PriView– Exploring Visualisations to Support Users' Privacy Awareness

Sarah Prange
sarah.prange@unibw.de
Bundeswehr University Munich
LMU Munich
Germany, Munich

Ahmed Shams
ahmed.s001999@gmail.com
German University in Cairo
Egypt, Cairo

Robin Piening
robin.j.piening@gmail.com
LMU Munich
Germany, Munich

Yomna Abdelrahman
yomna.abdelrahman@unibw.de
Bundeswehr University Munich
Germany, Munich

Florian Alt
florian.alt@unibw.de
Bundeswehr University Munich
Germany, Munich

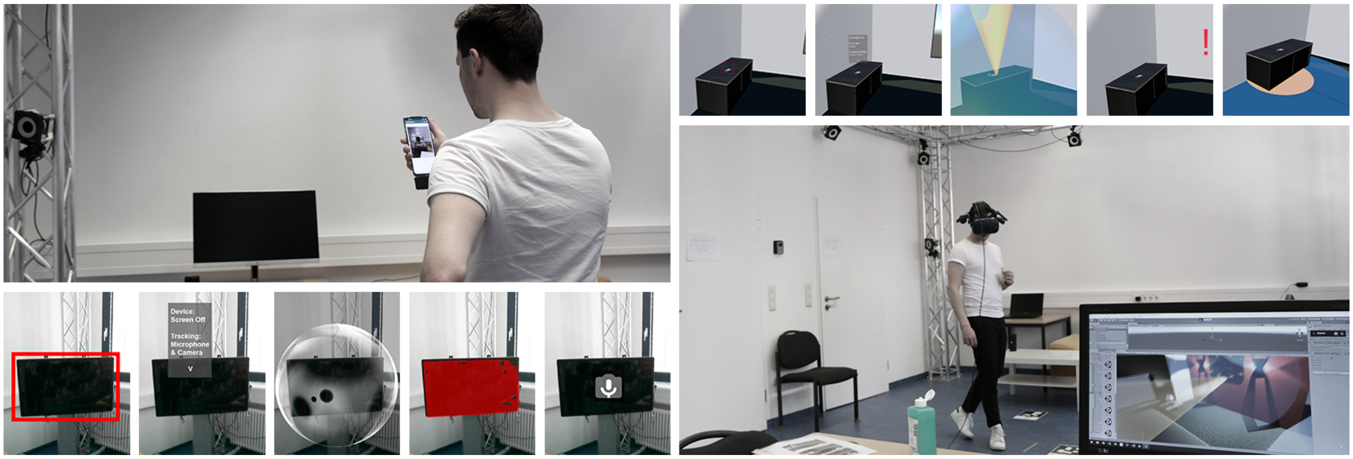


Figure 1: We present *PriView*, a concept to visualise potential privacy intrusion (i.e., video or audio recordings) in the users' vicinity. We compared two output devices, namely a mobile application (left) and a head-mounted display (right). We implemented five visualisations for each. We found that details in the form of text labels were preferred in both versions. However, more subtle indications were considered adequate in some scenarios.

ABSTRACT

We present *PriView*, a concept that allows privacy-invasive devices in the users' vicinity to be visualised. *PriView* is motivated by an ever-increasing number of sensors in our environments tracking potentially sensitive data (e.g., audio and video). At the same time, users are oftentimes unaware of this, which violates their privacy. Knowledge about potential recording would enable users to avoid accessing such areas or not to disclose certain information. We built two prototypes: a) a mobile application capable of detecting smart devices in the environment using a thermal camera, and b) VR mockups of six scenarios where *PriView* might be useful (e.g., a rental apartment). In both, we included several types of visualisation. Results of our lab study (N=24) indicate that users prefer simple, permanent indicators while wishing for detailed visualisations on demand. Our exploration is meant to support future designs of privacy visualisations for varying smart environments.

CCS CONCEPTS

• **Security and privacy** → **Usability in security and privacy**; • **Human-centered computing** → *Ubiquitous and mobile devices.*

KEYWORDS

Smart Home, Smart Environments, Smart Devices, IoT, Privacy, Thermal Camera, Mobile Application, AR, VR, Visualisation

ACM Reference Format:
Sarah Prange, Ahmed Shams, Robin Piening, Yomna Abdelrahman, and Florian Alt. 2021. *PriView*– Exploring Visualisations to Support Users' Privacy Awareness. In *CHI Conference on Human Factors in Computing Systems (CHI'21), May 8–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 18 pages. https://doi.org/10.1145/3411764.3445067

1 INTRODUCTION

Mark Weiser's vision of computers that "weave themselves into the fabric of everyday life" has become true [49], leading to increasing saturation of our environment with sensors. Such sensors can be found in both, personal devices as well as in our environment. For example, smart speakers can eavesdrop our conversations, smart TVs and smart vacuum cleaners can observe our homes using their built-in camera, surveillance cameras monitor public spaces, and cameras and microphones in smartphones and laptops can be accessed by many applications running on those devices.

While in many cases the data collected by those sensors serve a meaningful purpose, such as assisting users or ensuring public safety, their presence might be problematic from a privacy point of view. Users are often unaware of sensors in the first place and, hence, cannot avoid being exposed to them. Think about a public transport station where users generally do not know where surveillance cameras are placed and whether additional measures, such as face recognition, are employed[1]; similarly, guests in smart homes might be unaware of the loudspeakers serving as voice assistants or hidden cameras might be placed in rental apartments[2,3]; or smartphones carried by employees might observe their work environment or record conversations. In all these cases, people might want to know about such devices to deliberately decide to avoid a particular area or not to disclose certain information.

In this paper, we present *PriView* as a concept to support users in such situations. The idea is to visualise the position of sensors in the environment; provide users information about the sensor (e.g., which data is collected and with whom it is shared); and in particular, highlight areas of potential privacy intrusion (such as video or audio recording). An example output device for such visualisations is Augmented Reality (AR) glasses. AR is likely to find its way into users' everyday life in the near future (cf. Apple's new generation of AR glasses[4]).

In this paper, we first explore the design space and possible application scenarios of *PriView*. Secondly, we built two prototypes, namely a) a mobile application capable of detecting smart devices in the environment using a thermal camera; and b) VR mockups of possible application scenarios, private as well as public, where *PriView* might be useful (e.g., a public train station or a rental apartment). For both applications, we implemented various ways of visualising the privacy relevant information (e.g., text labels or frames around the device). Thirdly, we report on a user study (N=24) in which we investigated both versions of *PriView*. In particular, we let users try out our prototypes using the think aloud method and conducted semi-structured interviews.

Our results show that participants appreciated the ease of using a headset to explore their environments, but could also imagine using *PriView* in a mobile application on-demand. For unfamiliar private places in which device owners and the purpose of data collection might be unclear, participants generally wished for more detailed visualisations, while appreciating simple warning indications to get a first overview in a new scene.

Contribution Statement. With *PriView*, we contribute 1) potential application scenarios and design opportunities for privacy visualisations in both, private and public spaces; 2) we built two prototypes (a mobile and a VR application), exploring both, detection and visualisation of smart devices in the user's vicinity and various sample use cases (VR only); 3) we discuss our results, formulate design challenges, and suggest directions for future research.

2 BACKGROUND & RELATED WORK

With *privacy*, we refer to users' ability to decide about and control their personal data being captured [12]. However, staying in control becomes challenging as computational systems tend to be invisible and it is hard for users to know where their data is flowing [50]. Hence, users need to be *aware* of data being tracked in the first place. To enable users to be *aware* of potentially privacy relevant devices (i.e., recordings of their personal data), several *measures* have been suggested in related work. We present further measures closely related to our concept below.

2.1 Privacy Notices & Visualisations

Privacy policies are currently providers' main means to communicate their data collection and processing practices to consumers. Approaches to design such notices have been suggested [44]. However, such text-based policies are rarely read thoroughly by users [48]. To address this, several solutions have been suggested. For instance, *PriBot* is a conversational agent that can answer questions on privacy policies [20]. Kitkowska et al. stated that privacy UIs should enhance curiosity to foster the comprehension of privacy policies and suggested respective designs [23]. Mozilla provides an emoji-based crowd-sourced assessment of the "creepiness" of a number of smart devices[5]. Personalised privacy assistants support users to make and communicate their decision on privacy settings [11]. Furthermore, attempts to visualise information on devices [36] and data flows [5] within smart environments have been done.

2.2 Privacy Labelling

Privacy labels on IoT device's packaging have been subject to prior research [13, 16, 22] and recently became mandatory in several countries (e.g., UK[6], Singapoore[7]). Moreover, new data protection regulations make it mandatory in many countries to indicate by physical signs that CCTV is active in public spaces.

Kelley et al.'s privacy labels allow users to grasp information more quickly as compared to natural language privacy policies [22]. Following this approach, Naeini et al. found privacy and security as especially influencing users' purchase decisions if devices are capable of collecting sensitive data [16]. Thus, such information

[1] https://www.theguardian.com/technology/2020/jan/24/met-police-begin-using-live-facial-recognition-cameras, last accessed August 9, 2020

[2] https://www.theatlantic.com/technology/archive/2019/03/what-happens-when-you-find-cameras-your-airbnb/585007/, last accessed August 9, 2020

[3] https://www.forbes.com/sites/suzannerowankelleher/2020/01/27/why-you-should-start-screening-for-hidden-spy-cameras-when-you-travel/#ffe069b5afd8, last accessed September 1, 2020

[4] refer to, e.g. https://www.techradar.com/news/apple-glasses, last accessed June 26, 2020

[5] https://foundation.mozilla.org/en/privacynotincluded/, last accessed September 1, 2020

[6] 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

[7] https://www.csa.gov.sg/programmes/cybersecurity-labelling, last accessed September 1, 2020

should be included in privacy labels. The design of such labels was further evaluated with experts and consumers, suggesting that a secondary information layer beyond the packaging itself could carry more details [13]. Also, Apple recently introduced "nutrition labels" for apps[8]. However, users affected by the data collection are oftentimes not in hand of the device's packaging, e.g. for devices that have been installed in hotel rooms or public spaces. In addition, such labels do usually not cover the current *state* of the device (i.e., if it is currently recording data). Furthermore, for, e.g. CCTV signs, it remains unclear to users as to where exactly the tracking happens and if additional measures (e.g., face recognition) are being applied.

2.3 Device Indicators

Many IoT devices indicate their current *state* (i.e., currently active and/or recording data) by various indicators, e.g., small LEDs indicate that a webcam is on. As another example, Amazon's Alexa indicates by a light ring that it is currently recording [10, 26]. At the same time, this indication might be unclear to novice users and additional means to support users' privacy have been suggested, including wearables jamming the signal [6] and tangibles fostering the use of the device's muting functionality [47]. Furthermore, users tend to overlook such *device-centric* indicators [9, 41] and/or have only limited means to take consequences.

2.4 Device Locators

Related work has also looked into a) how to *detect* sensors and their state in the environment and b) how to *communicate* this information to users in the form of *device locators*.

