Do You Need to Touch? Exploring Correlations between Personal Attributes and Preferences for Tangible Privacy Mechanisms

SARAH DELGADO RODRIGUEZ, University of the Bundeswehr Munich, Germany
PRIYASHA CHATTERJEE, Ruhr University Bochum, Germany
ANH DAO PHUONG, LMU Munich, Germany
FLORIAN ALT, University of the Bundeswehr Munich, Germany
KAROLA MARKY, Ruhr University Bochum, Germany

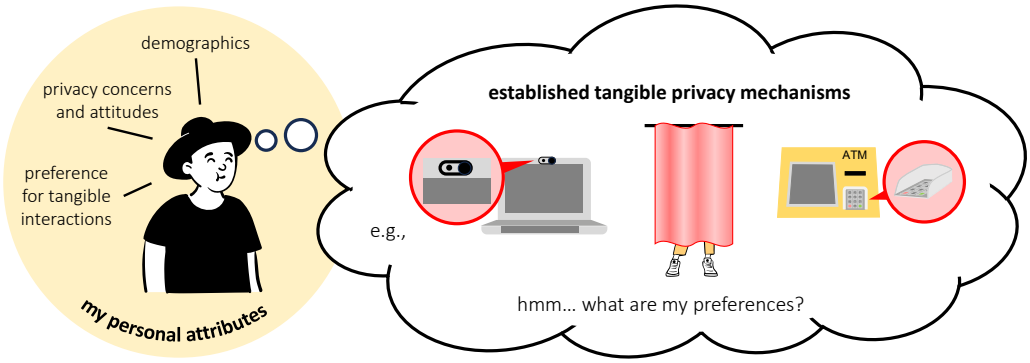


Fig. 1. We conducted an online survey ($N = 444$) to explore which personal attributes (demographics, privacy concerns, attitude, preference for tangible interaction aka. "need for touch") correlate with participants' perceptions of properties of established tangible privacy mechanisms. Besides general preferences, we investigated participants' perceptions of ATM pin pad privacy shields, webcam covers, headphones, sunglasses, remote controls, voting booths, floor distance marks, and dressing room curtains. This figure uses characters from Open Peeps by Pablo Standley.

This paper explores how personal attributes, such as age, gender, technological expertise, or "need for touch", correlate with people's preferences for properties of tangible privacy protection mechanisms, for example, physically covering a camera. For this, we conducted an online survey ($N = 444$) where we captured participants' preferences of eight established tangible privacy mechanisms well-known in daily life, their perceptions of effective privacy protection, and personal attributes. We found that the attributes that correlated most strongly with participants' perceptions of the established tangible privacy mechanisms were their "need for touch" and previous experiences with the mechanisms. We use our findings to identify desirable characteristics of tangible mechanisms to better inform future tangible, digital, and mixed privacy protections. We also show which individuals benefit most from tangibles, ultimately motivating a more individual and effective approach to privacy protection in the future.

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

Manuscript submitted to ACM

Additional Key Words and Phrases: internet of things, privacy, tangible, tangible privacy

ACM Reference Format:
Sarah Delgado Rodriguez, Priyasha Chatterjee, Anh Dao Phuong, Florian Alt, and Karola Marky. 2024. Do You Need to Touch? Exploring Correlations between Personal Attributes and Preferences for Tangible Privacy Mechanisms. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24), May 11–16, 2024, Honolulu, HI, USA.* ACM, New York, NY, USA, 35 pages. https://doi.org/10.1145/3613904.3642863

1 INTRODUCTION

In the current era of ubiquitous computing, where many sensor-enhanced devices are becoming part of our daily lives and our environment [71], protecting the privacy of individuals becomes increasingly challenging. For instance, the smartphone of the person standing behind one in the queue could be recording a private conversation with a pharmacist or a neighbor's security camera may record one's front door access code. There are several options to implement privacy protection in such ubicomp environments. *Purely digital privacy mechanisms* refer to software solutions (for example, a smartphone or augmented reality app) that make users aware of privacy-invasive devices in their surroundings [57, 65, 77] or provide control over collected personal data [13, 24].

In this paper, we focus on an alternative approach, that is, *purely tangible privacy mechanisms*. These make use of physical objects, offering privacy protection against sensor-enhanced smart devices [1, 53] (for example, by physically covering a camera [74]). An advantage, as compared to purely digital solutions, is that tangible privacy protection mechanisms directly affect people's awareness as well as the perception of privacy risks [16, 53] and are generally easy-to-understand or verify [1, 16]. This is rooted in the physical nature of the mechanisms. For instance, users can easily understand that it is impossible for a camera to capture pictures through a cover.

Yet, existing study results hint at tangible solutions maybe not being ideal for every user [16, 51, 74]. As is well-known from user interface design [11], one-fits-all solutions rarely lead to good user experiences. Therefore, developing privacy mechanisms inside the digital-tangible spectrum that are specifically tailored to the needs and preferences of varying user groups is desirable. Research on, for example, smartphone privacy settings showed personal attributes, such as age, gender, or technical affinity, to frequently influence users' privacy-related opinions and behaviors [2, 43].

We currently lack an in-depth understanding of how personal attributes shape a person's opinion about tangible mechanisms protecting their privacy from nearby sensor-enhanced devices. Yet this knowledge is valuable to develop suitable mechanisms targeted at specific user groups. Thus, our first research question is:

RQ1 – Personal Attributes: Which personal attributes (e.g., age, gender, technological expertise, perception of privacy risks, need for touch) correlate with peoples' general perception of purely tangible privacy mechanisms?

To inform the design of future privacy mechanisms in the digital-tangible spectrum (i.e., tangible, digital, or hybrid mechanisms), it is crucial to understand which properties of tangible mechanisms are particularly important to users. For example, users might assign importance to having a physical object that reminds them that their privacy may be at risk [37] while having little desire to touch a tangible mechanism. Hence, we assess the importance of the following properties of tangible privacy mechanisms: their ability to be touched, their ability to raise awareness, and the possibility to verify and understand their protective effect. Understanding users' preferences for these different properties of tangible privacy mechanisms enables future researchers and developers to make informed design decisions, particularly concerning hybrid mechanisms where some features may be tangible and others purely digital. This motivates our second research question:

RQ2 – Perception of Tangible Privacy Mechanisms: How do users perceive the different properties (tangible interactions, awareness, verification, physicality) of purely tangible privacy mechanisms in general? What differences and similarities in users' perceptions of the presented purely tangible privacy mechanisms can be observed?

Finally, the question arises as to how diverse target groups perceive the different properties of tangible mechanisms. This knowledge can enable one-fits-all solutions to be replaced by actual target-group-oriented designs, providing a better user experience. We, thus, connect our findings on personal factors and people's perception of the different properties of tangible privacy mechanisms to answer the third research question:

RQ3 – Personal Attributes' and Properties of Tangible Privacy Mechanisms: Which personal attributes correlate with peoples' perceptions of specific properties of purely tangible privacy mechanisms?

To investigate purely tangible privacy mechanisms in more depth, our descriptive research [17, 66] focuses on already well-established tangible privacy mechanisms – such as webcam covers and ATM pin pad privacy shields – assuming that a large part of the general population has experienced the use of these mechanisms.

First, we collected eight examples of established tangible privacy mechanisms based on feedback from risk-aware participants (e.g., voting booths, pin pad privacy shields, headphones, and webcam covers). We then conducted an online survey ($N = 444$), exploring peoples' perceptions of those mechanisms and capturing personal attributes that describe our participants, such as their experience, affinity for technology, or their personal "need for touch".

We found that the personal attributes most strongly related to participants' overall perception of tangible privacy mechanisms are 1) previous privacy-related usage of such mechanisms and 2) their personal preferences for touching objects. Participants saw the main value in tangible privacy mechanisms' ability to raise awareness and verify that their data is protected. Moreover, we found that more technology-affine participants appreciate having tangible interactions with privacy mechanisms more. Our findings further show that a stronger trust in technology among participants corresponds to a greater appreciation of the ease of verifying the functionality of tangible privacy mechanisms, as well as their impact on awareness. Surprisingly and in contrast to related work [16, 53], our results also indicate that older participants might be less likely to prefer tangible mechanisms over digital alternatives.

Our research highlights how personal attributes shape people's perceptions of well-established tangible privacy mechanisms. Hence, our work informs about the preferences of varying user groups, leading to a better understanding of for whom future tangible, digital, or mixed privacy mechanisms should be developed. As concise takeaway messages, we derive design recommendations for future privacy mechanisms targeting both the general population and more specific subgroups (e.g., technology- and security-savvy or older persons), as well as open questions for future research.

Contribution Statement. We contribute to research on *user-centered design of privacy protection mechanisms around sensor-enhanced devices* by 1) conducting an online survey ($N = 444$) to identify the personal attributes influencing perceptions of users of everyday *tangible privacy mechanisms*, and 2) providing design recommendations for preferred properties of future tangible, digital, or mixed privacy mechanisms.

2 BACKGROUND AND RELATED WORK

Our work draws from related literature on tangible interfaces and interactions, privacy in the Internet of Things (IoT), tangible privacy, as well as privacy profiling.

2.1 Tangible Interfaces & Interactions

Tangible user interfaces (TUIs) are physical objects used to interact with digital information [62]. They can be distinguished in two dimensions: (1) the metaphor they support and (2) the embodiment of tangible input and digital output [26]. Moreover, they are particularly easy to use since they leverage human's natural ability *"to act in physical space and interact with physical objects"* [62, p. 338]. Such natural, tangible interactions could be touching, squeezing, pushing, tilting, holding, tapping, shaking, swinging, thrusting, stroking, or moving objects [8, 31, 47, 58, 61, 70]. Most related work on TUIs presents the development of novel devices for specific application scenarios, such as support for learning and understanding [40, 41], digital augmentation of existing environments [15, 59], or offering more intuitive interaction modalities [19, 30, 51]. TUIs are frequently evaluated by potential end users testing them in the lab [30, 47, 59] or field [4, 69, 74]. However, we do not intend to experimentally evaluate a novel mechanism. Instead, our descriptive research investigates the existing opinions of users in connection with mechanisms already known to them [17, 66]. Hence, we recruited a large sample by conducting an online survey.

2.2 Privacy in the Internet of Things

IoT devices can invade the privacy of their users [45, 80] and are also perceived as such [7, 79]. However, such sensor-enhanced devices can also collect data on bystanders, such as visitors or incidental users [48, 73]. Researchers found that while bystanders want to be aware of IoT devices in their environment, they frequently struggle with interpreting devices' current states and capabilities [1, 48, 77]. Related work suggests approaches to overcome limitations in awareness and control of both, bystanders and users of IoT technology.

