of webcam indicator lights. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15 (pp. 1649–1658). Association for Computing Machinery.
45. Prange, S., Mayer, S., Bittl, M.-L., Hassib, M., & Alt, F. (2021). Investigating user perceptions towards wearable mobile electromyography. In *Proceedings of the 18th IFIP TC 13 International Conference on Human-Computer Interaction*, INTERACT '21. Springer.
46. Prange, S., Shams, A., Piening, R., Abdelrahman, Y., & Alt, F. (2021). PriView—exploring visualisations to support users' privacy awareness. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery.
47. Rodriguez, S. D., Prange, S., Ossenberg, C. V., Henkel, M., Alt, F., & Marky, K. (2022). PriKey—investigating tangible privacy control for smart home inhabitants and visitors. In *Proceedings of the 12th Nordic Conference on Human-Computer Interaction*, NordiCHI '22. Association for Computing Machinery.
48. Saha, M., Thakur, S., Singh, A., & Agarwal, Y. (2014). EnergyLens: Combining smartphones with electricity meter for accurate activity detection and user annotation. In *Proceedings of the 5th International Conference on Future Energy Systems*, e-Energy '14 (pp. 289–300). Association for Computing Machinery.
49. Sami, S., Tan, S. R. X., Sun, B., & Han, J. (2021). LAPD: Hidden spy camera detection using smartphone time-of-flight sensors. In *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems*, SenSys '21 (pp. 288–301). Association for Computing Machinery.
50. Sharma, R. A., Soltanaghaei, E., Rowe, A., & Sekar, V. (2022). Lumos: Identifying and localizing diverse hidden IoT devices in an unfamiliar environment. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association.
51. Song, Y., Huang, Y., Cai, Z., & Hong, J. I. (2020). I'm all eyes and ears: Exploring effective locators for privacy awareness in IoT scenarios. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20 (pp. 1–13). Association for Computing Machinery.

52. Tabassum, M., Kosiński, T., & Lipford, H. R. (2019). “I don’t own the data”: End user perceptions of smart home device data practices and risks. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*, SOUPS’19 (pp. 435–450). USENIX Association.
53. Teyssier, M., Koelle, M., Strohmeier, P., Fruchard, B., & Steimle, J. (2021). Eyecam: Revealing relations between humans and sensing devices through an anthropomorphic webcam. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI ’21. Association for Computing Machinery.
54. Thakkar, P. K., He, S., Xu, S., Huang, D. Y., & Yao, Y. (2022). “It would probably turn into a social faux-pas”: Users’ and bystanders’ preferences of privacy awareness mechanisms in smart homes. In *CHI Conference on Human Factors in Computing Systems*, CHI ’22. Association for Computing Machinery.
55. Volk, V., Prange, S., & Alt, F. (2022). PriCheck—an online privacy assistant for smart device purchases. In *Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI EA ’22. Association for Computing Machinery.
56. Waddell, T. F., Auriemma, J. R., & Sundar, S. S. (2016). Make it simple, or force users to read? Paraphrased design improves comprehension of end user license agreements. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI ’16 (pp. 5252–5256). Association for Computing Machinery.
57. Weiser, M., Gold, R., & Brown, J. S. (1999). The origins of ubiquitous computing research at PARC in the late 1980s. *IBM Systems Journal*, 38(4), 693–696.
58. Yao, Y. (2019). Designing for better privacy awareness in smart homes. In *Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing*, CSCW ’19 (pp. 98–101). Association for Computing Machinery.
59. Yao, Y., Basdeo, J. R., Kaushik, S., & Wang, Y. (2019). Defending my castle: A co-design study of privacy mechanisms for smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI ’19 (pp. 1–12). ACM.
60. Yao, Y., Basdeo, J. R., Mcdonough, O. R., & Wang, Y. (2019). Privacy perceptions and designs of bystanders in smart homes. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), 1–24.
61. Zeng, E., & Roesner, F. (2019). Understanding and improving security and privacy in multi-user smart homes: A design exploration and in-home user study. In *28th USENIX Security Symposium (USENIX Security 19)* (pp. 159–176). USENIX Association.
62. Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2019). The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal*, 6(2), 1606–1616.

**Open Access** This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter’s Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter’s Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