2.4.1 Detecting Sensors in the Environment. Various approaches to detect sensors and/or smart devices in the environment exist. For instance, the presence of smartphones can be determined by scanning for Bluetooth MAC addresses. Furthermore, the signal-to-noise ratio can reveal the distance of a device. Means to find hidden cameras in rental apartments were suggested[9], including network scans (e.g., Fing[10]), scanning rooms manually for plugged in items, or radio frequency detectors[11]. Finally, Youngjun et al. showed that thermal cameras can be used to detect surfaces [7]. Abdelrahman et al. highlighted the potential of using thermal imaging to determine whether devices are recording or not [1]. This motivated us to detect devices for *PriView* using a thermal camera.

2.4.2 Device Locators. To support users finding IoT devices in their environment, several means have been suggested in related work. Song et al. suggested visual and auditory cues attached to the devices, increasing their participants' search efficiency as compared to no locators [45]. Related mechanisms have been suggested to support users in finding objects using visualisations in smart glasses [17]. While such mechanisms can increase users' awareness about devices' position, they can also serve other purposes such as learning about IoT devices [45].

2.5 Summary

Users are oftentimes unaware of IoT devices collecting their personal data [8], which makes it impossible for users to exert control over the data collection, i.e. to protect their privacy [12, 50]. With *PriView*, our goal is to help users to not only *physically locate* IoT devices being *static* in arbitrary environments but to also identify *dynamic* devices (e.g., smartphones in bystanders' pockets) as well as *areas being covered* by potential recording (i.e., potential privacy intrusion) and to provide *additional information* (e.g., data practices). This will help users to take action, if necessary. Additionally, as opposed to existing measures, *PriView* is independent from device providers in the first place as we suggest to detect devices in users' vicinity using sensing technology such as a thermal camera.

3 RESEARCH APPROACH

Users might be unaware of (hidden) IoT devices and generally wish for information in that regard, in particular in spaces they perceive as private [45]. We implemented *PriView* to help users in not only *locating* but also *understanding* sources of potential tracking by providing them with AR visualisations in a mobile application or a head-mounted display (HMD). With our work, we contribute to answering the following research questions:

RQ1 Privacy Awareness: Can *PriView* support users in protecting their privacy?
RQ2 Information: Which amount of information do users prefer (in which context) and why?
RQ3 Visualisation: Which *type of visualisation* is most preferred by users for which setting?
RQ4 Interaction: How would users like to *interact* with such visualisations?

In the following, we describe potential application scenarios for our concept, based on factors that impact users' privacy concerns. Next, we describe our concrete implementations for *PriView*. We then report on our user study with two prototypes using two output devices, namely a mobile application and an HMD. We conclude with discussing opportunities and challenges of privacy visualisations for varying smart environments.

4 APPLICATION SCENARIOS FOR *PRIVIEW*

To choose a sample of application scenarios for *PriView*, we built upon factors impacting users' privacy concerns.

4.1 Factors Impacting Privacy Concerns

IoT devices are increasingly present in users' daily surroundings, including their own home, but also other places such as unfamiliar private households, hotel rooms or public spaces. While such devices provide a rich variety of features (cf. [33] for an overview), they have the potential to invade users' privacy by collecting and processing their data. Users' acceptance of IoT devices is influenced by a myriad of factors, including perceived privacy risks [25] and perceived benefits [42]. Tabassum et al. investigated user perceptions and concerns towards smart homes and respective data policies and highlighted the need for increased awareness [46].

[8] https://mashable.com/article/apple-privacy-nutrition-labels-ios14/?europe=true, last accessed September 1, 2020

[9] https://www.abc15.com/decodedc/technology/apps-help-track-hidden-cameras-in-airbnb-and-hotel-rentals, last accessed August 23, 2020

[10] https://play.google.com/store/apps/details?id=com.overlook.android.fing&hl=de, last accessed July 03, 2020

[11] https://www.cnbc.com/2019/06/28/how-to-find-cameras-in-your-airbnb-or-hotel-room.html, last accessed August 23, 2020

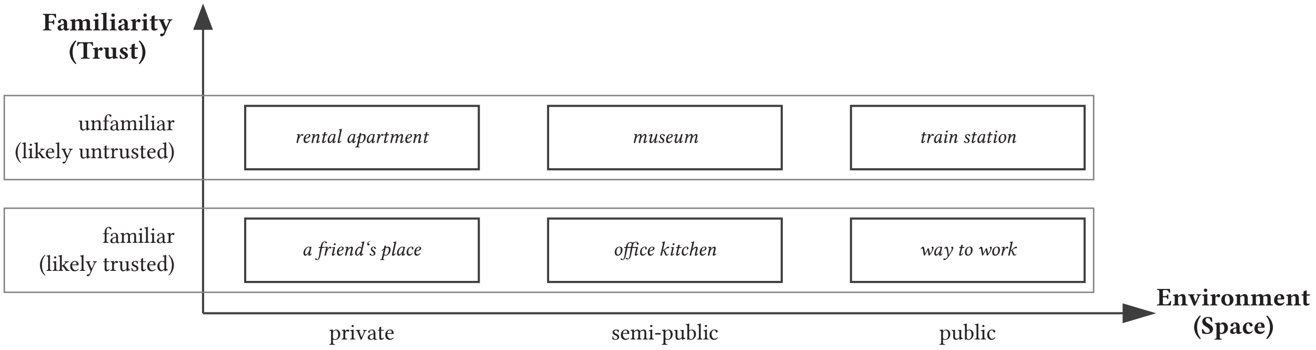


Figure 2: We created 6 scenarios for the evaluation of *PriView*, differing in the space (cf. "Environment", namely private, semi-public and public) and the users' familiarity with it (cf. "Familiarity"). Note that we consider familiar places to be likely trusted by users, while unfamiliar places are likely to be untrusted.

Moreover, concerns are no longer bound to a device, but rather to the whole scenario. In particular, related work identified a myriad of factors that influence users' privacy perception as well as ultimately their concerns [9, 15, 27–30, 53, 54] and decisions as to when and where data collection is acceptable. Among these are the (perceived) information sensitivity, receiver, and usage [2] as well as who is collecting what data, where, for which reason, and at which frequency (i.e., once vs continuously) [29]. We discuss a number of these factors in detail below.

4.1.1 Social Aspects & Trust. Social aspects and relationships have been identified as a crucial factor for users when it comes to making their own decisions on their opinion of data collection [15, 28, 53, 54]. For example, users are more willing to accept data collection if friends do so as well [15]. Furthermore, it is very important to users who is collecting their data (i.e., the identity of the "information inquirer") [28]. In particular, users are more willing to share their data if they know and/or trust the owner of a device [34]. Finally, users also tend to make a difference as to whether or not they trust the environment. For instance, in unfamiliar smart home settings, such as rental apartments, users are concerned about hidden IoT devices and even tend to search for them manually [45].

4.1.2 Environment. Also, users' relation to the environment plays an important role when assessing potential privacy concerns. For instance, data monitoring in private spaces such as users' own or others' homes is completely unacceptable, while they are more comfortable with data collection in semi-public (e.g., restaurants) or public spaces [14, 29]. Furthermore, users' privacy concerns are influenced by how often and for how long data is monitored [29]. This is often coupled to the frequency at which they visit a certain place. Note that while an environment is unfamiliar – hence likely untrusted – upon users' first visit, this fact is likely to change over time as users visit a place more often. Finally, in semi-public and public places, data collection might be dynamic as passers-by might carry further tracking technologies.

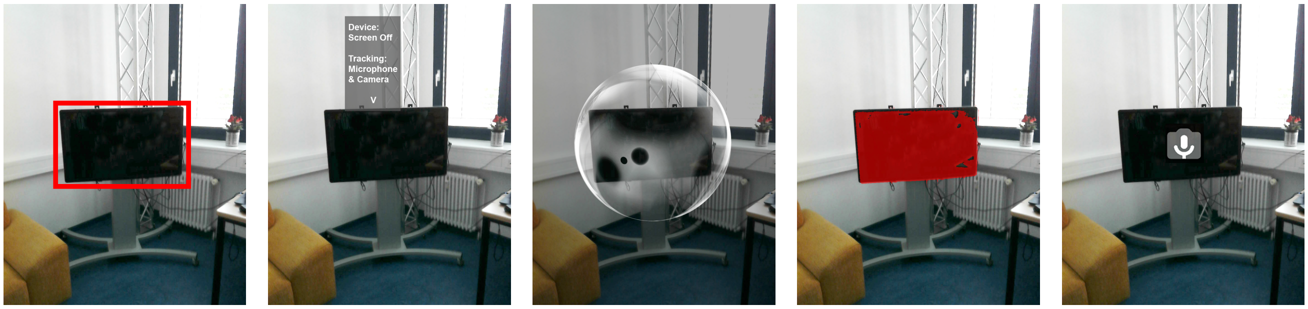
4.1.3 Context, Devices & Purpose. Furthermore, the context – including the purpose, type and frequency of data collection [9, 29, 30], data processing policies and storage – as well as the concrete devices and their capabilities are important factors. For example, cameras and microphones have been shown to be particularly privacy invasive sensors to users as they are capturing sensitive data [24]. Photo and video-based monitoring is generally considered unacceptable, regardless of the purpose [29]. Users are also uncomfortable with continuously recording audio and are – while still feeling uncomfortable – more willing to accept occasional recordings, especially for work environments requiring confidentiality [24].

Many sample devices exist that include these sensors. Examples are personal devices (such as smartphones) as well as ubiquitous devices in public spaces (such as CCTV cameras). While personal sensing is gaining popularity and acceptance (for example, monitoring personal data for long term goals, such as losing weight [3]), ubiquitous sensing in varying environments is less personal, but at the same time less controllable for users, which makes informed privacy decision challenging.

4.1.4 Summary. Users' perception of privacy and concerns are highly dependent on context [14, 39], what is being recorded in a particular context, and the perceived value of the recordings [24]. Furthermore, users are concerned about their privacy and wish to be *aware* of IoT devices capable of recording their data and the affected space [35, 45, 54], as well as respective data processing [46]. This motivated us to build *PriView* for various scenarios.

4.2 Sample Scenarios

As privacy highly depends on context [39, 40, 53], related work has used various scenarios when it comes to privacy in the IoT (cf., e.g. [15, 53, 54]). However, using fictional IoT scenarios for research purpose comes with several limitations. In case participants are not familiar with the factors that build the scenario (such as, e.g., devices, place), results might be limited. IoT scenarios being used in online surveys suffer from the fact that participants conduct the survey in a decoupled place that may not at all be related to the scenario [29]. In our lab study, we used VR as a means to overcome this limitation and immerse participants in the scenario as best as possible. Based on the factors discussed in Section 4.1, we chose the following six sample scenarios (cf. Figure 2 for an overview).



(a) Bounding Boxes **(b) Text Labels** **(c) 3D Shapes** **(d) Segmentation** **(e) Sensor Icons**

Figure 3: *PriView* in a mobile application: We implemented five types of visualisation, namely a) Bounding Boxes (framing the device), b) Text Labels (indicating the device's state), c) 3D Shapes (around the device), d) Segmentation (thermal highlighting), and e) Sensor Icons (camera or microphone).