Awareness. Privacy labels on the packaging of IoT devices could enhance people's awareness of possible risks before purchasing them [22, 35]. Device locators, such as LEDs, QR codes, or augmented reality-based visualizations can increase awareness, while also providing additional information on the devices [57, 65, 77].

Control. Most related work on privacy controls for IoT contexts suggests software-based systems [24, 32, 60, 78]. While these allow for fine-grained control, they frequently suffer from usability issues due to their complexity and dependence on specific hardware or software [9, 60]. Furthermore, they can be difficult to verify for users. Hence, researchers have suggested *tangible privacy mechanisms*, enabling intuitive, direct, and uncomplex control [1, 16, 52].

2.3 Tangible Privacy

Tangible privacy mechanisms range from simple, purely tangible solutions (e.g., pin pad privacy shields or webcam covers [1]) to digitally enhanced approaches (e.g., mechanisms that disable sensors in a particular context or automatized webcam covers [16, 74]). Suggested research prototypes include, for example, an armband vibrating if the user is being localized [51], a hat to cover and mute a smart speaker's microphone [68], a key-shaped privacy control for smart homes [16], automatic camera covers [18, 74], a tangible smart home privacy dashboard [74] or a smart calendar only showing sensitive data in a private environment [36].

Prior research also addressed tangible privacy from a conceptual point of view. Ahmad et al. [1] defined tangible privacy *"as those privacy control and feedback mechanisms that are 'tangible', i.e., manipulated or perceived by touch, and of 'high assurance', i.e., they provide clear confidence and certainty of privacy to observers"* [1, p. 18]. Hence, such mechanisms are not only related to *tangible interactions* but also *unambiguously display information.* Moreover, Mehta et al. suggest privacy management through *"tangible and embodied style interactions"* [53, p. 7]. The authors also argue that tangible

mechanisms can *raise awareness* and *provide seamless control* by embedding them into users' everyday environments and routines. Interacting with such mechanisms can be particularly direct because they draw on *well-known metaphors for physical manipulation* (e.g., push, pull, block) [53]. Delgado Rodriguez et al. discussed that *"tangible mechanisms materialize the abstract concept 'privacy' by making it physically graspable and directly manipulable"* [16, p. 3].

In summary, tangible privacy mechanisms are different from purely digital approaches as they are *physical objects* [14, 53]. They can be manipulated or perceived through *tangible interaction* [1, 14, 53] and *increase awareness* [16, 53] of privacy risks. They *communicate their state unambiguously, intuitively, and verifiably* [1, 53].

2.4 Personal Attributes and Privacy Perceptions

Individuals have different concerns, needs, and preferences regarding protecting their privacy. Related work proposes several approaches to clustering and profiling users based on self-reported privacy attitudes [20, 44, 64, 75, 76] or actual privacy behavior [2, 10, 43]. Westin's three categories (i.e., unconcerned, fundamentalists, and pragmatists) are frequently reported as the first approach to privacy profiling [39]. However, more recent work found that these categories might be unrelated to peoples' corresponding behavior intentions [10, 76]. To overcome this limitation, Dupree et al. [20] suggested five privacy personas (i.e., fundamentalists, lazy experts, technicians, amateurs, and marginally concerned) based on the self-reported behavior of 32 users. These personas are distinguished by their different levels of knowledge and motivation. Other researchers focused on specific subdomains of privacy behavior, such as smartphone privacy settings [28], app permissions [2, 42, 43], location sharing [10], or social media privacy behavior [75].

In summary, related work established a wide variety of personal attributes influencing people's security-related perceptions and behaviors. In particular, demographical factors (i.e., gender, age, expertise in technology, and trust in technology), as well as privacy concerns and attitudes were shown to be influential.

2.5 Research Gap

In recent years, extensive research has been carried out to find possible solutions for supporting people in protecting their privacy from sensor-enhanced devices in their surroundings. Proposed mechanisms span a continuum ranging from *purely digital* (i.e., only software, e.g., [13] or [24]) to *purely tangible privacy mechanisms* (i.e., only hardware, e.g., privacy shields or webcam covers). Related work comparing users' opinions on purely digital and tangible mechanisms found that users are strongly divided in their preferences [16]. However, to develop a user-centered design, one must first understand who a system is being developed for [55]. Therefore, the question arises: Who favors tangible mechanisms, and who does not? And, more specifically: Which user groups like each of the various properties of tangible mechanisms? *This paper* addresses these questions by analyzing the relationship between personal attributes and people's perceptions of purely tangible privacy mechanisms.

3 RESEARCH APPROACH

The objective of this work is to *identify correlations between individuals' personal attributes and their preferences regarding different properties of tangible privacy mechanisms*. In this section, we discuss how we derived the relevant personal attributes and properties of tangible privacy mechanisms.

3.1 Investigated Personal Attributes

We derived personal attributes that could influence the perception of tangible privacy mechanisms from prior work.

3.1.1 *Demographics.*

Gender and Age: Demographics, such as age [5, 53, 82] or gender [5, 28], affect privacy behavior or concerns.

Expertise in Technology: Both general affinity for technology [5, 53] and specific expertise in interacting with potentially privacy-invasive devices [1, 20] might influence a person's corresponding perception and behavior.

Trust in Technology: The concepts of 'privacy' and 'trust' are strongly intertwined since a user has to trust any technology to safeguard potentially sensitive data [33, 38]. Thus, a person's trust in technology in general, but also in specific devices could affect their perceptions of privacy mechanisms.

3.1.2 *Privacy Concerns and Attitudes.*

Security Attitudes / Behavior Intentions: Users' privacy and security attitudes and intentions have been previously used to profile end-user behaviors by creating 'Privacy Personas' [20] and can be considered an influencing factor in regard to tangible privacy mechanisms.

Privacy Concerns: Even though research has shown privacy concerns do not necessarily translate to correspondingly privacy-protecting behavior (i.e., *privacy paradox* [3]), such concerns still affect user's perceptions and usage of privacy mechanisms [7]. Prior work also found privacy concerns depend on the type of smart device (e.g., video camera vs. smart speaker) [7, 16, 79] and the role of the individual (e.g., owner of the device vs. bystander) [29, 46].

3.1.3 Perception of Tangible Interaction. User perceptions of tangible privacy mechanisms are also likely to be affected by an individual's personal preferences for tangible interactions (i.e., physical manipulation/touch), thus "need for touch" is also an interesting personal attribute in the context of this paper.

3.2 Investigated Properties of Tangible Privacy Mechanisms

Based on related work, we derived properties of tangible privacy for which we asses users' perceptions in this work.

Involve Tangible Interaction: Tangible privacy mechanisms can be manipulated or perceived through tangible interaction, i.e., touch [1, 14, 53].

Affect Awareness: A tangible privacy mechanism can increase awareness on possible privacy intrusions [16, 53].

Unambiguous / Intuitively Verifiable: Tangible privacy mechanisms can distinctly communicate their state and are intuitively verifiable [1, 53].

Physicalization: Tangible privacy mechanisms, due to their tangibility, are physical objects and, thus, are physicalized representations of the abstract concept of "privacy" [14, 53].

4 METHODOLOGY

To gather feedback on established tangible privacy mechanisms, we first collected well-known examples of such mechanisms from risk-aware researchers. Then, we developed an online questionnaire to gain insights into user perceptions of these mechanisms and how they vary based on personal attributes. We used an online questionnaire to reach a large pool of diverse participants. This is necessary to derive ecologically valid findings on how people's personal attributes correlate with their perceptions of privacy mechanisms. Therefore, we specifically investigate established everyday privacy mechanisms that many users can be assumed to have had experiences with. Moreover, prior works successfully conducted online surveys on participants' perceptions of tangible privacy [16, 54].

4.1 Collecting Established Tangible Privacy Mechanisms

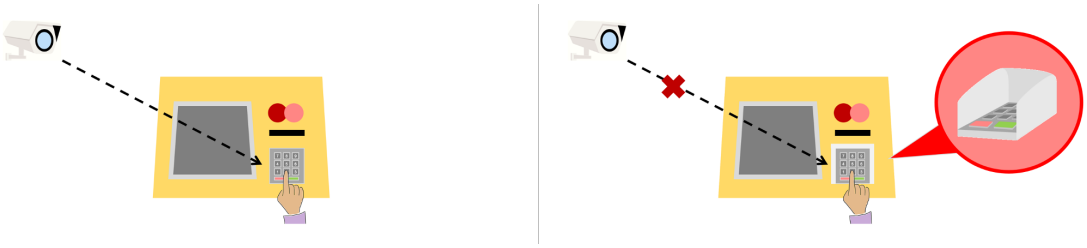
We conducted a group discussion to collect examples of well-known established tangible privacy mechanisms, as related work does not provide a broader list of such mechanisms. Hence, we recruited three persons who were aware of the privacy risks associated with sensor-enhanced devices using personal messages. We expected these participants to be particularly attentive to privacy mechanisms in their everyday environment, as they were researchers in the field of usable security and privacy (2 male, and 1 female, aged 27–29, 2 PhD students, and 1 master student). Note that we did not aim to collect a comprehensive list of established tangible privacy mechanisms but exemplary mechanisms that come to mind easily from their personal experience. In the group discussion, participants were first presented with a broad definition of tangible privacy (cf. Appendix A) and then asked to name tangible privacy mechanisms well-established in everyday life in their opinion. They identified 19 examples of such mechanisms.