4.2.1 Public Environment. In public environments, users might be more hesitant to share their personal data, especially if they are unaware of data collection and policies. At the same time, if benefits are clear, users are more willing to accept their data being tracked [38, 42] (e.g., CCTV in a train station for safety reasons).

unfamiliar. Users who are travelling in a foreign country might be interested in knowing which data is being collected, e.g. in a *train station*. While their main goal is finding their way, they might also want to avoid their personal data being collected in this public space (e.g. avoid being on CCTV). Such places tend to be crowded, opening the opportunity for further data collection sources being carried by other people, but also for hiding in the crowd.

familiar. Users on their daily *way to work* are highly familiar with the place. However, it is still public and they might be unaware of potential data collection. Especially in this scenario, data collection might be inconspicuous, such as through personal devices carried by passers-by or through sensors in smart cars.

4.2.2 Semi-Public Environment. In semi-public environments, the number of ubiquitous sensors might be more limited as compared to public spaces, as the fluctuation of personal devices is less high and/or owners of personal devices are known to the user.

unfamiliar. In a *museum*, users' primary intention is usually visiting the exhibition. At the same time, data recording in the form of surveillance cameras, interactive exhibits or other visitors' personal devices might be present.

familiar. In a shared *office kitchen*, users usually enjoy coffee/tea or lunch breaks during long workdays. However, smart kitchen appliances including audio recording capabilities might be present. While users are familiar with all people who can access this space, they might want to avoid, e.g., being eavesdropped by the device owner (i.e., their boss).

4.2.3 Private Environment. In private environments, users expect their privacy to be protected by default. However, in times of smart home devices being on the rise, data recording might not stop at private places' doors.

unfamiliar. In a *rental apartment*, users might appreciate the convenience of smart devices, but on the other hand be concerned about their privacy, hence, be reluctant to share personal information (e.g., browsing history) with their (unknown) host [32]. Such scenarios have been applied in prior investigations [53, 54].

familiar. In contrast, at *a friend's place*, the device owner as well as the environment are well known to users. However, users still might not want to share, for example, their private conversations, with device providers.

5 DESIGN & IMPLEMENTATION SAMPLES OF *PRIVIEW*

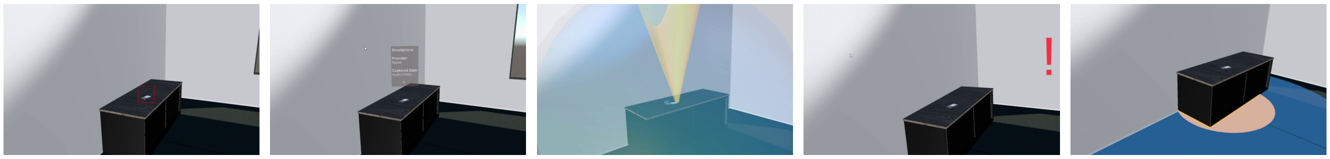
To explore the rich opportunities of *PriView*, we implemented a set of *visualisations* on two different *output devices* (i.e., a smartphone (mobile) and a head-mounted display (HMD)). Table 1 provides an overview on which visualisation was shown on which device.

5.1 Visualisations

With many sensors being present in personal devices and our environment(s), it becomes increasingly harder for users to keep track of what information is collected about them when and where. At the same time, there are several factors influencing users' privacy concerns (cf. Section 4.1) that can be addressed by communicating respective information to users. *PriView* could provide, e.g., information on device position, type of sensor, type of data being collected, tracking space, and device status. We implemented the following sample visualisations, differing in the provided information:

Bounding Boxes To highlight devices in the users' vicinity, red frames are displayed around them (mobile cf. Fig. 3a, HMD cf. Fig. 4a). *Bounding Boxes* are mainly creating awareness of specific devices and their location.

Text Labels To hint at devices while at the same time providing additional information, we implemented *Text Labels* (mobile cf. Fig. 3b, HMD cf. Fig. 4b). Similar to the Bounding Boxes, labels show the devices' position, but also information such as the device name, provider, and data being collected. This information was selected as prior work shows that this particularly matter to users [9, 24, 29, 30].



(a) Bounding Boxes (b) Text Labels (c) 3D Shapes (d) Warning Icon (e) Floor Markers

Figure 4: *PriView* in VR: We implemented five types of visualisation, namely a) Bounding Boxes (framing the device), b) Text Labels (indicating manufacturer, sensor and data being collected), c) 3D Shapes (highlighting the tracking space for audio: blue bubble, and video: yellow cone), d) a Warning Icon (warning), and d) Floor Markers (highlighting the tracking space for audio: blue circle, and video: yellow circle).

3D Shapes To visualise devices' potential tracking space, this visualization shows *3D Shapes* emerging from the devices' sensors (mobile cf. Fig. 3c, HMD cf. Fig. 4c). As users generally wish for information about the physical space being affected [35, 54], this visualisation informs users about and enables them to avoid such spaces.

Segmentation To not only highlight a device but also indicate their (thermal) state, we use *Segmentation.* This visualisation is strongly coupled to our detection modality, i.e. the thermal camera (mobile application only, cf. Fig. 3d).

Sensor Icons As an unobtrusive indicator per device, we implemented camera and microphone icons as these data types are especially relevant to users [24] (mobile application only, cf. Fig. 3e).

Warning Icon As an additional visual indicator, we added an exclamation mark in a general, static position (bound to the users' view, HMD only, cf. Fig. 4d). This supports users' wish to be generally aware of data being recorded [45].

Floor Markers As a more decent variant of showing devices' tracking spaces, we implemented 2D *Floor Markers* (HMD only, cf. Fig. 4e).

We argue that there is no "one-fits-all" solution of *PriView*. Rather the specific visualisations are intended to support particular scenarios. For instance, in some cases it might be sufficient for users to have the *Warning Icon* as a general indicator, while in other cases the visualisation should be as detailed as the *Text Labels* or an indication of the specific tracking space is desired.

5.2 Output Devices: Handheld vs. Handsfree

While *PriView*'s visualisations could be shown on any handheld output device such as a smartphone screen or as a physical image of the environment (cf. [45] for an example of IoT device locators on contextual images), it could be used more immersively by means of, e.g., augmented reality as it provides an "ideal interface to IoT applications" [51]. We particularly investigated a handheld device (smartphone) and a handsfree device (head-mounted display).

Furthermore, while most visualisations are *device-centric* and thus should be shown within the environment, a *general* indicator such as our warning icon could be shown on any personal device.

While IoT locators, as suggested by Song et al. [45], locate devices that are static in the environment, using *PriView* in a mobile application or an HMD allows new and/or moving devices in the users' environment to be *dynamically* highlighted. Regardless of the output modality, *PriView* can be activated and interacted with in various ways. For instance, scanning the environment with the smartphone is equivalent to an "on demand" concept, while mockups in the HMD can be "always on". Alternatives could show visualisations implicitly on change or on proximity.

6 STUDY: EXPLORING THE OPPORTUNITIES OF *PRIVIEW*

To explore the rich opportunities of *PriView*, and to answer our *RQs*, we implemented two prototypes, namely device detection and visualisation in a mobile application (Part I, Section 6.1) and visualisations in an HMD in various scenarios using virtual reality (VR) scenes (Part II, Section 6.2). We implemented a total of seven possible visualisations, three of which are similar in both systems and two that are unique for the respective output device (cf. Table 1 for an overview). We evaluated both prototypes in an exploratory lab study in combined study sessions (i.e., participants experienced both prototypes subsequently).

6.1 Part I: Smart Device State Detection using *PriView*

6.1.1 Implementation. We built an Android application capable of detecting a) locations of smart devices and b) their state (on/off) by means of a FLIR One[12] thermal camera attached to the smartphone. Our implementation utilises the fact that different devices have different temperature profiles captured by thermal cameras. Additionally, this temperature profile changes based on the operation state of the device. Our application analyses the FLIR One's camera stream. We trained the real-time object detection framework Yolo [43] to detect the position of a subset of smart devices, namely an Amazon Echo Dot, a speaker, a laptop, a screen, and a mobile phone, with an average loss of 0.4143[13]. Furthermore, we created another model that can detect the devices' state (i.e., on vs off) with an accuracy of over 90%.

6.1.2 Visualisations. The mobile application can represent the respective information (i.e., device position and state) in five different visualisations (cf. Figure 3). Note that combinations of these might be suitable. However, we showed them separately to participants.

[12] https://developer.flir.com/flir-one-software-development-kit/, last accessed July 28, 2020

[13] Note that loss is a way of evaluating models by giving them a larger penalty for each mistake, i.e. the lower the loss, the better.

Table 1: Visualisation samples we implemented for *PriView*, in the mobile application and VR prototype, respectively.

Bounding Boxes	Text Labels	3D Shapes	Segmentation	Sensor Icons	Warning Icon	Floor Markers
frames around devices	textual descriptions	3D tracking space	thermal highlighting	camera, microphone icons	static exclamation mark	2D tracking space
Mobile HMD	Mobile HMD	Mobile HMD	Mobile –	Mobile –	– HMD	– HMD

6.1.3 Apparatus. For the study, we designed a setting in our lab including the aforementioned sample of devices that our mobile application is able to detect. In particular, we placed an Amazon Echo Dot, a speaker, a laptop, a screen and a mobile phone in varying positions in our lab. Note that we also used varying specific devices (e.g., we used multiple smartphones) to reduce learning effects. We provided participants with the application running on a OnePlus 8 smartphone complemented with the FLIR One thermal camera dongle. Participants were to search for the devices without (i.e., baseline) and using all visualisations in the mobile application (i.e., five search tasks in counterbalanced order). We created a device layout for every visualisation, consisting of five devices each. We made sure to have a consistently low search difficulty (i.e., all devices were visible rather than hidden) as we wanted participants to focus on the visualisations. We ensured consistent environmental conditions (e.g., lightning). After every search tasks, participants answered 5-point Likert items on comfort, learnability, understandability, and frequency of use (cf. Appendix A.1). In a final questionnaire, we acquired usability using the system usability scale (SUS) [4] and cognitive workload using the NASA-TLX (Raw TLX [21]). We additionally conducted semi-structured interviews particularly covering participants' experience with the application and potential use cases (cf. Appendix A.2 for full interview guide).

6.1.4 Study Design. We conducted a within subjects study with Visualisation Type and Device Position as independent variables. We counterbalanced the order of Visualisation Type according to a Latin Square [52]. For each representation, participants' conducted a search task using our mobile application, i.e. name all devices they could find in our lab. We deliberately did not reveal the total number of devices present per condition (five devices per condition). Note that in this part of the study, using *PriView* was participants' *primary task*. We varied Device Position in our lab setting to avoid learning effects. However, we coupled Device Position to Visualisation Type, i.e. device position per visualisation was consistent for each participant to ensure comparability.

We asked participants to think aloud while searching and particularly include the devices they found as well as the information they got from the application. In addition, participants rated use and feel per visualisation on 5-point Likert scales (cf. Appendix A.1). We complemented this part of the session with a questionnaire (SUS and Raw TLX) and semi-structured interview (cf. Appendix A.2).

6.2 Part II: *PriView* in Various VR Scenarios

6.2.1 Visualisations. We implemented five samples of visualisations (refer to Figure 4) in the HMD. We did not investigate possible combinations of these but showed them separately to participants.