Two experimenters met afterward to identify and discuss common themes observed during the group discussion. In particular, we found that the mentioned mechanisms (1) protect *different kinds of data* (i.e., *visual* and *auditory data*), as well as the *physical identity and state of the user*. Consequently, the mentioned mechanisms protect their users, specifically from cameras and microphones, which are particularly often integrated with ubiquitous computing devices [37]. Moreover, the mechanisms are (2) situated in different locations that relate to both the potential privacy-invasive device and the user (i.e., *on the potentially privacy-invasive device*, *on the user*, or *distant from both*). This distinction is similar to the *embodiment* dimension of Fishkin's taxonomy of tangible interfaces [26], which expresses different spatial relationships between tangible user input and digital output. However, we additionally considered the location of the user in the spatial setting. Applying both distinction criteria, we could cluster the proposed mechanisms into eight different groups (cf. Appendix B). Then, we selected one mechanism from each of these groups to continue our study with. This ensured that the participants in our online survey were not overwhelmed by an excessive number of mechanisms while still reflecting a broad variety of well-known tangible privacy mechanisms. This resulted in the selection of the following eight tangible privacy mechanisms:

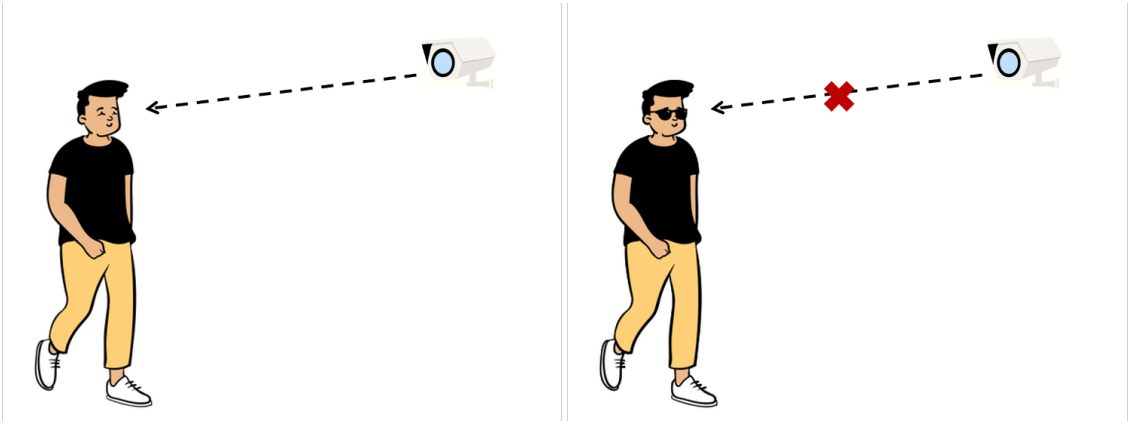
1. **Voting booth** obscures your vote from being recorded by a camera. [visual data | distant]
2. **Floor distance marking** limits eavesdropping by providing guidelines for maintaining safe distances (e.g. a microphone at a certain distance is not able to record your private conversation with your pharmacist). [auditory data | distant]
3. **Dressing room curtain** creates a barrier between you and nearby cameras. [identity | distant]
4. **Pin pad privacy shield** covers the PIN pad to prevent your PIN from getting recorded by cameras. [visual data | on device]
5. **Webcam cover** creates a barrier between you and your webcam. [identity | on device]
6. **Headphones** prevent eavesdropping by nearby microphones while listening to audio content like voice messages. [auditory data | on user]
7. **Sunglasses** prevent your face from being identifiably recorded by nearby cameras. [identity | on user]
8. **Remote control for volume** can protect against eavesdropping by nearby microphones. E.g., turning up the volume on a smart TV to make sure that its microphone is unable to record your conversation. [auditory data | on device]

Next, we created clickable illustrations for each of the eight mechanisms to effectively visualize their functionality[1]. We aimed to convey to any participant, regardless of prior knowledge, how each mechanism can be used for privacy

[1]Illustrations were created using characters from Open Peeps by Pablo Standley. https://blush.design/collections/open-peeps/open-peeps, last accessed in September 2023



(a) A pin pad being recorded by a camera without (left) and with (right) a privacy shield.



(b) A person being recorded by a camera without (left) and with (right) sunglasses on.

Fig. 2. Our illustrations[1] show how each exemplary tangible privacy mechanism can protect a person's privacy from surrounding sensor-enhanced devices. The user can switch between two images (i.e., left and right images in (a) and (b)) by clicking on a button.

protection around smart devices. Each visualization consisted of two illustrations: one showing a scenario without the tangible privacy mechanism and the second one with the mechanism. Users can switch between both illustrations by clicking on a button (see Figure 2).

4.2 Questionnaire Design

To survey a large and diverse sample of the general population, we developed an online questionnaire. We included items on participants' perception of established tangible privacy mechanisms and their personal attributes (see Table 1 for an overview). Appendix C.1 lists all items of our online questionnaire.

4.2.1 Consent & Introduction. Participants were first asked to provide their informed consent and confirm they were over 18 years old. We then included definitions of "privacy" and "privacy in IoT".

4.2.2 Demographics. We asked our participants about their age, gender, and education level. In a multiple-choice question, participants were asked to select all IoT devices they regularly use. We provided a list of 16 IoT devices to select from, derived from an earlier (2021) survey on popular smart devices in the US by Reviews.org[2]. Using the Affinity for Technology (ATI) scale [27], we measured participants' technological affinity. Moreover, we assessed our

[2]https://www.reviews.org/home-security/most-popular-smart-home-device-statistics/#:~:text=The%20majority%20of%20Americans%20own,Amazon%20Echo%20and%20Google%20Nest, last accessed in September 2023

Table 1. Overview of our questionnaire design, showing which constructs were included for each investigated factor. (*) marks author-generated items.

investigated factor		**number of items**
demographics	age, gender (*)	4
experiences with technology	Internet of Things (IoT) device usage (*)	1
	Affinity for Technology Interaction (ATI) [27]	9
	Trust in Technology (TIT) [49]	7
security attitudes / behavior intentions	Security Attitudes (SA-6) [23]	6
	Security Behaviour Intention Scale (SeBIS) [21]	16
privacy concerns	Concern for Information Privacy (CFIP) [64]	15
	Internet Users' Information Privacy Concerns (IUIPC) [44]	10
preference for tangible interaction	Need For Touch (NFT) [56]	12
	general need for touch (NFT+) (*, derived from NFT)	5
tangible privacy	perception of 8 exemplary mechanisms (*)	7 for each
	tangible interaction (*, derived from NFT)	3
	effect on awareness (*)	2
	ease verification (*)	2
	physicalization (*)	3

participants' Trust in Technology (TIT), which is composed of the Faith in General Technology and Trusting Stance – General Technology subscales [49].

4.2.3 Privacy Concerns and Attitudes. We asked participants about their information privacy concerns using the Internet Users' Information Privacy Concerns (IUIPC) [44] and Concern for Information Privacy (CFIP) [64] scales. We measured participants' intentions to comply with common security advice using the Security Behavior Intention Scale (SeBIS) [21] and determined participants' security attitudes using the Security Attitudes (SA-6) scale [23].

4.2.4 Preference for Tangible Interaction. We used the Need For Touch (NFT) [56] scale to measure individuals' preferences for tangible interactions (i.e., touch / physical manipulation). While this scale is already well established, it focuses on interaction with products and their effect on purchasing decisions. Thus, we derived five additional items (i.e., NFT+). In particular, we adapted the NFT items by replacing "product" with "object" and "purchase" with "use" to improve comprehensibility where applicable.

4.2.5 Perception of Tangible Privacy. We collected participants' perceptions of tangible privacy mechanisms in two steps. First, we inquired about their perceptions of each of the eight exemplary privacy mechanisms. For this, we presented the mechanisms randomly to participants, allowing them to develop a general understanding of what tangible privacy mechanisms are. Second, we included items assessing their general perception of such mechanisms.

Mechanism-Related Items. Each established tangible privacy mechanism was first introduced through a short descriptive text and a clickable illustration (cf. Section 4.1). We made sure to re-iterate to our participants that they should *focus on the mechanisms' ability to protect their privacy from surrounding sensor-enhanced devices*, rather than from bystanders. We then asked about participants' perceptions of the mechanism, specifically assessing (a) their previous usage of the mechanism, (b) their reason for using it, (c) the importance of owning the mechanism, (d) its purposefulness as a privacy mechanism, (e) participants' corresponding behavior intention if the mechanism is not available and (f) whether they would prefer a non-materialized digital alternative[3]. These questions reflect people's previous experiences with the

[3]To ensure a common understanding of such purely digital alternatives, we specifically included a brief description in this statement: "I would prefer using a purely digital alternative instead of the presented privacy mechanisms to protect my privacy from other technical devices (e.g. automatically blurring my body/data on camera images, jamming of microphones)."

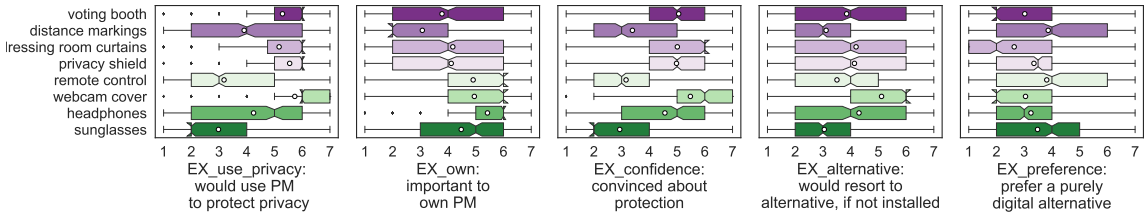


Fig. 3. Participants' feedback on each tangible privacy mechanism (PM). Participants could select from a 7-point Likert scale ranging from strongly disagree (1) to strongly agree (7). Medians are marked by indents and means by white dots.

mechanisms, their trust in and concerns towards them, their behavior intentions, and their preference compared to digital alternatives, as related work highlights the importance of these aspects regarding the perception of privacy mechanisms [1, 16, 20, 53].

General Items. To capture users' general perceptions, we develop corresponding questionnaire items. We gathered feedback on the previously mentioned properties of tangible privacy mechanisms, i.e., they (a) involve tangible interaction (i.e., touch), (b) increase awareness of privacy risks, (c) are intuitively verifiable, and (d) are physical objects (cf. Section 3.2).

4.3 Pilot Study

We pilot-tested our questionnaire first internally ($N = 5$) and then externally with 10 participants recruited through Prolific[4]. Participants were asked to provide details on any ambiguous or unclear statements and tasks (incl. the clickable illustrations). Therefore, we added a text-response box at the end of each page of the questionnaire. We planned for the pilot test to take up to 45 minutes, but Prolific participants only needed 24.8 to fill out the questionnaire and additional feedback items ($std = 8.33$). We compensated the participants recruited through Prolific with 9.45 pounds. The feedback gathered through both pilot studies was used to rephrase multiple descriptions and author-generated items. No ambiguities in regard to the clickable illustrations were reported. Furthermore, we found that prolific pilot participants have used $mean = 7.0$ of the 8 mechanisms before ($std = 1.15$,range: $5 - 8$), confirming that the selected eight tangible privacy mechanisms were indeed well-known to our pilot sample.

4.4 Ethical Considerations

Our study was approved by the institution's IRB board. The online questionnaire started with detailed information on which data would be collected, the purpose of the data collection, how it would be stored, and that participation was voluntary and could be aborted at any time. Participants were then asked to consent to the data collection and confirm that they were at least 18 years old. To complete anonymization, we deleted participants' Prolific IDs after finishing the compensation procedure. Participants were compensated an amount of 4.5 pounds (average duration of 24.97 minutes).