6.2.2 Scenes. We implemented 6 sample scenes (cf. Figure 2 for an overview and Appendix B.1 for detailed descriptions):

Rental apartment (bedroom): an unfamiliar private place
A friend's place (living room): a familiar private place
Museum: an unfamiliar semi-public space
Office kitchen: a familiar semi-public space
Train station: an unfamiliar public space
Way to work (street): a familiar public space

In every scene, we placed various tracking sources (i.e., devices with cameras and microphones) for which we employed the visualisations (cf. Section 6.2.1). However, not all of them might have been able to actually track the user (e.g., in the train station scene, passengers on the train were recording audio using their smartphone while the user was on the track outside the train).

6.2.3 Implementation. We built the scenes using the Unity game engine and made it accessible to participants via an HTC VIVE Pro headset (2880 × 1600 pixels combined, 90 Hz, 110° fov), using the SteamVR plugin. The application was running on a stationary HP VR backpack computer with Windows 10. Participants were free to move within a 4 m × 4 m tracking space, covered by 2 VIVE base stations (Gen 2.0). Participants' view and actions could be monitored from the Unity "ingame" view. In every scene, every visualisation could be activated and deactivated during run time by the experimenter. Some visualisations were rendered to be always on top (*Bounding Boxes*, *Text Labels* and the *Warning Icon*), others blended with the environment (*3D Shapes* and *Floor Markers*).

6.2.4 Apparatus. We implemented five samples of visualisations (cf. Figure 4) in six sample environments (cf. Figure 2) in VR. In every scene, we gave participants a number of details such as their relation to the environment (cf. Appendix B.1 for detailed scenario descriptions). We chose VR as a tool to immerse participants in the respective scenarios, together with the story details. Note that the VR application did not include a detection part, but mockups of devices and respective tracking spaces within the virtual scene. Participants tried every scene using an HTC Vive Pro headset. There was no search task for the scenes, however, we asked them to think aloud and report on their experience. After every scene, participants answered 5-point Likert items on comfort and frequency of use and ranked the five visualisations from most preferred to least preferred (referring to the current scene, respectively). After all scenes, we put 5-point Likert items per visualisation on learnability and understandability (we provided screenshots of all five visualisations for recap). We measured usability of an HMD as an output device for *PriView* using SUS [4] and workload using the Raw TLX [21]. We conducted a final semi-structured interview covering participants' experience, potential usage contexts, preferred visualisation, and preferred output device (i.e., mobile application vs head-mounted display, cf. Appendix B.3 for full interview guide).

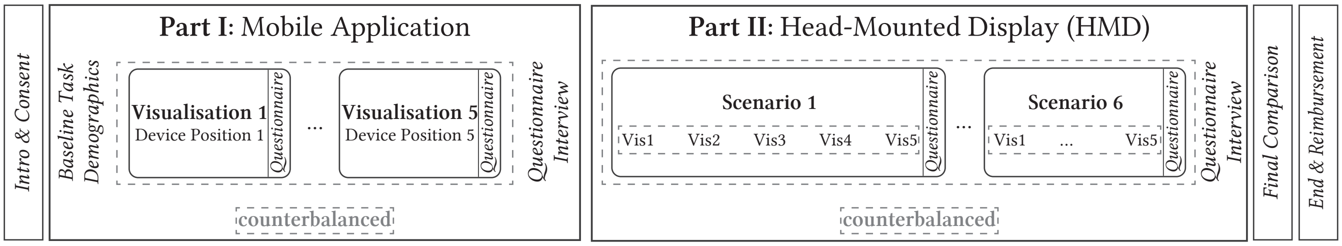


Figure 5: Study Procedure: We investigated two *output devices* of *PriView*, namely a mobile application (Part I) and a head-mounted display (Part II). We used a within-subjects design in which every participant encountered Part I and II in this order. In both parts, we explored various visualisations. For the mobile application, participants conducted a total of 6 search tasks: one without using the application (baseline) and, in counterbalanced order, one for every visualisation. Each task was followed by a questionnaire. For the HMD, participants experienced various application scenarios in counterbalanced order. Within every scenario, we counterbalanced all five visualisations. Each scenario was followed by a questionnaire. We complemented the session with an interview and a final comparison of both output devices.

6.2.5 Study Design. We conducted a within subjects study with scenario and visualisation as independent variables. Every participant experienced every visualisation in every scenario. The order of scenarios was counterbalanced using a Latin Square [52]. Within scenario, we counterbalanced the order of visualisation. Note that in most scenarios, using *PriView* would be the *secondary tasks* (e.g., at a train station, users' main task is usually to find their way). However, within the study, exploring the environment and visualisations was participants' main task. We asked participants to think aloud while exploring the environments. Each scenario was complemented by a questionnaire on comfort, use, and preferred visualisation (refer to Appendix B.2). The session ended with a final questionnaire on the VR part (including Likert items for every visualisation, SUS, and Raw TLX), the IUIPC scale [31] to acquire participants general privacy perception and a semi-structured interview, including opinions on the VR prototype, potential use cases and a comparison to the mobile application (refer to Appendix B.3).

6.3 Procedure

To ensure a smooth study procedure, we conducted a total of three pilot runs. The final procedure was as follows. Upon arrival at our institute, we asked participants to disinfect and wash their hands (the two experimenters did the same). They then signed a consent form and we introduced them to the general concept of *PriView*. Participants then conducted the study (cf. Figure 5):

Part I Participants first conducted the baseline task (i.e., search for devices in our lab without using the mobile application). We then send them to a PC behind a black curtain to fill in demographics, while we would rearrange the Device Position. We then introduced them to our mobile application. Next, they conducted five search tasks using every Visualisation in counterbalanced order. After every task, they filled in Likert items (on comfort, learnability, understandability and frequency of use, cf. Appendix A.1) on the PC behind the black curtain while we changed device position. After the last search task, participants filled the SUS and Raw TLX for the mobile application and we conducted a semi-structured interview (cf. Appendix A.2 for the full interview guide).

Part II We introduced participants to the idea of using *PriView* in everyday life using a head-mounted display (in the form of, e.g., AR glasses), and presented our prototype. Participants then experienced every Visualisation in every Scenario in counterbalanced order. After every Scenario, participants filled in Likert items on comfort, potential use and preferred visualisation (cf. Appendix B.2.1). After the last Scenario, participants filled in a final questionnaire (including learnability and understandability of the visualisations, SUS and Raw TLX of the VR application, and the IUIPC scale, cf. Appendix B.2.2) and we interviewed them (cf. Appendix B.3 for the full interview guide).

We concluded with a final question on comparing the two prototypes (i.e., handheld vs handsfree) and an opportunity for participants for further comments or questions. We recorded audio during the whole session. We conducted interviews in English or German.

6.4 Recruitment

We recruited 24 participants through university mailing lists and social networks. The study took place in a single, separate room at our institute. A study session took around 90 minutes in total. Participants were reimbursed with € 15.

6.5 Ethical Considerations

We carefully followed all guidelines provided by the ethics committees at our institutions. We made sure to preserve participants' privacy and gather informed consent prior to the study following our national data protection regulations. We stored all study data anonymously on university servers. We only used participants' personal data for handling the consent and reimbursement. We did not connect this information to the rest of the study data and deleted it afterwards. Finally, at the time of the study, we took great care to comply with all Covid-19 related rules in Bavaria, Germany. In particular, we kept the minimum distance to participants at all times and made sure to disinfect the whole setup after every session.

6.6 Participants

A total of 24 people participated in our study, 9 female and 15 male (we additionally provided "other" and "prefer not to say", but no participant chose that). Participants' age ranged from 20 to 56 (Mean=25.54, SD=6.95). Most of them were students (18), others employed full and part time (3 each). Participants rated their prior experience with VR (Mean=2.33), AR (Mean=2.21), and Smart Homes (Mean=2.87) on a 5-point scale (1=Low). We additionally asked participants to list their smart devices. They mentioned between 0 and 10 devices (mean number of devices: 2.79), mostly smartphones (22), but also smart TVs (7), smart speakers (6), and more. To assess participants' general privacy attitude, we used the IUIPC [31]. Participants rated their wish for *control* (Mean=5.75[14], SD=1.19), a high *awareness* (Mean=6.24[14], SD=1.05), and the perceived ratio between benefits and *collection* (Mean=5.44[14], SD=1.39).

6.7 Limitations

For our study, we chose a within-subject design to make participants experience our approach from both, a technical (Part I) and a conceptual (Part II) perspective. We only compare participants' preference regarding output device after they experienced both parts, hence we assume latency and recency effects to be minimal.

For our lab setting (Part I), we applied randomisation to the order of visualisations and respective device positions, yet we cannot fully exclude learning effects in the search tasks. Moreover, we only explored a subset of devices and visualisations. Lastly, the study was conducted in a single room to avoid noise in the device detection, hence we cannot make assumptions about different settings.

For the varying scenarios in VR (Part II), we took great care to immerse participants in the different settings. However, not every scenario might have been realistic to every participant (e.g., if they never happened to find a recording device in a rental apartment). Furthermore, self-reports on privacy preferences are known to differ from users' actual behaviour (cf. the "privacy paradox", see [19] for an overview). Lastly, our sample is biased towards young male students and might not be representative.

6.8 Data Analysis

All think aloud and interview recordings from both parts were transcribed for analysis (except for one corrupted audio recording). Initially, three researchers performed inductive coding for three participants independently and discussed results with each other. The researchers agreed on a code book containing a total of 67 codes (cf. Appendix C). Disagreements were tracked, and inter-rater agreement was calculated at 89.82%. Then, two coders proceeded with half of the remaining transcripts each and coded them independently by means of the code book. Researchers compared and discussed codes and resolved any disagreements. In the following, we present first qualitative insights towards our concept[15]. We enumerate participants from P1 to P24. Quotes were translated from German where necessary.

7 RESULTS & DISCUSSION

We summarise and discuss the results of our study in the form of **design challenges**. While some results are strongly coupled to the respective *output device*, we will also highlight overarching opinions towards our concept.

7.1 Overall Perception of *PriView*

Participants overall were positive towards the idea of *PriView*, e.g.:

> *"Actually, I think the idea is pretty cool. I think there is a lot of concerns about technology nowadays (...), so that's good to have something user friendly."* (P2)

> *"It was a very good experience for me to see that some devices are on, (...) and informed me that they are tracking or recording anything of me."* (P6)

> *"It was interesting, especially the [Text Labels] so I can actually see that the device is turned on and I see there is a microphone and it could actually record me (...) It was also fun to see visually, (...)."* (P8)

> *"I like that they show you where there is a recording device. The application, I think, is really useful."* (P18)

In particular, it made them feel safer (e.g., *"I really felt safer, because I feel like when I walk out of here, I will think a lot about which information I'm sharing with third parties."*, P16), supported them to protect their privacy (e.g., *"I wouldn't say it protects it directly, but when you use the app and you see that there is a camera or microphone you might behave differently and this protects your privacy."*, P7) and enabled them to take countermeasures, if necessary:

> *"Let's take the hotel room example. There I could unplug the smart TV or something like that."* (P14)

> *"And I would turn it off or ask the host to pick it up or take it away. For the smart TV, I think I would put a post-it or so [to cover the camera]."* (P19)

PriView also supported participants in finding devices (e.g., *"(...) it did help me know a lot of devices which otherwise I would have had no chances of knowing."*, P24), which was perceived positively.