[4] https://www.prolific.co/, last accessed in September 2023

5 RESULTS

5.1 Recruitment & Participants

We recruited 501 participants for our study over the online platform Prolific. We used Prolific's option to recruit a sample that is representative of the general US population in terms of gender, age, and ethnicity. Hence, our sample was limited to persons living in the US. Participants took on average 24.97 minutes to answer our questionnaire ($std = 10.31$). For our analysis, we excluded 57 participants who 1) filled in the questionnaire in less than half of the mean duration or 2) failed at least one attention check, leaving us with 444 participants. The final sample included 230 participants identifying as female and 206 as male. Participants' mean age was 46.47 ($std = 16.14$, range $18 - 85$) and most finished a bachelor's degree ($N = 184$), high school ($N = 97$), or a master's degree ($N = 60$) (see Appendix D.1 for more details).

5.2 Perception of Exemplary Tangible Privacy Mechanisms

To summarize, we presented eight established tangible privacy mechanisms to our participants through clickable illustrations.

5.2.1 Overall Perception. Overall, our participants slightly agreed that if they were to use the presented mechanisms, it would be to protect their privacy ($median_{EX\_use\_privacy} = 5.0$, see Appendix D.2). It was also somewhat important to participants to own the mechanisms ($median_{EX\_own} = 5.0$). Moreover, participants were rather convinced that the mechanisms would protect their privacy from other technical devices ($median_{EX\_confidence} = 5.0$). They did neither agree nor disagree with the statement, that they would resort to a similar alternative if the mechanism was not installed by default ($median_{EX\_alternative} = 4.0$). Finally, participants slightly disagreed with preferring a purely digital alternative to the presented tangible mechanisms ($median_{EX\_preference} = 3.0$).

5.2.2 Comparison of Different Mechanisms. We compared participants' answers to our questions for each presented established tangible privacy mechanism. Figure 3 provides a detailed overview of the corresponding results. Regarding *EX_use_privacy* (i.e., if participants would use the mechanism to protect their privacy), we found that participants disagreed with this statement for *sunglasses* ($median = 2$) and *remote controls* ($median = 3$), rated *distance marking* ($median = 4$) neutrally and agreed for *headphones* ($median = 5.0$), *dressing room curtains*, *voting booths*, pin pad *privacy shields*, and *webcam covers* ($medians = 6.0$). Participants also disagreed with feeling that it is important to own *distance markings* ($median = 2.0$) while rating this statement neutrally for *voting booths*, *privacy shields*, and *dressing room curtains* ($median = 4.0$). They agreed for *sunglasses* ($median = 5.0$), *remote controls*, *webcam covers*, and *headphones* ($median = 6.0$). Regarding being convinced that the mechanism protects their privacy, participants disagreed for *sunglasses* ($median = 2.0$), *remote controls* and *distance markings* ($median = 3.0$) and agreed for *headphones*, pin pad *privacy shields*, *voting booths* ($median = 5.0$), *dressing room curtains*, and *webcam covers* ($median = 6.0$). We inquired if participants would resort to similar alternatives if the corresponding mechanism is not installed by default. Participants disagreed with this statement for *sunglasses* and *distance markings* ($median = 3.0$) while agreeing for *webcam covers* ($median = 6.0$) and being neutral for *all other mechanisms* ($median = 4.0$). Furthermore, participants disagreed with preferring a purely digital alternative for protecting their privacy from surrounding technical devices for *dressing room curtains*, *voting booths*, *webcam covers* ($median = 2.0$), *headphones* ($median = 3.0$) and *privacy shields* ($median = 3.5$). They rated this statement neutrally for *sunglasses*, *remote controls*, and *distance markings* ($median = 4.0$).

5.2.3 Similarities and Differences Between Mechanisms. We then analyzed which mechanisms were perceived similarly by participants. For this, we calculated pairwise Euclidean distances d between all mechanisms' mean response

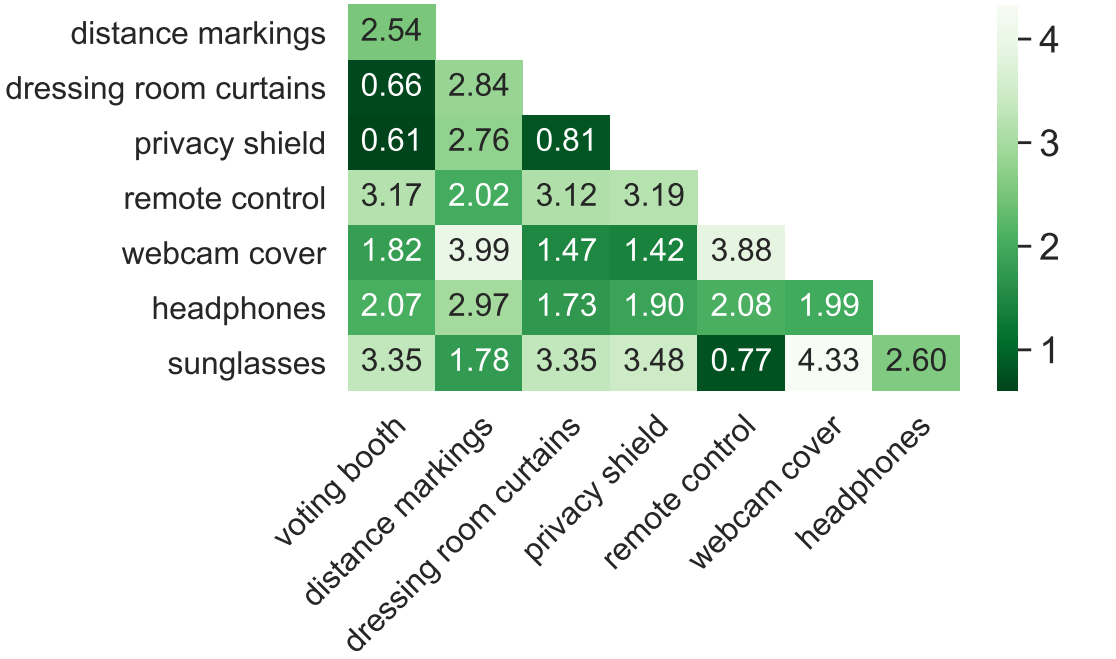


Fig. 4. Euclidean distances between the mean response vectors for each presented tangible privacy mechanism. Please find the same results as a table in Appendix D.5.

Table 2. Participants' answers to tangible privacy items, using a 7-point scale ranging from strongly disagree (1) to strongly agree (7). PM denominates tangible privacy mechanisms and the answers for item TP09_08 were reverse-coded.

factor	item		mean	std	median
tangible interaction	TP-I_fun	Touching PMs can be fun.	3.32	1.64	4.0
	TP-I_trust	I place more trust in PMs that can be touched.	4.17	1.81	4.0
	TP-I_confidence	I feel more confident using a PM after touching it.	3.82	1.75	4.0
effect on awareness	TP-A_aware	Having the PM nearby makes me aware that my privacy could be invaded.	5.19	1.50	6.0
	TP-A_consider	Having the PM nearby makes me consider to use it to protect my privacy.	5.42	1.35	6.0
ease of verification	TP-V_understand	It is easy to understand how the PMs protect my privacy from other technical devices.	5.43	1.38	6.0
	TP-V_verify	I can easily verify by myself if the PMs protect my privacy from other technical devices.	4.69	1.62	5.0
physicalization	TP-P_preference	I would prefer using a purely digital alternative instead of the PMs to protect my privacy from other technical devices (e.g. automatically blurring my body/data on camera images, jamming of microphones). (reverse coded)	4.67	1.60	5.0
	TP-P_performance	I think that the PMs protect my privacy better from other technical devices than purely digital alternatives.	4.86	1.46	5.0
	TP-P_trust	I place more trust in the PMs compared to purely digital alternatives.	5.01	1.48	5.0

vectors (i.e., a 5-dimensional vector for each mechanism, since there were 5 corresponding items. Figure 4 shows the corresponding results.

Smallest Euclidean Distances ($d < 1$). *Dressing room curtains*, *privacy shield*, and *voting booth* had a very small distance between each other ($0.61 <= d <= 0.81$), indicating similar perceptions among participants toward these mechanisms. *Sunglasses* and *remote controls* were also perceived very similarly ($d = 0.77$).

Table 3. Results of the principal component analysis conducted on tangible privacy items. We applied a promax rotation to the component loadings matrix. We highlighted the highest loadings in bold, which also indicates their component assignment. TP-P_preference was reverse-coded.

	awareness\ verification	**tangible interaction**	**physicalization**
TP-I_fun	-0.050	**0.894**	-0.220
TP-I_trust	-0.004	**0.769**	0.275
TP-I_confidence	-0.084	**0.947**	0.070
TP-A_aware	**0.737**	0.081	-0.279
TP-A_consider	**0.894**	-0.077	-0.056
TP-V_understand	**0.788**	-0.123	0.226
TP-V_verify	**0.588**	0.005	0.206
TP-P_preference	-0.324	-0.137	**0.842**
TP-P_performance	0.266	0.105	**0.712**
TP-P_trust	0.229	0.111	**0.747**
median	4	6	5
mean (std)	3.77 (1.769)	5.184 (1.498)	4.845 (1.52)

Largest Euclidean Distances ($d > 3.5$). The three largest Euclidean distances are all related to the *webcam cover*. Hence, participants' corresponding responses differed the most between the *webcam cover* and *sunglasses* ($d = 4.33$), *distance markings* ($d = 3.99$), and *remote controls* ($d = 3.88$).

5.2.4 Summary: RQ2.2 – Differences and Similarities Between the Presented Tangible Privacy Mechanisms. Participants generally perceived the presented tangible privacy mechanisms positively. They felt that the mechanisms were capable of protecting their privacy ($median = 5.0$) and preferred them over digital alternatives ($median_{reverse} = 5.0$). Participants would use *privacy shields*, *voting booths*, *dressing room curtains*, and *webcam covers* to protect their privacy, were convinced of their performance and preferred them over digital alternatives. They were not convinced of the protection provided by *sunglasses*, *distance markings*, and *remote controls* and felt neutral towards potential digital alternatives.

5.3 General Perception of Tangible Privacy

After assessing the presented mechanisms, participants answered ten items on the general perception of tangible privacy mechanisms regarding 1) tangible interactions, 2) effects on awareness, 3) ease of verification, and 4) physicalization.