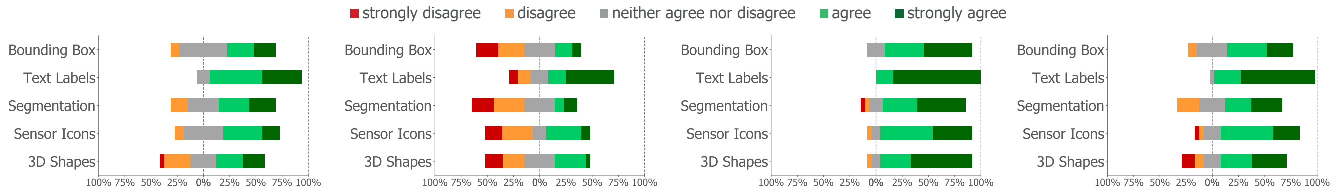
7.2 Output Devices

We particularly compared two output devices for using *PriView*, namely a mobile application and an HMD. Participants saw benefits in both, but mostly preferred the HMD ($N = 19$).

7.2.1 Handheld: Mobile Application. Overall, the mobile application received positive feedback with a rather high SUS (Mean=71.14[16], SD=8.53) and a rather low cognitive workload ((Raw) NASA-TLX Mean=14.28[17], SD=4.52). Participants particularly liked that the app was *"very innovative and comfortable"* (P24), convenient (P17, P20), and easy to use (P15, P16, P19, P20). Participants preferring the mobile application over the HMD particularly appreciated the fact that they would have it with them anyways (P17) and could put it away anytime (P11).

[14] the IUIPC ranges from 1 to 7, where 7 denotes high sensitivity towards privacy
[15] Our sample comprises 24 participants. Note that only little new information is gained beyond 20 participants [37].

[16] the SUS score ranges from 0 to 100, while a score greater than 68 is "above average" [4]
[17] the NASA-TLX workload score ranges from 0 to 100 [21]



(a) I felt comfortable using this visualisation. **(b) I would use this application frequently.** **(c) This visualisation was easy to learn.** **(d) This visualisation was understandable.**

Figure 6: Study Part I (using *PriView* in a mobile application): Likert Ratings per visualisation for a) comfort, b) frequent use, c) learnability, and d) understandability.

Furthermore, they felt rather comfortable using any of the visualisations (Median over all visualisations: 4, cf. Fig. 6a for details per visualisation) and would use the application frequently if they had access to a thermal camera (Median over all visualisations: 3, cf. Fig. 6b for details per visualisation).

7.2.2 Handsfree: Head-Mounted Display (HMD). Likewise, using *PriView* in a head-mounted display (HMD) overall received positive feedback. Participants found our prototype usable (SUS Mean=73.85[16], SD=7.52) while perceiving a rather low cognitive workload ((Raw) NASA-TLX Mean=12.85[17], SD=4.66). In particular, participants liked that it was easy to use (e.g., P4, P7, P18, P20), and that there was no need to scan the environment manually using their mobile phone (e.g., *"I guess just for convenience it's easier to take off and on a pair of glasses rather than having to scan the room with the phone."*, P2). Participants wearing glasses per se could well imagine having it integrated with their daily life (P6 and P10).

Output Devices. For *PriView* being applicable in daily life, it should be easily accessible and ideally be integrated with personal devices. Thus, some participants preferred the smartphone. Yet, this might change as smart glasses become more ubiquitous. In any case, scanning the environment for potential privacy intrusion should be effortless and fast.

7.3 Visualisations

7.3.1 Learnability & Understanding. Overall, our visualisations were understandable as well as easy to learn in both modalities. For the mobile application, participants strongly agreed that the *Text Labels* and *3D Shapes* were easy to learn (Median: 5). They agreed (Median: 4) for the other visualisations (cf. Fig. 6c). Regarding understanding, they strongly agreed for the *Text Labels* (Median: 5) and agreed for the rest (Median: 4, cf. Fig. 6d).

As for the second part of the study (using the HMD), we exposed participants to the same visualisations multiple times in various scenes (in counterbalanced order). Overall (i.e., at the end of the study session), participants strongly agreed that all visualisations were easy to learn (Median: 5), except for the *Floor Markers* (Median: 4, cf. Fig. 7a). Regarding understandability, participants strongly agreed on *Text Labels* and *Bounding Boxes* (Median: 5, cf. Fig. 7b). Looking into more detail at participants' comments, we found that they understood the *Text Labels* immediately:

> *"This is way easier to understand."* (P18)

> *"So this one does give me a bit more comfort in a sense. It tells me that the provider is from this place – because I expect the security camera to be from this place. "* (P9)

Also, the *Bounding Boxes* were mostly clear and easy to understand to participants:

> *" Okay, so now it's again with the red squares. It's very intuitive to use. Usually, when you stand here at the station you actually move forward and maybe around so you can (...) look around and spot them. So in this case it's very practical actually."* (P8)

In contrast, the meaning of the *3D Shapes* and *Floor Markers* sometimes was not clear on first sight and/or only became clear after a while:

> for the *Floor Markers*: *"I think it could be some kind of escape route or direction sign."* (P7)

> for the *3D Shapes*: *"As soon as I figured out how it worked, I liked the 3D Shapes."* (P21)

> *"There is a cone of light emerging from the fridge. I am not a 100% sure what that is."* (P10)

For the *Warning Icon*, participants often expected more to it, while it was just a static indicator in our current mockups:

> *"I don't know what this is supposed to show me. It's just an exclamation mark."* (P6)

> *"There is a red exclamation mark. It stays there (...). It doesn't change, nor change its position."* (P7)

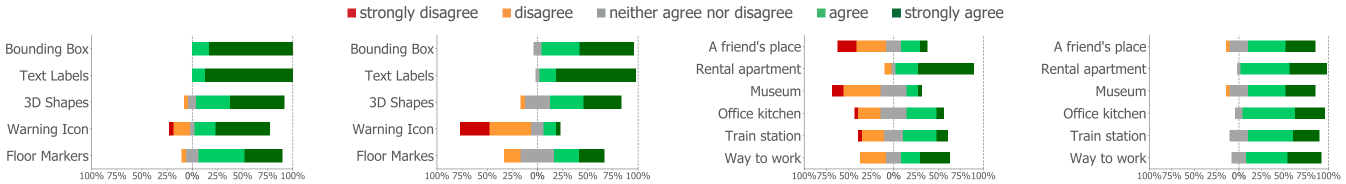
Enhance Understanding. Our results indicate that textual information is immediately easy to understand, while visualisations of tracking spaces might be misleading at first sight. However, the latter transported information that users would like to understand (e.g., where they can stand in a train station without being recorded):

> *"Now the question is where I can stand without being tracked."* (P11)

> *"Yes I like this because now I can see I am in an area where it does not record me that well."* (P19)

Future work should thus investigate in more detail how such visualisations can be made understandable.

7.3.2 Preferred Visualisations. In every part of the study (mobile app and HMD), we asked participants for their preferred visualisation, addressing **RQ3**. For the second part (HMD), we additionally asked participants to rank the visualisations from most preferred



(a) This visualisation was easy to learn.

(b) This visualisation was understandable.

(c) I would use this application frequently (per scene).

(d) I felt comfortable using this application (per scene).

Figure 7: Study Part II (using *PriView* in an HMD in various scenes): Likert Ratings per visualisation for a) learnability and b) understandability; and per scene for c) frequent use and d) comfort.

(rank 1) to least preferred (rank 5) for every scene, resulting in a total of 144 rankings (see Figure 8 for an overview of rankings and Appendix D for details on the ranking per scenario).

Participants mainly preferred the *Text Labels* (ranked first $N = 17$ for the mobile application and $N = 62$ for the HMD), mainly due to the fact that it gave them the highest level of information, i.e. most details on the devices. P19 additionally valued the arrow within the text labels (HMD) pointing to the concrete devices. However, participants also raised concerns regarding the visibility of the text boxes (i.e., they were transparent in grey which was hard to see in, e.g., the train station scene), text boxes disappearing before having them read completely (for the mobile application, P17), and also the source of information. In addition, many participants did not want this information about their own personal devices to be revealed.

The second most favourite (38 times on rank 1) in the HMD were the *3D Shapes*, again due to their high level of detail in terms of covering the tracking space. However, participants tended to feel visually overloaded with this visualisation, especially in places crowded with sensors. They would have preferred to turn them off after having completed inspecting the scene. However, the *3D Shapes* supported participants to even localise out-of-view cameras and the direction in which they are placed, especially in the "way to work" scenario. Furthermore, P23 doubted that the "sharp edges" of the 3D shapes are realistic, especially for the audio bubbles. P19 mentioned that environmental noise might crucially influence the tracking space, which was not included in the visualisation. Within the mobile application, the 3D Shapes around the devices were perceived differently by participants. On one hand, participants found them visually appealing:

> *"I really liked them. The bubbles were aesthetically the one that I liked the most."* (P15)

On the other hand, the shapes were perceived as transporting no information (P18), and being *"very intrusive"* (P14), but then again potentially hard to spot for small devices (P14).

The third most favourite (20 times on rank 1 for the HMD) were the *Bounding Boxes*. Participants especially valued these for the fast localisation of – especially hidden – devices. However, many participants would have liked the option to then reveal additional information upon having found the framed devices. In the mobile application, the red frames were preferred by 3 participants.

As for the *Floor Markers* (HMD only), participants' had split opinions (18 times on rank 1, 15 on rank 5). Some participants appreciated the respective information, i.e. the highlighting of the areas with potential privacy intrusion. P19 even mentioned the floor markers to be *"suitable for daily life"*, but still raised concerns about the accuracy.

Lastly, the *Warning Icon* (HMD only) was least preferred by participants (6 times on rank 1, 97 on rank 5). Main reasons for this were the low amount of information (e.g., *"I don't know what this is supposed to show me."*, P6) and the possibility of getting too used to it, i.e. not recognising it anymore (e.g., *"In the city centre, where there are lots of cameras, you probably don't recognise it anymore"*, P19). Participants would however see benefits in combining the warning icon with more detailed information on demand or the icon flashing up on changes they would not be aware of otherwise.

In the mobile application, the *Segmentation* was appreciated for being conspicuous and easy to recognise (e.g., *"It's easier to catch it"*, P13). While the *Sensor Icons* were not preferred by some participants for being too small or unclear (e.g., *"It's hard to really walk very close to the device in order to get the icon. It's so small."*, P22), others suggested iconography as visualisations (e.g., *"Though I would think that having this information, (...) probably easier for me to grasp if it was in some kind of iconography or symbols."*, P14).

How to visualise? Overall, participants liked the visualisations that we suggested. However, they raised two main questions. Firstly, participants would have liked a hint to out-of-view devices before having to scan the environment manually. As an example, in the "way to work" scene, we placed a security camera around the corner from the participants' perspective. This means they couldn't see text information next to or red frames around it but could recognise the camera's tracking space using the *3D Shapes* or *Floor Markers* (e.g., *"Ah, back there is more yellow. I didn't see this so far."*, P19).

Secondly, participants were questioning if particularly audio recording has such a sharp border as suggested by our visualisations. However, there is probably many factors to this, including not only the devices' specifications but also environmental noise and volume of the users' voice. Moreover, participants were interested in whether data collection would actually affect them. For instance, in the train station scene, we placed passengers on the train recording audio while users were standing outside the train. In the office kitchen scene, P7 would have liked to know whether they can still be overheard by the coffee machine while sitting at the table.

7.3.3 Amount of Information. Generally, participants valued cases in which they got information through *PriView* that they would not have known otherwise. As an example, in the rental apartment scene, where data collection was unexpected to most participants,

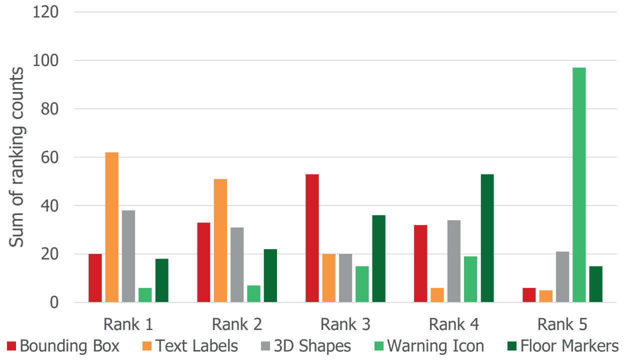


Figure 8: Study Part II (using *PriView* in an HMD): Overall ranking of visualisations, i.e. sum of count of rank positions over all scenes. Each of the 5 visualisation was ranked in 6 scenes by 24 participants.

they generally wished for a higher level of information. For instance, the *Warning Icon* was most of the time providing too little information for participants: participants perceived the conveyed information sometimes redundant (e.g., in the train station, where participants already expected CCTV to be present) and in other situations as insufficient (e.g., in the rental apartment).

Few participants wished for additional information, e.g. the precise position (P23) and type of sensor (P8, P23), whether or not it is actually capturing them (P7, P15), as well as more fine-grained device status information, i.e. if it is currently on or recording (P13). P21 suggested to also add the owners of personal devices. P15 and P19 were especially interested in differentiating devices that belong to a public organisation from private ones. Moreover, the desired amount of information might vary over time, e.g., P12 would have preferred to see all available details on first use, but would subsequently be fine with a less detailed visualisation, such as the bounding boxes. Lastly, the adequate information level also depends on the number of devices being present according to P21.

The right amount of information. The main question that arises is how to balance the desired level of information with visual overload. Participants recognised that especially if scenes are crowded, visual clutter might overwhelm them (e.g., *"If I imagine, there was hundreds of people on the platform, this would be a huge blue mass."*, P23). However, detailed information about, e.g., tracking spaces was still appreciated. To reduce visual overload, P7 suggested a lower level of information for devices that do not actually capture them (e.g., the smartphone in somebody's pocket).

Moreover, the information should be justified. For instance, in public scenes, we added some device providers as "unknown" in the text labels. This was irritating participants more than actually informing them (e.g., *"There is another one, provider 'unknown'. This is different from the other one. This makes me suspicious."*, P19). In such cases, it might be more meaningful to present reliable information only. To summarise, the right amount of information is highly context-dependent (cf. **RQ2**).

7.4 Usefulness and Potential Use Cases

Overall, participants saw benefits in using *PriView* in the scenarios we presented them. However, most participants would not use it in places where the information is redundant (e.g., in a train station or museum, CCTV being present was obvious for them). Other *scenarios* were more convincing to them for the following *purposes*.

7.4.1 Scenarios. From the scenarios we presented in VR to our participants, they strongly agreed to use it frequently in a rental apartment (Median: 5, cf. Figure 7c). They, however, felt comfortable with using it in all scenarios (Median: 4 for all scenes, cf. Figure 7d).

Some participants mentioned further scenarios, including unfamiliar and/or public restrooms (P1, P19), changing rooms (P15), and doctors' waiting rooms (P19). Other participants mentioned unspecific locations such as *"outside my home"* (P6), *"places where I don't feel well"* (P4), or *"foreign private spaces"* (P11). P19 even mentioned a rental car as it is *"temporarily private"*.

Contextualise *PriView*. There is a myriad of factors that impacts users' privacy concerns (cf. Section 4.1) and thus their preference on where to use *PriView*. Our results indicate that places that are considered private beyond users' homes are especially relevant. At the same time, this is where they did not necessarily expect data collection to happen. *PriView* should thus adapt to such cases.

7.4.2 Purposes. The main purpose we imagine *PriView* to be used for is supporting privacy by increasing users' awareness. Many participants agreed that this is indeed the case, e.g.:

> *"In most buildings, cameras are signed, but not in every building. (...) In a law office or when you talk about certain contracts or another example is in the restroom, I don't want a camera to be in the cabin."* (P7)

> *"Maybe if there are meetings where there is some secret information. Then I might check the room first."* (P10)

Furthermore, many other interesting purposes were mentioned, from curiosity and fun to maintenance and search for lost devices. P19 mentioned to apply the concept for safety and warn about dangerous parts in the street. P4 would also check if devices are still on to improve sleep quality. P3 and P19 reversed the museum scene and argued that *PriView* could help thieves not to be recorded.

Why to use *PriView*. Regardless of the specific scenario, *PriView* should not stand in the way of users' primary task. While in some cases, this might be identical with using *PriView* (e.g., for maintenance), in other cases the visualisation should stand behind (e.g., in a train station where users are mainly trying to find their way). However, it remains questionable how to verify users and their purposes to avoid thieves and potential attackers misusing *PriView*.

7.5 Interaction Modalities

In our study, the mobile application was following an "on demand" approach (i.e., actively scanning the environment), while the VR mockups from a participants' perspective were "always on", controlled by the experimenter. However, participants generally wished for an opportunity to interact with *PriView* (cf. **RQ4**). On one hand, many explicit approaches to activate the visualisations were mentioned, including buttons (P2, P10) or gestures (P14). On the other hand, participants also wished for an opportunity to be notified about changes by the system rather than to actively interact. e.g.:

> *"(...), if you leave an untracked area or an area where you turned it off, then (...) the exclamation mark could reappear and you could click on it for details."* (P23)

Others emphasised a wish for turning it off (rather than on), e.g.:

> *"Maybe in the museum, just being aware for the first 5 - 10 seconds, and then having the option to switch it off could be useful. Because a museum is not a dangerous environment. I just want to be made aware and then have the personal choice to continue. But I don't want that information to be there 24/7."*, P22).

P23 would prefer to have control over the level of detail at any time. Moreover, many participants could imagine nested approaches, i.e., having the possibility to reveal more details on demand, e.g.:

> *"I think this [text labels] would be the third level I want to have. I want to be notified by the exclamation mark: 'hey, something is going on'. I want to see where the thing is that's tracking me and then I would go to this one to actually see."* (P14)

Interacting with *PriView*. When using *PriView*, users should a) not miss out important information, but at the same time b) not be overwhelmed with information they do not need. This raises the question to what extent the system should keep users (not) in control what and when to show.

7.6 Privacy: Self vs Others

Participants agreed on the fact that *PriView* could actually help them to protect their privacy by increasing their awareness, answering **RQ1**. Some participants explicitly mentioned they would take countermeasures, e.g. unplug devices in a rental apartment or create noise in the office kitchen (P19). While participants were highly interested in the shown information, some explicitly mentioned that they would not want to reveal information about their own personal devices:

> *"To a certain degree, it's redundant and maybe even TMI [too much information], because like it tells me about other people's devices. At the same time, I'm still kind of wondering that – if they have the same features that I do – can they also see my phone and the brand of my phone?"* (P9)

> *"In a train station, I can imagine having this running to see if somebody is recording me. However, this is a bit paradox as I then record others as well."* (P19)

Moreover, participants reacted differently when thinking about others using *PriView* in their vicinity. While some would be comfortable, many would not like *PriView* to be used in their surroundings, especially in their own places, as it might create an atmosphere of mistrust:

> *"If it was at my home, I would not feel comfortable, because I would like my friends or guests to trust me. In a public building, I would maybe use it too, so it would be not that unusual and it would be okay for me."* (P7)

> *"In my place, if somebody whom I invited is walking in my living room and would be using the app, just per standard protocol, I think that would be rude. I wouldn't mind if someone used it, for example, when they're going to my bathroom, because I mean, there have been cases where people have been recorded in other people's bathrooms. I think as long as the person is using it in a situation or in a moment where [they have] a reasonable expectation of privacy, I would consider it okay. If you're just generally suspecting that I'm recording you in any way, then I would think it's kind of rude because you could have just asked me."* (P19)

> *"At my place, I would probably feel a little bit insulted, since like for me it would mean that he's not feeling safe at my place. (...) In public, I think it wouldn't really disturb me."* (P21)

How to (not) protect privacy using *PriView*. While all participants were interested in the information provided trough *PriView*, many of them would not like to have their personal devices included and shown in the system. Thus, *PriView* needs to strike a balance which information (not) to reveal, also considering multiple users' privacy needs. Prior work, e.g., suggested to consider different types of relationships between device users [18] and to provide usable access control mechanisms [55]. For *PriView*, this eventually means to refrain from including personal devices, to consider users' relationship to the place and device owner as well as potential bystanders being present, or to give users the opportunity to explicitly opt-out the fact that their devices are included and shown to others.

8 DIRECTIONS FOR FUTURE RESEARCH

8.1 Information Sources

One prerequisite to employ *PriView* is gathering the respective information to visualise. For our mobile application, we used a training dataset of 1239 photos and computer vision techniques. However, gathering such training data would be costly in terms of time and effort. Another opportunity would require providers to reveal general device information, which might be another limiting factor (cf. [45]). While this information might reveal the device specifications (including tracking space), it might not include the current device status. The latter would then need to be detected on spot using, e.g., a thermal camera. Moreover, such information could also be crowdsourced (cf. the *IoT Assistant*[18]). However, this again requires contribution by individuals as well as knowledge about devices.

This opens interesting directions for future research. Firstly, how can the respective information be collected to be visualised in *PriView*? Secondly, how can this information be handled in a way that preserves the privacy of device owners, recorded users and bystanders? Thirdly, how to choose the information that is relevant for users in the respective situation?

[18] https://www.iotprivacy.io/login, last accessed September 1, 2020

8.2 Adapting, Configuring, Contextualising

In our study, using *PriView* was participants' primary task. However, in most of the settings, this is not necessarily the case (e.g., enjoying a museum exhibition). Thus, many participants wished for more subtle visualisations and/or for a possibility to turn it off to focus on their actual goal. Other wishes for personalising *PriView* included colour (P19) and information (P9, P22) choice.

To summarise, future research should investigate the following questions: how can *PriView* be adapted to users' needs automatically, e.g. based on context? Which options should be given to users to adapt *PriView* to their needs manually? And how would a configuration interface for *PriView* be integrated?

9 CONCLUSION

In this paper, we present *PriView*, a concept with which we can visualise potential privacy intrusion in the users' vicinity (by, e.g., audio or video recordings). We explored sample application scenarios and visualisations for *PriView* and implemented two prototypes, namely a mobile application and a head-mounted display showing mockups of various scenes in VR. We found that users generally appreciated the idea of *PriView* and saw interesting use cases, including, but also beyond protecting their privacy. We further found that more detailed visualisations were preferred in most settings, while in other settings subtle indications might be more suitable. We summarise our results in design challenges and point out future research directions, meant to support researchers and practitioners alike. We hope our exploration to inform further work on privacy visualisations for varying smart environments.