5.3.1 Overall Feedback. Participants rated their preference for tangible interactions with privacy mechanisms overall neutrally ($median = 4$, see Table 2). Yet, they agreed to perceive positive effects on their awareness of possible privacy intrusions ($median = 6$) and also agreed that the functionality of tangible privacy mechanisms is easy to verify or understand ($median = 6{,}5$). Moreover, participants overall slightly agreed to prefer tangible privacy mechanisms over potential purely digital alternatives, assessing the physicalization of these mechanisms ($median = 5$).

5.3.2 Principal Component Analysis. Next, we conducted a principal component analysis to determine if multiple tangible privacy items are related to the same factors. Based on the Kaiser criterion [34] (i.e., eigenvalues >1), we extracted three principal components from the tangible privacy items ($\chi^2(18) = 423$, $p < 0.001$). We applied an oblique promax rotation to the component matrix since we expected our factors to be related [25]. We named the resulting three principal components *tangible interaction*, *awareness\verification*, and *physicalization*, based on our intended investigation factors (Table 3). We calculated Cronbach's α to evaluate the internal consistency of the components. Resulting α-values were larger than 0.7 ($\alpha_{tangible\_interaction} = 0.825$, $\alpha_{awareness\backslash verification} = 0.739$, and $\alpha_{physicalization} = 0.735$).

5.3.3 Summary: RQ2.1 – General Perception of Purely Tangible Privacy. Participants felt overall neutral towards being able to touch tangible privacy mechanisms ($median = 4.0$). However, they perceived the positive effects of such

Table 4. Participants' previous experiences with each exemplary tangible privacy mechanism. The table shows how many of the $N = 444$ participants have 1) generally used each mechanism or 2) used it to protect their privacy.

mechanism	generally used	used to protect privacy
dressing room curtains	92.79%	68.92%
privacy shield	73.87%	65.32%
voting booth	83.11%	63.96%
webcam cover	57.88%	53.60%
headphones	92.12%	48.42%
distance markings	54.05%	19.82%
remote control	79.73%	18.92%
sunglasses	79.28%	14.19%

mechanisms on their awareness ($median = 6.0$) and felt that these mechanisms are easy to verify ($medians = 5.0, 6.0$). They also indicated a slight preference for tangible mechanisms over non-physicalized purely digital alternatives ($median = 5.0$). Moreover, we found that awareness and verifiability items measured the same underlying latent variable.

5.4 Personal Attributes

In addition to participants' demographics, we derived their experiences with IoT technology and the eight presented established tangible privacy mechanisms, as well as their standard scale scores.

5.4.1 Previous Experiences. We counted the number of IoT devices participants use regularly and the number of "yes" answers to both previous usage questions regarding each presented established tangible privacy mechanism (i.e., *"I have used the object described above in the past"* and *"I have used the object described above in the past to protect my privacy from other technical devices"*). Participants had varying prior experiences with IoT devices and tangible privacy mechanisms. On average, they reported using $mean = 5.32$ of 16 possible IoT devices regularly (range: $1 - 14$, $std = 2.45$).

Moreover, participants had used $mean = 6.13$ of the eight presented established tangible privacy mechanisms before (range: $0 - 8$, $std = 1.45$). Since some mechanisms can also be used for non-privacy-related purposes, we asked participants if they had used each mechanism before to protect their privacy from surrounding devices. Participants had used $mean = 3.53$ of the eight mechanisms before for this purpose (range: $0 - 8$, $std = 2.00$). When comparing the mechanisms, we observed that most participants reported having used *dressing room curtains* to protect their privacy from surrounding technical devices (68.92%), followed by *privacy shield* (65.32%), *voting booth* (63.96%), *webcam cover* (53.60%), and *headphones* (48.42%, see Table 4). *Distance markings*, *remote controls* and *sunglasses* were used by less than 20% of the participants to protect their privacy from surrounding devices.

5.4.2 Standard Scales. We first analyzed the internal consistency of each standard scale. Cronbach's alpha [12] for all standard scales ranged from 0.772 to 0.963, indicating acceptable internal consistencies [6, 67]. To achieve comparability between the standard scales, we subsequently summarized each by calculating corresponding mean values (see Table 5). Next, we standardized the resulting values and analyzed correlations between standard scale means, by calculating Pearson's r correlation coefficient (see Appendix D.4 for a complete list). Only two correlation coefficients were larger than 0.8, which indicates that the corresponding standard scales ($r_{IUIPC-CFIP} = 0.805$, $p_{IUIPC-CFIP} < 0.001$ and $r_{NFT-NFT+} = 0.981$, $p_{NFT-NFT+} < 0.001$) might measure the same latent variables. We then assessed the internal consistencies of IUIPC-CFIP and NFT-NFT+. Both resulting standardized Cronbach's alpha [12] values were acceptable

Table 5. Internal validity (Cronbach's alpha [12]) and descriptive statistics of all used standard scales and additional questions on participants' general need for touch (NFT+).

scale	internal consistency	possible range	means range	means mean	means std
ATI	0.905	[1,6]	1.000 - 6.0	3.831	1.023
IUIPC	0.874	[1,7]	3.600 - 7.0	6.167	0.753
CFIP	0.870	[1,7]	3.667 - 7.0	6.025	0.692
TIT	0.846	[1,5]	1.571 - 5.0	3.681	0.620
SeBIS	0.772	[1,5]	2.062 - 5.0	3.790	0.542
SA	0.870	[1,5]	1.000 - 5.0	3.551	0.768
NFT	0.963	[1,7]	1.000 - 7.0	3.720	1.410
NFT+	0.893	[1,7]	1.000 - 7.0	3.763	1.485

Table 6. Participants' perception of tangible privacy mechanisms in relation to their gender.

gender	n	tangible interaction mean	tangible interaction std	awareness\ verification mean	awareness\ verification std	physicalization mean	physicalization std
female	230	3.68	1.41	5.14	0.99	4.70	1.27
male	206	3.84	1.59	5.21	1.22	4.97	1.14
other	5	4.27	1.38	5.55	1.01	6.13	1.41
unknown	3	5.00	1.00	5.92	0.38	5.00	1.00

($\alpha_{IUIPC-CFIP} = 0.892$ and $\alpha_{NFT-NFT+} = 0.981$) [6, 67]. Hence, we summarized the corresponding standard scales naming the constructs *information privacy concerns* (IUIPC-CFIP) and *extended need for touch* (NFT-NFT+).

5.5 Correlation Between Personal Attributes and Perception of Tangible Privacy

To answer RQ3 we analyzed the link between participants' personal attributes and their perception of tangible privacy.

5.5.1 Analysis of Gender. Table 6 summarizes participants' perception of tangible privacy distinguished by chosen gender category. Male participants' response means for all three tangible privacy components were higher than female participants' ($means_{female}$: 3.68, 5.14 and 4.70; $means_{male}$: 3.84, 5.21 and 4.97). The mean values of participants who selected the gender category "other" were higher than both male and female participants' values for all three components ($means_{other}$: 4.27, 5.55, and 6.13). We subsequently analyzed the subset of male or female participants ($N = 436$) for gender-related correlations with tangible privacy components, as these two categories each contain a sufficiently large number of participants to conduct such tests. We found Pearson's correlation coefficients of $r = 0.05$ ($p = 0.265$) for *tangible interaction*, $r = 0.03$ ($p = 0.502$) for *awareness\verification* and $r = 0.11$ ($p = 0.021$) for *physicalization*. Only the correlation between male/female and *physicalization* was significant ($p < 0.05$).

5.5.2 Correlations. Next, we assessed correlations between the remaining personal attributes and components of tangible privacy. Correlation coefficients r varied from -0.21 to 0.47 ($mean = 0.10$, $std = 0.14$). Due to space limitations, we report only significant ($p < 0.05$) correlations. Figure 5 shows all Pearson's coefficients.

Tangible Interaction. We found statistically significant positive correlations between participants' perception of *tangible interaction* related aspects and their extended need for touch ($r = 0.47$, $p < 0.001$), the number of tangible privacy mechanisms they have used before to protect their privacy ($r = 0.28$, $p < 0.001$), ATI ($r = 0.16$, $p = 0.001$), TIT ($r = 0.11$, $p = 0.019$), as well as SA mean scores ($r = 0.10$, $p = 0.035$). Participants' age was negatively correlated with this component ($r = -0.21$, $p < 0.001$).

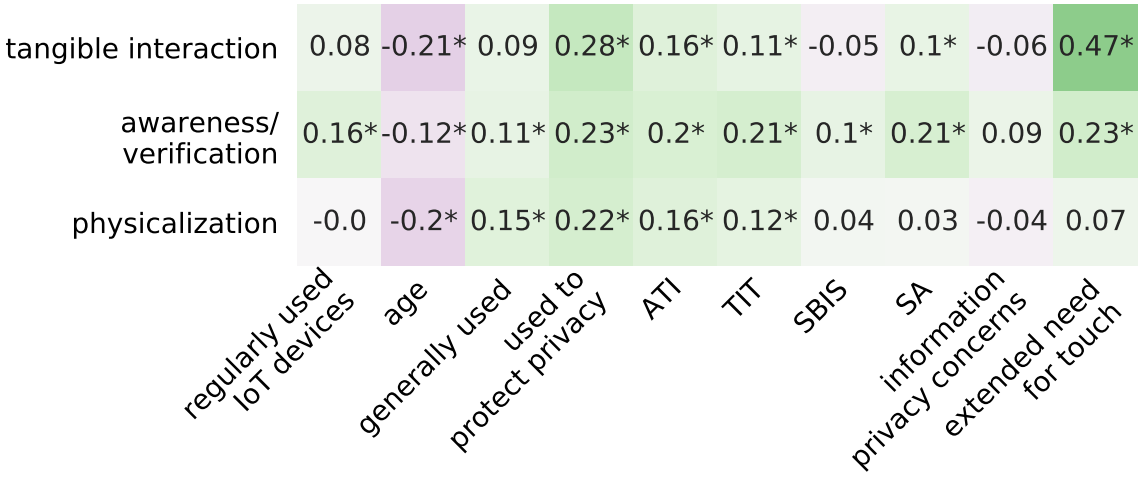


Fig. 5. Pearson's correlation coefficients of personal attributes against tangible privacy scores. Significant correlations with a p-value of $p < 0.05$ are highlighted with (*). Please refer to Appendix D.5 for a similar table.

Physicalization. Participants' feedback to *physicalization* aspects of tangible privacy mechanisms was positively correlated with how many mechanisms they used before to protect their privacy ($r = 0.21$, $p < 0.001$), their ATI mean scores ($r = 0.16$, $p = 0.001$), general experience with the mechanisms (i.e., not necessary privacy related) ($r = 0.15$, $p = 0.001$) and TIT mean scores ($r = 0.12$, $p = 0.012$). Participants' age was negatively correlated with *physicalization* aspects of tangible privacy ($r = -0.2$, $p < 0.001$).