ACKNOWLEDGMENTS

We would like to thank Christian Gessner for creating the VR scenes and all subjects who participated in our study for their time and valuable feedback on our concept. This work received funding from DTEC.Bw in the context of the "MuQuaNet" project.

REFERENCES

[1] Yomna Abdelrahman, Paweł W. Woundefinedniak, Pascal Knierim, Dominik Weber, Ken Pfeuffer, Niels Henze, Albrecht Schmidt, and Florian Alt. 2019. Exploring the Domestication of Thermal Imaging. In *Proceedings of the 18th International Conference on Mobile and Ubiquitous Multimedia* (Pisa, Italy) *(MUM '19)*. Association for Computing Machinery, New York, NY, USA, Article 9, 7 pages. https://doi.org/10.1145/3365610.3365648

[2] Anne Adams. 2000. Multimedia Information Changes the Whole Privacy Ballgame. In *Proceedings of the Tenth Conference on Computers, Freedom and Privacy: Challenging the Assumptions* (Toronto, Ontario, Canada) *(CFP '00)*. Association for Computing Machinery, New York, NY, USA, 25–32. https://doi.org/10.1145/332186.332199

[3] Debjanee Barua, Judy Kay, and Cécile Paris. 2013. Viewing and Controlling Personal Sensor Data: What Do Users Want?. In *Persuasive Technology*, Shlomo Berkovsky and Jill Freyne (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 15–26.

[4] John Brooke. 1996. SUS: a "quick and dirty" usability scale. *Usability evaluation in industry* 1 (1996), 189.

[5] Nico Castelli, Corinna Ogonowski, Timo Jakobi, Martin Stein, Gunnar Stevens, and Volker Wulf. 2017. What Happened in My Home? An End-User Development Approach for Smart Home Data Visualization. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 853–866. https://doi.org/10.1145/3025453.3025485

[6] Yuxin Chen, Huiying Li, Shan-Yuan Teng, Steven Nagels, Zhijing Li, Pedro Lopes, Ben Y. Zhao, and Haitao Zheng. 2020. Wearable Microphone Jamming. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376304

[7] Youngjun Cho, Nadia Bianchi-Berthouze, Nicolai Marquardt, and Simon J. Julier. 2018. Deep Thermal Imaging: Proximate Material Type Recognition in the Wild through Deep Learning of Spatial Surface Temperature Patterns. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3173574.3173576

[8] R. Chow. 2017. The Last Mile for IoT Privacy. *IEEE Security & Privacy* 15, 6 (2017), 73–76. https://doi.org/10.1109/MSP.2017.4251118

[9] Richard Chow, Serge Egelman, Raghudeep Kannavara, Hosub Lee, Suyash Misra, and Edward Wang. 2015. HCI in Business: A Collaboration with Academia in IoT Privacy. In *HCI in Business*, Fiona Fui-Hoon Nah and Chuan-Hoo Tan (Eds.). Springer International Publishing, Cham, 679–687.

[10] Hyunji Chung, Michaela Iorga, Jeffrey Voas, and Sangjin Lee. 2017. Alexa, Can I Trust You? *Computer* 50, 9 (2017), 100–104. https://doi.org/10.1109/MC.2017.3571053

[11] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. 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* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376389

[12] Mary J. Culnan and Pamela K. Armstrong. 1999. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science* 10, 1 (1999), 104–115. https://doi.org/10.1287/orsc.10.1.104

[13] P. Emami-Naeini, Y. Agarwal, L. Faith Cranor, and H. Hibshi. 2020. Ask the Experts: What Should Be on an IoT Privacy and Security Label?. In *2020 IEEE Symposium on Security and Privacy (SP)* (San Francisco, CA, USA). IEEE, New York, NY, USA, 447–464. https://doi.org/10.1109/SP40000.2020.00043

[14] Pardis Emami-Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Cranor, and Norman Sadeh. 2017. Privacy Expectations and Preferences in an IoT World. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS '17)*. USENIX Association, Berkeley, CA, USA, 399–412.

[15] Pardis Emami Naeini, Martin Degeling, Lujo Bauer, Richard Chow, Lorrie Faith Cranor, Mohammad Reza Haghighat, and Heather Patterson. 2018. The Influence of Friends and Experts on Privacy Decision Making in IoT Scenarios. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 48 (Nov. 2018), 26 pages. https://doi.org/10.1145/3274317

[16] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, Article 534, 12 pages. https://doi.org/10.1145/3290605.3300764

[17] Markus Funk, Robin Boldt, Bastian Pfleging, Max Pfeiffer, Niels Henze, and Albrecht Schmidt. 2014. Representing Indoor Location of Objects on Wearable Computers with Head-Mounted Displays. In *Proceedings of the 5th Augmented Human International Conference* (Kobe, Japan) *(AH '14)*. Association for Computing Machinery, New York, NY, USA, Article 18, 4 pages. https://doi.org/10.1145/2582051.2582069

[18] Christine Geeng and Franziska Roesner. 2019. Who's In Control? Interactions In Multi-User Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300498

[19] Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security* 77 (2018), 226 – 261. https://doi.org/10.1016/j.cose.2018.04.002

[20] Hamza Harkous, Kassem Fawaz, Kang G. Shin, and Karl Aberer. 2016. PriBots: Conversational Privacy with Chatbots. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 6 pages. https://www.usenix.org/conference/soups2016/workshop-program/wfpn/presentation/harkous

[21] Sandra G. Hart. 2006. Nasa-Task Load Index (NASA-TLX); 20 Years Later. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 50, 9 (2006), 904–908. https://doi.org/10.1177/154193120605000909

[22] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "Nutrition Label" for Privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (Mountain View, California, USA) *(SOUPS '09)*. Association for Computing Machinery, New York, NY, USA, Article 4, 12 pages. https://doi.org/10.1145/1572532.1572538

[23] Agnieszka Kitkowska, Mark Warner, Yefim Shulman, Erik Wästlund, and Leonardo A. Martucci. 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)*. USENIX Association, Berkeley, CA, USA, 437–456. https://www.usenix.org/conference/soups2020/presentation/kitkowska

[24] Predrag Klasnja, Sunny Consolvo, Tanzeem Choudhury, Richard Beckwith, and Jeffrey Hightower. 2009. Exploring Privacy Concerns about Personal Sensing. In *Pervasive Computing*, Hideyuki Tokuda, Michael Beigl, Adrian Friday, A. J. Bernheim Brush, and Yoshito Tobe (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 176–183.

[25] Tobias Kowatsch and Wolfgang Maass. 2012. Privacy Concerns and Acceptance of IoT Services. In *The Internet of Things 2012 : New Horizons*. IERC - Internet of Things European Research Cluster, Halifax, UK, 176–187. https://www.alexandria.unisg.ch/212316/

[26] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 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 (2018), 102. https://doi.org/10.1145/3274371

[27] Scott Lederer, Anind K. Dey, and Jennifer Mankoff. 2002. *A Conceptual Model and a Metaphor of Everyday Privacy in Ubiquitous*. Technical Report. University of California at Berkeley, USA.

[28] Scott Lederer, Jennifer Mankoff, and Anind K. Dey. 2003. Who Wants to Know What When? Privacy Preference Determinants in Ubiquitous Computing. In *CHI '03 Extended Abstracts on Human Factors in Computing Systems* (Ft. Lauderdale, Florida, USA) *(CHI EA '03)*. Association for Computing Machinery, New York, NY, USA, 724–725. https://doi.org/10.1145/765891.765952

[29] H. Lee and A. Kobsa. 2016. Understanding user privacy in Internet of Things environments. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)* (Reston, VA, USA). IEEE, New York, NY, USA, 407–412.

[30] H. Lee and A. Kobsa. 2017. Privacy preference modeling and prediction in a simulated campuswide IoT environment. In *2017 IEEE International Conference on Pervasive Computing and Communications (PerCom)* (Kona, HI, USA). IEEE, New York, NY, USA, 276–285.

[31] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research* 15, 4 (2004), 336–355. https://doi.org/10.1287/isre.1040.0032

[32] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. 01 Apr. 2020. Smart Devices in Airbnbs: Considering Privacy and Security for both Guests and Hosts. *Proceedings on Privacy Enhancing Technologies* 2020, 2 (01 Apr. 2020), 436 – 458. https://doi.org/10.2478/popets-2020-0035

[33] Davit Marikyan, Savvas Papagiannidis, and Eleftherios Alamanos. 2019. A systematic review of the smart home literature: A user perspective. *Technological Forecasting and Social Change* 138 (2019), 139 – 154. https://doi.org/10.1016/j.techfore.2018.08.015

[34] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. 2020. "You Just Can't Know about Everything": Privacy Perceptions of Smart Home Visitors. In *19th International Conference on Mobile and Ubiquitous Multimedia* (Essen, Germany) *(MUM 2020)*. Association for Computing Machinery, New York, NY, USA, 83–95. https://doi.org/10.1145/3428361.3428464

[35] Karola Marky, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder, and Max Mühlhäuser. 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* (Tallinn, Estonia) *(NordiCHI '20)*. Association for Computing Machinery, New York, NY, USA, Article 4, 11 pages. https://doi.org/10.1145/3419249.3420164

[36] Simon Mayer, Yassin N. Hassan, and Gábor Sörös. 2014. A Magic Lens for Revealing Device Interactions in Smart Environments. In *SIGGRAPH Asia 2014 Mobile Graphics and Interactive Applications* (Shenzhen, China) *(SA '14)*. Association for Computing Machinery, New York, NY, USA, Article 9, 6 pages. https://doi.org/10.1145/2669062.2669077

[37] M Granger Morgan, Baruch Fischhoff, Ann Bostrom, Cynthia J Atman, et al. 2002. *Risk communication: A mental models approach*. Cambridge University Press, Cambridge, United Kingdom.

[38] David H. Nguyen, Alfred Kobsa, and Gillian R. Hayes. 2008. *An Empirical Investigation of Concerns of Everyday Tracking and Recording Technologies*. Association for Computing Machinery, New York, NY, USA, 182–191. https://doi.org/10.1145/1409635.1409661

[39] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.

[40] Helen Nissenbaum. 2009. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press, Stanford, CA, USA.

[41] Rebecca S. Portnoff, Linda N. Lee, Serge Egelman, Pratyush Mishra, Derek Leung, and David Wagner. 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* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 1649–1658. https://doi.org/10.1145/2702123.2702164

[42] I. Psychoula, D. Singh, L. Chen, F. Chen, A. Holzinger, and H. Ning. 2018. Users' Privacy Concerns in IoT Based Applications. In *2018 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)* (Guangzhou, China). IEEE, New York, NY, USA, 1887–1894.

[43] Joseph Redmon and Ali Farhadi. 2018. YOLOv3: An Incremental Improvement. arXiv:1804.02767 [cs.CV]

[44] Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. 2015. A Design Space for Effective Privacy Notices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 1–17. https://www.usenix.org/conference/soups2015/proceedings/presentation/schaub

[45] Yunpeng Song, Yun Huang, Zhongmin Cai, and Jason I. Hong. 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* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376585

[46] Madiha Tabassum, Tomasz Kosiński, and Heather Richter Lipford. 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* (Santa Clara, CA, USA) *(SOUPS'19)*. USENIX Association, Berkeley, CA, USA, 435–450.