Awareness\Verification. Our analysis indicates that *awareness\ verification* aspects of tangible privacy mechanisms are significantly correlated to all investigated personal attributes but participants' information privacy concerns. Hence, we found positive correlations with how many of our exemplary mechanisms participants' used before to protect their privacy ($r = 0.233$, $p < 0.001$), participants' extended need for touch ($r = 0.229$, $p < 0.001$) as well as their TIT ($r = 0.214$, $p < 0.001$), SA ($r = 0.209$, $p < 0.001$) and ATI mean scores ($r = 0.202$, $p < 0.001$). We further found corresponding significant positive correlations with the number of IoT devices our participants used regularly ($r = 0.163$, $p = 0.001$), the number of exemplary tangible privacy mechanisms they used before (not necessarily to protect their privacy) ($r = 0.109$, $p = 0.021$) and their SeBIS mean scores ($r = 0.103$, $p = 0.030$). Participants' age was again negatively correlated ($r = -0.117$, $p = 0.014$).

Summary: Largest Correlations ($|r| > 0.2$). To summarize the largest observed correlations, we found positive correlations between some of our three components of tangible privacy and participants' extended need for touch ($r > 0.22$), previous usage of the presented established tangible privacy mechanisms ($r > 0.21$), their experiences with technology (i.e., ATI and TIT, $r > 0.20$) and their security attitudes (SA, $r = 0.21$). Our analysis also indicated negative correlation coefficients for participants' age ($r < -0.12$).

5.5.3 Linear Regression. Next, we conducted a linear regression analysis between selected personal attributes and the three factors of tangible privacy. We focused our analysis only on pairwise significant correlations since we considered those to be the most promising candidates for identifying relationships. Hence, we defined either participants' opinions in regard to tangible interaction, physicalization, or awareness\verification as the dependent variable. As independent

variables, we selected all corresponding personal attributes with significant correlations. Table **??** shows the results of the regression analysis conducted on the standardized values.

Tangible Interactions. Participants' tangible interaction-related perception of privacy mechanisms could be predicted by their *extended need for touch* ($\beta = 0.446$, $p < 0.001$), their *usage of tangible mechanisms to protect their privacy* ($\beta = 0.164$, $p < 0.001$) and *ATI* scores ($\beta = 0.114$, $p = 0.022$).

Physicalization. Our results suggest that physicalization aspects of tangible privacy can be predicted by participants' *usage of tangible mechanisms to protect their privacy* ($\beta = 0.139$, $p = 0.009$) and their *age* ($\beta = -0.116$, $p = 0.021$).

Awareness\Verification. Participants' *previous usage of tangible mechanisms to protect their privacy* ($\beta = 0.135$, $p = 0.011$), *extended need for touch* ($\beta = 0.208$, $p < 0.001$), *TIT* ($\beta = 0.147$, $p = 0.002$) and *SA* scores ($\beta = 0.144$, $p = 0.016$) predicted their perception of positive effects of tangible privacy mechanisms on their awareness and ability to verify the functionality of mechanisms.

5.6 Summary: RQ1 and RQ3

5.6.1 RQ1 – Personal Attributes. Our regression analysis indicates that participants' privacy-related previous experiences with the presented eight mechanisms correlated positively with their perceptions of all investigated properties of tangible privacy. Moreover, participants' extended need for touch (NFT and NFT+) was related to their perceptions of multiple properties of tangible privacy (i.e., tangible interaction and awareness/verification). We conclude that 1) prior experience in privacy-related use of tangible privacy mechanisms and 2) personal preference for touch strongly influence participants' general opinions about tangible privacy mechanisms.

5.6.2 RQ3 – Personal Attributes' and Properties of Tangible Privacy Mechanisms. To answer RQ3, we do not consider our findings regarding the impact of participants' previous experiences and their need for touch, since those are generalizable findings (i.e., they relate to multiple properties of tangible privacy mechanisms), and thus, are discussed above while answering RQ1. Here we discuss the results of our regression analysis that indicate participants' preferences regarding tangible interactions with privacy mechanisms correlate with their ATI scores. People's perceptions regarding awareness\verification properties of tangible privacy mechanisms could be predicted through their trust in technology (i.e., TIT scores), and their security attitudes (SA). Moreover, we found a negative impact of participants' age on their perception of physicalization (i.e., potential preference for tangible over digital alternatives).

5.7 Limitations

Selection of Tangible Privacy Mechanims. To collect a list of established tangible privacy mechanisms, we recruited a few persons who were aware of privacy risks associated with sensor-enhanced devices. We expected these subjects to be particularly attentive to privacy mechanisms in their everyday environment. The findings of this group discussion are therefore neither representative of the general population nor exhaustive, as our aim was rather to identify some exemplary mechanisms that come to mind easily. Nevertheless, both the findings of our pilot survey and the main survey confirm that the selected mechanisms were indeed well-known by the majority of participants.

Online Survey. As our study relies on self-reported data, it might be subject to self-report bias, social desirability bias, and availability bias. We also mentioned in the recruitment message that our study aims to assess privacy protection mechanisms (see Appendix C.2.1). This may have resulted in people interested in such topics being more likely to apply

for participation (i.e., self-selection bias). Moreover, our participant sample was representative of the US population, which might affect generalizability. We also selected eight specific examples of established tangible privacy mechanisms for this study – so it remains to be investigated if our findings can be replicated with other established tangible privacy mechanisms. In particular, we presented rather low-tech mechanisms to our participants since both the review of related work and the results of our group discussion indicated that only those are widely established at this point. Hence, we encourage researchers to replicate our results for more high-tech mechanisms in the future.

6 DESIGN RECOMMENDATIONS & FUTURE WORK

By examining how personal attributes relate to user preferences for tangible privacy mechanisms, we gained insight into which properties are preferred or disliked by which users. While the presented tangible privacy mechanisms were low-tech solutions, we believe that our gained insights can be extrapolated to future high-tech solutions. Based on our findings, we formulate and discuss the following design recommendations to inform future privacy mechanisms within the digital-tangible spectrum.

6.1 Privacy Mechanisms For the General Population

6.1.1 Tangible Features Generally Support Awareness and Ease of Verification. Participants overall agreed most strongly with perceiving awareness and verification properties of tangible privacy mechanisms as beneficial. They believed that having tangible privacy mechanisms would improve their awareness of possible privacy intrusions and that the function of these mechanisms would be easy to understand and verify. Therefore, our results emphasize the strong positive impact of tangible mechanisms on both awareness and ease of verification. *Future privacy mechanisms aimed at the general population should consider tangibility to increase awareness of risks and enable easy verifiability.* Based on our results, we argue that this does not necessarily require a system to support tangible interaction as user input or output modality. *We surmise automated or ambient mechanisms that enforce physical privacy protections could facilitate this without burdening the user with additional tasks.* In related work, one can already find a few examples of such mixed mechanisms, like automatic webcam covers [18, 74]. Similarly, a curtain could close automatically when a device with a camera is nearby. Or a distance marking could light up or change its color if there are microphones in the vicinity.

6.1.2 Privacy-Related Previous Experiences Are Key. Our regression analysis indicates that the number of tangible mechanisms our participants have previously used to protect their privacy correlates with all investigated perceptions of tangible privacy mechanisms. However, non-privacy-related usage of the mechanisms did not show significance in the regression analysis. We assume these results are not indicative of a familiarity bias but rather indicate a very strong impact of already established mental models on the perceived purpose of the tangible mechanisms. Hence, *if people have already gained privacy-related experiences with multiple similar privacy mechanisms, they have a better opinion overall of such mechanisms.* When comparing participants' feedback for the different mechanisms, we found that corresponding to their previous experiences with each mechanism, privacy shield, voting booth, dressing room curtains, and webcam covers were perceived as more competent than the remaining mechanisms. We believe that *the acceptance of future privacy mechanisms will evolve gradually with increased and more widespread usage. Our results also lead us to question how novel prototypical privacy mechanisms can be meaningfully evaluated considering this strong prior experience effect.*

6.2 Recommendations for Targeted Designs of Privacy Mechanisms

6.2.1 People with a Strong Need for Touch Appreciate Multiple Properties of Tangible Mechanisms. As we already anticipated, we found a strong correlation between people's extended need for touch and their perception of tangible interactions. People who generally have a preference for tangible interactions maintain this preference when considering privacy mechanisms. Furthermore, our results indicate that people with a high need for touch appreciate the positive impact of a tangible privacy mechanism on becoming aware of possible risks and their ease of verification. Moreover, our correlation analysis indicated a slight positive correlation between participants' need for touch and their preference for tangible mechanisms (i.e., physicalization properties), although not statistically significant. *Thus, we recommend that developers of novel privacy mechanisms consider the need for touch of their targeted users and opt for corresponding designs.*

6.2.2 Affinity for Technology or Security Positively Impacts Opinions on Tangible Privacy. Our regression analysis indicated that participants with a higher affinity for technology appreciated being able to manipulate such mechanisms tangibly. This result contrasts with prior works' assumptions that less tech-savvy individuals might benefit from tangible privacy controls [16, 50]. Our findings also revealed that participants knowledgeable about security routines and willing to follow them (i.e., high SA-6 scores), appreciate the positive impact and ease of verification of tangible privacy mechanisms. Hence, while tech-savvy persons enjoy tangible interactions, security-affine people prefer tangible mechanisms' positive impact on awareness and ease of verification. *Therefore, we see an overarching need for privacy mechanisms for expert users that incorporate particular tangible properties.* Our results lead us to recommend that *future privacy mechanisms should integrate means for tangible interactions for the generally tech-savvy users while providing increased awareness of privacy risks and easy-to-verify privacy protections by design for more security-affine users.*

6.3 Open Question for Future Research

6.3.1 It is Unclear How To Support Persons With Little Trust in Technology. We expected that persons with high trust in technology might feel less of a need to be aware of risks or able to verify how the tangible privacy mechanism operates. However, we found participants' trust in technology positively correlated with their opinions on awareness\verification properties of tangible privacy mechanisms. While we found this surprising, we assume that it might be rooted in people with low trust in technology also being distrustful of privacy mechanisms. Such individuals could find awareness\verification features pointless. This reasoning is based on prior work identifying *learned helplessness* among people when it comes to protecting their own privacy [63]. We, thus, argue that *future research is needed to investigate how to specifically support individuals with little trust in technology.*