[47] Christian Tiefenau, Maximilian Häring, Eva Gerlitz, and Emanuel von Zezschwitz. 2019. Making Privacy Graspable: Can we Nudge Users to use Privacy Enhancing Techniques? arXiv:1911.07701 [cs.HC]

[48] T. Franklin Waddell, Joshua R. Auriemma, and S. Shyam Sundar. 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* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 5252–5256. https://doi.org/10.1145/2858036.2858149

[49] Mark Weiser. 1991. The Computer for the 21 st Century. *Scientific American* 265, 3 (1991), 94–105. http://www.jstor.org/stable/24938718

[50] M. Weiser, R. Gold, and J. S. Brown. 1999. The origins of ubiquitous computing research at PARC in the late 1980s. *IBM Systems Journal* 38, 4 (1999), 693–696.

[51] Gary White, Christian Cabrera, Andrei Palade, and Siobhán Clarke. 2019. Augmented Reality in IoT. In *Service-Oriented Computing – ICSOC 2018 Workshops*, Xiao Liu, Michael Mrissa, Liang Zhang, Djamal Benslimane, Aditya Ghose, Zhongjie Wang, Antonio Bucchiarone, Wei Zhang, Ying Zou, and Qi Yu (Eds.). Springer International Publishing, Cham, 149–160.

[52] EJ Williams. 1949. Experimental designs balanced for the estimation of residual effects of treatments. *Australian Journal of Chemistry* 2, 2 (1949), 149–168.

[53] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 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* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300428

[54] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 59 (Nov. 2019), 24 pages. https://doi.org/10.1145/3359161

[55] Eric Zeng and Franziska Roesner. 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)*. USENIX Association, Santa Clara, CA, 159–176. https://www.usenix.org/conference/usenixsecurity19/presentation/zeng

A STUDY PART I: SMART DEVICE STATE DETECTION USING *PRIVIEW*

A.1 Questionnaire

Intermediate Questions after every search task (i.e., after every visualisation) on a 5-point Likert scale:

- I felt comfortable using this visualisation.
- This visualisation was easy to learn.
- This visualisation was understandable.
- Finding the devices was fast.
- I would use this application frequently (if I had access to a thermal camera).

A.2 Interview Guide

- How was your experience?
- Would an application like this one be useful for you?
- Where would you use such an application? [e.g., Friend's house, Parent's House, Airbnb, Other]
- How frequently would you use this application? [E.g. every time you visit a place, first time visiting a place, when suspecting a place, . . .]
- Why would you use such an application? For which purpose?
- Which representation did you like most? Why?
- Would you like a combination of representations? Why?
- How much Information would you like to see? Might this be different per device? Further factors?
- Did the application assist you in finding the devices or did you find them yourself?
- Do you think the application would find devices you wouldn't?
- Does having access to such an application make you feel safer?
- Does it support you to protect your privacy?
- How did you feel using this application?
- How would you feel if someone around you is using this application (e.g., at your place)?
- What did you (not) like about the application?
- What suggestions or options could be added to the future?
- Do you have any further insights to share?

B STUDY PART II: *PRIVIEW* IN VR

B.1 Scenarios

S1: Train Station. Imagine you are on vacation and this is a train station that you have never been to before in a foreign, far away country. This place tends to be crowded, so many other people might be present as well.

S2: Museum. Imagine you are in this museum that you have never been to before. Other visitors might be present as well. There might be interactive exhibits that include some form of sensors.

S3: Rental apartment (bedroom). Imagine you are on vacation and this is an apartment that you rented via AirBnB or any other platform. You have never been here before. You rented the whole apartment for you and whomever is travelling with you. You do not know the host.

S4: A friend's place (living room). Imagine this is the place of a good friend of yours. You visit this place frequently and thus know it very well. This friend recently bought smart home devices.

S5: A shared/office kitchen. Imagine this is the kitchen in your office. You spent valuable coffee or tea time here during long work days. You know all people that come here as they are your colleagues. This includes your boss.

S6: Way to work (a public place and/or road). Imagine this is your daily way to work, so you know this place very well. It is a public road, so other (foreign) people, cars, bikes might be present as well.

B.2 Questionnaire

B.2.1 *Intermediate Questions.*

Intermediate Questions after every scene:

- Overall, I felt comfortable using this application. [5-point Likert scale]
- I would use this application frequently in this scenario (if I had access to AR glasses). [5-point Likert scale]
- Which visualisation did you like best in this scenario? Please rank all visualisations (use drag and drop) according to your preference in this scene, from most preferred (1) to least preferred (5).

B.2.2 *Final Questions.*

At the end of the session, for every visualisation (we provided screenshots for recap):

- This visualisation was easy to learn. [5-point Likert scale]
- This visualisation was understandable. [5-point Likert scale]

B.3 Interview Guide

- How was your experience?
- Would an application like this one be useful for you?
- Where would you use such an application? [e.g., Friend's house, Parent's House, Airbnb, Other]
- For which purpose would you use such an application?
- How frequently would you use this application? [E.g. every time you visit a place, first time visiting a place, when suspecting a place, . . .]
- When would you like to see the visualisations? e.g., on demand, permanently (like now), only on change, only when you are close to a source of tracking, . . .
- How much Information would you like to see? Might this be different per device? Might this be different depending on the location? Further factors?
- Which representation did you like most overall? If there is an overall, otherwise maybe specifically? Why?
- Would you like to rather have a combination of visualisations?
- What else could you imagine?
- Does having access to such an application make you feel safer?
- Does it support you to protect your privacy?
- How did you feel using this application?
- How would you feel if someone around you is using this application (e.g., at your place) ?
- What did you (not) like about the application?

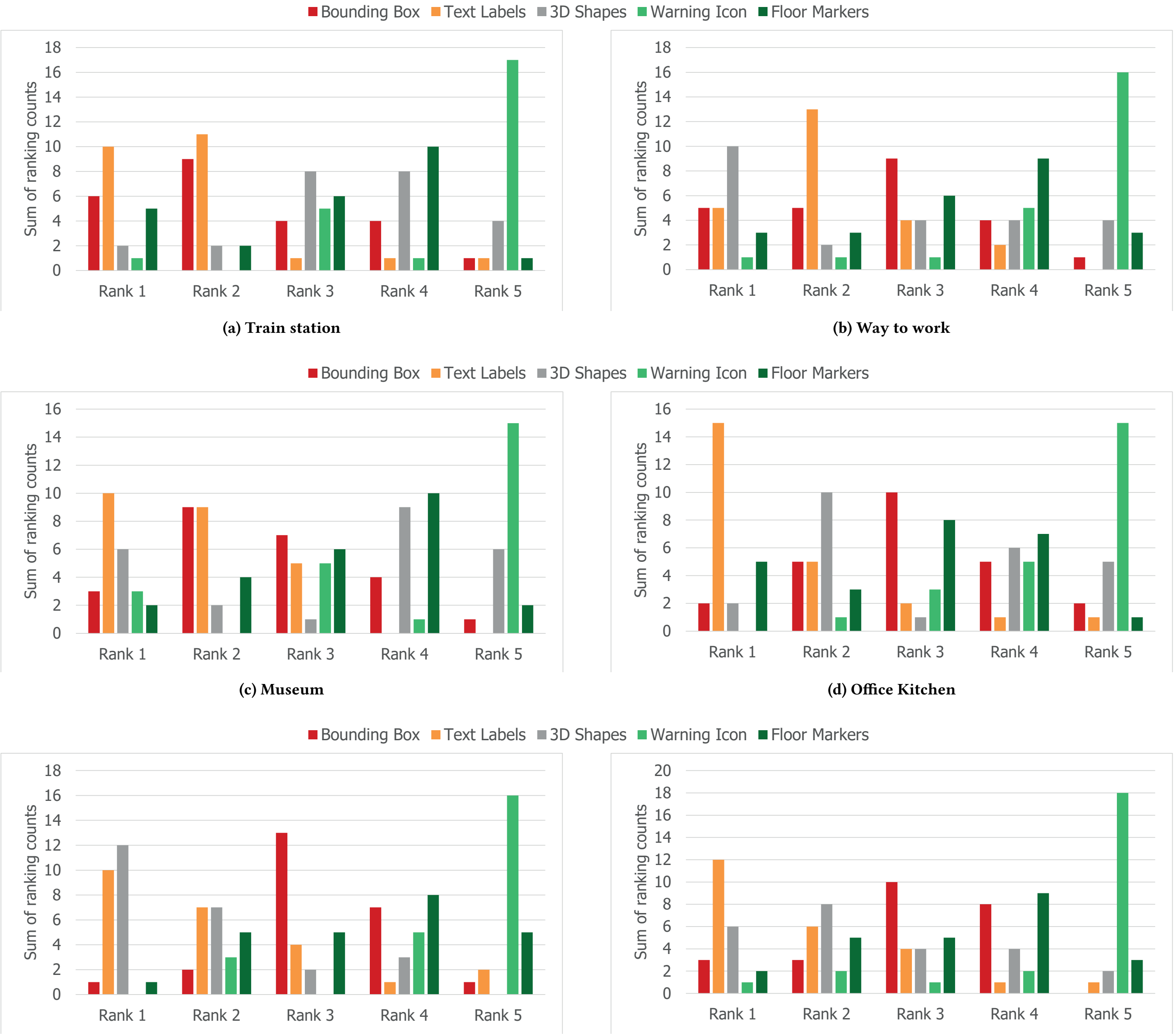
- What suggestions or options could be added to the future?
- Comparing the mobile application and the VR / glasses version, which one would you prefer (think about integrated prototypes)? Why?
- Any further insights to share?

C CODE BOOK

Final coding tree for the thematic analysis:

- Found Devices – Baseline
- Found Devices – Mobile Application
- General Feedback
  - Mobile Application
    - Positive
    - Negative
    - Suggestion for Improvement
  - Head-Mounted Display
    - Positive
    - Negative
    - Suggestion for Improvement
- Usefulness
  - Frequency (of visited place)
    - Once
    - Everytime
  - Overtime (e.g., learnability or redundancy)
    - Floor Markers
      - Understood
      - Not understood
    - Bounding Boxes
      - Understood
      - Not understood
    - Warning Icon
      - Understood
      - Not understood
    - Text Labels
      - Understood
      - Not understood
    - 3D Shapes
      - Understood
      - Not understood
- Usage
  - Potential Use Cases
    - Finding Devices
    - Awareness
  - Location
    - Familiarity
    - Space (i.e., private vs public)
    - Trusted
  - Context
    - Redundancy
- Privacy
  - Self
  - Other
    - Comfort
    - Acceptance
    - Social Trust
- Preference
  - Interaction Modality
    - Activation Methods
      - Notification for Updates
      - Always on
      - Button
      - Nested
  - Form Factor
    - Why
  - Visualisation
    - Why
      - Distraction
      - Quick Overview
      - Easy to Understand
      - Information Level (level of detail)
More information | Less information
    - Suggestion for Improvement
    - Context
    - Location

D *PRIVIEW* RANKING OF VISUALISATIONS PER SCENARIO



(a) Train station

(b) Way to work

(c) Museum

(d) Office Kitchen

(e) Rental apartment

(f) A friend's place

Figure 9: Study Part II (using *PriView* in an HMD in various scenes): Detailed ranking of visualisations per scene, i.e. sum of count of rank positions per scene.