6.3.2 Potential Preference for Purely Digital Privacy Mechanisms of Older Participants. The results of our regression analysis suggest a negative impact of age on participants' potential preference for tangible mechanisms over digital alternatives (i.e., physicalization properties of tangible privacy mechanisms). Hence, participants' self-reported preference for tangible mechanisms over digital alternatives decreased with increased age. In other words, *older participants reported perceiving physicalization less positively (i.e., compared to potential digital alternatives).* Moreover, our correlation analysis revealed that age was significantly negatively correlated to the perception of all investigated properties of tangible privacy. These findings are surprising since related work suggests that tangible privacy mechanisms could be more attractive for older adults [16, 53]. We believe that these seemingly contradictory observations may be indicative of self-report bias in our work. Moreover, related work indicates that older peoples' vulnerabilities and privacy needs

are impacted by their unique interplay of multiple personal factors rather than by age alone [81]. Therefore, *we see a need for further research on the design of privacy mechanisms for this specific group.*

7 CONCLUSION

In this work, we conducted a detailed exploration of the relationship between users' personal attributes and their perceptions of various properties of tangible privacy mechanisms. We conducted an online survey with $N = 444$ participants, through which we evaluated users' preferences for touching tangible privacy mechanisms, effects on awareness, perceived ease of verification, and physicalization. We found users' prior experience of privacy-related usage of the mechanisms and "need for touch" most impact their perception of privacy mechanisms. Additional influential factors were age, trust in technology, technical affinity, and security attitudes. Our work offers valuable insights and recommendations for the design of future privacy mechanisms, whether tangible, digital, or mixed. Our findings highlight open questions for future research, particularly concerning the identification of reasons for the observed correlations, and the development of privacy mechanisms that support individuals with little trust in technology.

ACKNOWLEDGMENTS

We would like to thank our study participants for their time and valuable feedback. We also thank Prof. Dr. Philipp Rauschnabel for his input on the applied statistical analysis. This project has been funded by the European Union – NextGeneration EU and the dtec.bw – Center for Digitization and Technology Research of the Bundeswehr as part of the project MuQuaNet. Moreover, this work was supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972.

REFERENCES

[1] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. 2020. Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy. *Proc. ACM Hum.-Comput. Interact.* 4, CSCW2, Article 116 (Oct. 2020), 28 pages. https://doi.org/10.1145/3415187

[2] Ashwaq Alsoubai, Reza Ghaiumy Anaraky, Yao Li, Xinru Page, Bart Knijnenburg, and Pamela J. Wisniewski. 2022. Permission vs. App Limiters: Profiling Smartphone Users to Understand Differing Strategies for Mobile Privacy Management. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 406, 18 pages. https://doi.org/10.1145/3491102.3517652

[3] Susan B Barnes. 2006. A privacy paradox: Social networking in the United States. *First Monday* (2006).

[4] Moritz Behrens, Nina Valkanova, Ava Fatah gen. Schieck, and Duncan P. Brumby. 2014. Smart Citizen Sentiment Dashboard: A Case Study Into Media Architectural Interfaces. In *Proceedings of The International Symposium on Pervasive Displays* (Copenhagen, Denmark) *(PerDis '14)*. Association for Computing Machinery, New York, NY, USA, 19–24. https://doi.org/10.1145/2611009.2611036

[5] Steven Bellman, Eric J. Johnson, Stephen J. Kobrin, and Gerald L. Lohse. 2004. International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society* 20, 5 (2004), 313–324. https://doi.org/10.1080/01972240490507956 arXiv:https://doi.org/10.1080/01972240490507956

[6] Mohamad Adam Bujang, Evi Diana Omar, and Nur Akmal Baharum. 2018. A review on sample size determination for Cronbach's alpha test: a simple guide for researchers. *The Malaysian journal of medical sciences: MJMS* 25, 6 (2018), 85.

[7] George Chalhoub, Martin J Kraemer, Norbert Nthala, and Ivan Flechais. 2021. "It Did Not Give Me an Option to Decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 555, 16 pages. https://doi.org/10.1145/3411764.3445691

[8] Keywon Chung, Michael Shilman, Chris Merrill, and Hiroshi Ishii. 2010. OnObject: gestural play with tagged everyday objects. In *Adjunct proceedings of the 23nd annual ACM symposium on user interface software and technology*. 379–380.

[9] 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

[10] Sunny Consolvo, Ian E. Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. 2005. Location Disclosure to Social Relations: Why, When, What People Want to Share. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Portland, Oregon, USA) *(CHI '05)*. Association for Computing Machinery, New York, NY, USA, 81–90. https://doi.org/10.1145/1054972.1054985

[11] Alan Cooper, Robert Reimann, David Cronin, and Christopher Noessel. 2014. *About face: the essentials of interaction design.* John Wiley & Sons.

[12] Lee J Cronbach and Paul E Meehl. 1955. Construct validity in psychological tests. *Psychological bulletin* 52, 4 (1955), 281.

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

[14] Sarah Delgado Rodriguez, Sarah Prange, and Florian Alt. 2021. Take Your Security and Privacy Into Your Own Hands! Why Security and Privacy Assistants Should be Tangible. In *Mensch und Computer 2021 - Workshopband*, Carolin Wienrich, Philipp Wintersberger, and Benjamin Weyers (Eds.). Gesellschaft für Informatik e.V., Bonn. https://doi.org/10.18420/muc2021-mci-ws09-393

[15] Sarah Delgado Rodriguez, Sarah Prange, Lukas Mecke, and Florian Alt. 2021. ActPad– A Smart Desk Platform to Enable User Interaction with IoT Devices. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI EA '21)*. Association for Computing Machinery, New York, NY, USA, Article 325, 6 pages. https://doi.org/10.1145/3411763.3451825

[16] Sarah Delgado Rodriguez, Sarah Prange, Christina Vergara Ossenberg, Markus Henkel, Florian Alt, and Karola Marky. 2022. PriKey – Investigating Tangible Privacy Control for Smart Home Inhabitants and Visitors. In *Nordic Human-Computer Interaction Conference* (Aarhus, Denmark) *(NordiCHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 74, 13 pages. https://doi.org/10.1145/3546155.3546640

[17] Verena Distler, Matthias Fassl, Hana Habib, Katharina Krombholz, Gabriele Lenzini, Carine Lallemand, Lorrie Faith Cranor, and Vincent Koenig. 2021. A Systematic Literature Review of Empirical Methods and Risk Representation in Usable Privacy and Security Research. *ACM Trans. Comput.-Hum. Interact.* 28, 6, Article 43 (dec 2021), 50 pages. https://doi.org/10.1145/3469845

[18] Youngwook Do, Jung Wook Park, Yuxi Wu, Avinandan Basu, Dingtian Zhang, Gregory D. Abowd, and Sauvik Das. 2022. Smart Webcam Cover: Exploring the Design of an Intelligent Webcam Cover to Improve Usability and Trust. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 5, 4, Article 154 (dec 2022), 21 pages. https://doi.org/10.1145/3494983

[19] David Dobbelstein, Philipp Hock, and Enrico Rukzio. 2015. Belt: An Unobtrusive Touch Input Device for Head-Worn Displays. 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, 2135–2138. https://doi.org/10.1145/2702123.2702450

[20] Janna Lynn Dupree, Richard Devries, Daniel M. Berry, and Edward Lank. 2016. Privacy Personas: Clustering Users via Attitudes and Behaviors toward Security Practices. 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, 5228–5239. https://doi.org/10.1145/2858036.2858214

[21] Serge Egelman and Eyal Peer. 2015. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). 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, 2873–2882. https://doi.org/10.1145/2702123.2702249

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

[23] Cori Faklaris, Laura A. Dabbish, and Jason I. Hong. 2019. A Self-Report Measure of End-User Security Attitudes (SA-6). In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 61–77. https://www.usenix.org/conference/soups2019/presentation/faklaris

[24] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. 2021. A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 64, 16 pages. https://doi.org/10.1145/3411764.3445148

[25] AP Field. 2005. Discovering statistics using SPSS.

[26] Kenneth P. Fishkin. 2004. A Taxonomy for and Analysis of Tangible Interfaces. *Personal Ubiquitous Comput.* 8, 5 (sep 2004), 347–358.

[27] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale. *International Journal of Human–Computer Interaction* 35, 6 (2019), 456–467. https://doi.org/10.1080/10447318.2018.1456150 arXiv:https://doi.org/10.1080/10447318.2018.1456150

[28] Alisa Frik, Juliann Kim, Joshua Rafael Sanchez, and Joanne Ma. 2022. Users' Expectations About and Use of Smartphone Privacy and Security Settings. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 407, 24 pages. https://doi.org/10.1145/3491102.3517504

[29] 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

[30] Juha Häikiö, Arto Wallin, Minna Isomursu, Heikki Ailisto, Tapio Matinmikko, and Tua Huomo. 2007. Touch-based user interface for elderly users. In *Proceedings of the 9th international conference on Human computer interaction with mobile devices and services*. 289–296.

[31] Beverly L. Harrison, Kenneth P. Fishkin, Anuj Gujar, Carlos Mochon, and Roy Want. 1998. Squeeze Me, Hold Me, Tilt Me! An Exploration of Manipulative User Interfaces. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Los Angeles, California, USA) *(CHI '98)*. ACM Press/Addison-Wesley Publishing Co., USA, 17–24. https://doi.org/10.1145/274644.274647

[32] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. 2018. Rethinking Access Control and Authentication for the Home Internet of Things (IoT). In *27th USENIX Security Symposium (USENIX Security 18)*. USENIX Association, Baltimore, MD, 255–272. https://www.usenix.org/conference/usenixsecurity18/presentation/he

[33] Adam N Joinson, Ulf-Dietrich Reips, Tom Buchanan, and Carina B Paine Schofield. 2010. Privacy, trust, and self-disclosure online. *Human–Computer Interaction* 25, 1 (2010), 1–24.

[34] Henry F Kaiser. 1960. The application of electronic computers to factor analysis. *Educational and psychological measurement* 20, 1 (1960), 141–151.

[35] 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

[36] Nari Kim, Juntae Kim, Bomin Kim, and Young-Woo Park. 2021. *The Trial of Posit in Shared Offices: Controlling Disclosure Levels of Schedule Data for Privacy by Changing the Placement of a Personal Interactive Calendar.* Association for Computing Machinery, New York, NY, USA, 149–159. https://doi.org/10.1145/3461778.3462073

[37] Marion Koelle, Katrin Wolf, and Susanne Boll. 2018. Beyond LED Status Lights - Design Requirements of Privacy Notices for Body-Worn Cameras. In *Proceedings of the Twelfth International Conference on Tangible, Embedded, and Embodied Interaction* (Stockholm, Sweden) *(TEI '18)*. Association for Computing Machinery, New York, NY, USA, 177–187. https://doi.org/10.1145/3173225.3173234

[38] Oksana Kulyk, Kristina Milanovic, and Jeremy Pitt. 2020. Does My Smart Device Provider Care About My Privacy? Investigating Trust Factors and User Attitudes in IoT Systems. 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 29, 12 pages. https://doi.org/10.1145/3419249.3420108

[39] Ponnurangam Kumaraguru and Lorrie Faith Cranor. 2005. *Privacy indexes: a survey of Westin's studies.* Carnegie Mellon University, School of Computer Science, Institute for ....

[40] Yanhong Li, Meng Liang, Julian Preissing, Nadine Bachl, Michelle Melina Dutoit, Thomas Weber, Sven Mayer, and Heinrich Hussmann. 2022. A meta-analysis of tangible learning studies from the tei conference. In *Sixteenth International Conference on Tangible, Embedded, and Embodied Interaction*. 1–17.

[41] Meng Liang, Yanhong Li, Thomas Weber, and Heinrich Hussmann. 2021. Tangible interaction for children's creative learning: A review. In *Creativity and Cognition*. 1–14.

[42] Jialiu Lin, Bin Liu, Norman Sadeh, and Jason I. Hong. 2014. Modeling Users' Mobile App Privacy Preferences: Restoring Usability in a Sea of Permission Settings. In *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security* (Menlo Park, CA) *(SOUPS '14)*. USENIX Association, USA, 199–212.

[43] Bin Liu, Jialiu Lin, and Norman Sadeh. 2014. Reconciling Mobile App Privacy and Usability on Smartphones: Could User Privacy Profiles Help?. In *Proceedings of the 23rd International Conference on World Wide Web* (Seoul, Korea) *(WWW '14)*. Association for Computing Machinery, New York, NY, USA, 201–212. https://doi.org/10.1145/2566486.2568035

[44] 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. http://www.jstor.org/stable/23015787

[45] Shrirang Mare, Logan Girvin, Franziska Roesner, and Tadayoshi Kohno. 2019. Consumer Smart Homes: Where We Are and Where We Need to Go. In *Proceedings of the 20th International Workshop on Mobile Computing Systems and Applications* (Santa Cruz, CA, USA) *(HotMobile '19)*. Association for Computing Machinery, New York, NY, USA, 117–122. https://doi.org/10.1145/3301293.3302371

[46] Karola Marky, Sarah Prange, Max Mühlhäuser, and Florian Alt. 2021. Roles Matter! Understanding Differences in the Privacy Mental Models of Smart Home Visitors and Residents. In *20th International Conference on Mobile and Ubiquitous Multimedia* (Leuven, Belgium) *(MUM 2021)*. Association for Computing Machinery, New York, NY, USA, 108–122. https://doi.org/10.1145/3490632.3490664

[47] Karola Marky, Martin Schmitz, Verena Zimmermann, Martin Herbers, Kai Kunze, and Max Mühlhäuser. 2020. 3D-Auth: Two-Factor Authentication with Personalized 3D-Printed Items. 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/10.1145/3313831.3376189

[48] 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

[49] D. Harrison Mcknight, Michelle Carter, Jason Bennett Thatcher, and Paul F. Clay. 2011. Trust in a Specific Technology: An Investigation of Its Components and Measures. *ACM Trans. Manage. Inf. Syst.* 2, 2, Article 12 (jul 2011), 25 pages. https://doi.org/10.1145/1985347.1985353

[50] Vikram Mehta. 2019. Tangible Interactions for Privacy Management *(TEI '19)*. Association for Computing Machinery, New York, NY, USA, 723–726. https://doi.org/10.1145/3294109.3302934

[51] Vikram Mehta, Arosha K. Bandara, Blaine A. Price, and Bashar Nuseibeh. 2016. Privacy Itch and Scratch: On Body Privacy Warnings and Controls. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI EA '16)*. Association for Computing Machinery, New York, NY, USA, 2417–2424. https://doi.org/10.1145/2851581.2892475

[52] Vikram Mehta, Arosha K. Bandara, Blaine A. Price, Bashar Nuseibeh, and Daniel Gooch. 2021. Up Close & Personal: Exploring User-Preferred Image Schemas for Intuitive Privacy Awareness and Control. In *Proceedings of the Fifteenth International Conference on Tangible, Embedded, and Embodied Interaction* (Salzburg, Austria) *(TEI '21)*. Association for Computing Machinery, New York, NY, USA, Article 7, 13 pages. https:

//doi.org/10.1145/3430524.3440626

[53] Vikram Mehta, Daniel Gooch, Arosha Bandara, Blaine Price, and Bashar Nuseibeh. 2021. Privacy Care: A Tangible Interaction Framework for Privacy Management. *ACM Trans. Internet Technol.* 21, 1, Article 25 (Feb. 2021), 32 pages. https://doi.org/10.1145/3430506

[54] Vikram Mehta, Daniel Gooch, Arosha Bandara, Blaine A. Price, and Bashar Nuseibeh. 2023. A Card-Based Ideation Toolkit to Generate Designs for Tangible Privacy Management Tools. In *Proceedings of the Seventeenth International Conference on Tangible, Embedded, and Embodied Interaction* (Warsaw, Poland) *(TEI '23)*. Association for Computing Machinery, New York, NY, USA, Article 19, 13 pages. https://doi.org/10.1145/3569009.3572903

[55] Donald A. Norman and Stephen W. Draper. 1986. *User Centered System Design; New Perspectives on Human-Computer Interaction*. L. Erlbaum Associates Inc., USA.

[56] Joann Peck and Terry L. Childers. 2003. Individual Differences in Haptic Information Processing: The "Need for Touch" Scale. *Journal of Consumer Research* 30, 3 (12 2003), 430–442. https://doi.org/10.1086/378619 arXiv:https://academic.oup.com/jcr/article-pdf/30/3/430/11425838/30-3-430.pdf

[57] Sarah Prange, Ahmed Shams, Robin Piening, Yomna Abdelrahman, and Florian Alt. 2021. PriView – Exploring Visualisations Supporting Users' Privacy Awareness. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3313831.3376840

[58] Sarah Delgado Rodriguez, Oliver Hein, Ismael Prieto Romero, Lukas Mecke, Felix Dietz, Sarah Prange, and Florian Alt. [n.d.]. Shake-It-All: A Toolkit for Sensing Tangible Interactions on Everyday Objects. ([n. d.]).

[59] Valkyrie Savage, Xiaohan Zhang, and Björn Hartmann. 2012. Midas: Fabricating Custom Capacitive Touch Sensors to Prototype Interactive Objects. In *Proceedings of the 25th Annual ACM Symposium on User Interface Software and Technology* (Cambridge, Massachusetts, USA) *(UIST '12)*. Association for Computing Machinery, New York, NY, USA, 579–588. https://doi.org/10.1145/2380116.2380189

[60] William Seymour, Martin J. Kraemer, Reuben Binns, and Max Van Kleek. 2020. Informing the Design of Privacy-Empowering Tools for the Connected Home. 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, 1–14. https://doi.org/10.1145/3313831.3376264

[61] Orit Shaer, Nancy Leland, Eduardo H Calvillo-Gamez, and Robert JK Jacob. 2004. The TAC paradigm: specifying tangible user interfaces. *Personal and ubiquitous computing* 8 (2004), 359–369.

[62] Ehud Sharlin, Benjamin Watson, Yoshifumi Kitamura, Fumio Kishino, and Yuichi Itoh. 2004. On tangible user interfaces, humans and spatiality. *Personal and Ubiquitous Computing* 8 (2004), 338–346.

[63] Irina Shklovski, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14)*. Association for Computing Machinery, New York, NY, USA, 2347–2356. https://doi.org/10.1145/2556288.2557421

[64] H. Jeff Smith, Sandra J. Milberg, and Sandra J. Burke. 1996. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly* 20, 2 (1996), 167–196. http://www.jstor.org/stable/249477

[65] 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

[66] Charles Stangor and Jennifer Walinga. 2014. *Introduction to psychology*. BCcampus.

[67] Keith S Taber. 2018. The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in science education* 48, 6 (2018), 1273–1296.

[68] 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] https://arxiv.org/abs/1911.07701

[69] Mark Turner, Martin Schmitz, Morgan Masichi Bierey, Mohamed Khamis, and Karola Marky. 2023. Tangible 2FA – An In-the-Wild Investigation of User-Defined Tangibles for Two-Factor Authentication. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. 245–261.

[70] Brygg Ullmer and Hiroshi Ishii. 2000. Emerging frameworks for tangible user interfaces. *IBM systems journal* 39, 3.4 (2000), 915–931.

[71] Mark D Weiser. 1994. Ubiquitous computing. In *ACM Conference on Computer Science*, Vol. 418. 197530–197680.

[72] Alan F. Westin. 1967. PRIVACY AND FREEDOM.

[73] Maximiliane Windl and Sven Mayer. 2022. The Skewed Privacy Concerns of Bystanders in Smart Environments. *Proc. ACM Hum.-Comput. Interact.* 6, MHCI, Article 184 (sep 2022), 21 pages. https://doi.org/10.1145/3546719

[74] Maximiliane Windl, Albrecht Schmidt, and Sebastian S. Feger. 2023. Investigating Tangible Privacy-Preserving Mechanisms for Future Smart Homes. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 70, 16 pages. https://doi.org/10.1145/3544548.3581167

[75] Pamela J Wisniewski, Bart P Knijnenburg, and Heather Richter Lipford. 2017. Making privacy personal: Profiling social network users to inform privacy education and nudging. *International Journal of human-computer studies* 98 (2017), 95–108.

[76] Allison Woodruff, Vasyl Pihur, Sunny Consolvo, Laura Brandimarte, and Alessandro Acquisti. 2014. Would a Privacy Fundamentalist Sell Their DNA for $1000...If Nothing Bad Happened as a Result? The Westin Categories, Behavioral Intentions, and Consequences. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. USENIX Association, Menlo Park, CA, 1–18. https://www.usenix.org/conference/soups2014/proceedings/presentation/woodruff

[77] Yaxing Yao. 2019. Designing for Better Privacy Awareness in Smart Homes. In *Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing* (Austin, TX, USA) *(CSCW '19)*. Association for Computing Machinery, New York, NY, USA, 98–101.

https://doi.org/10.1145/3311957.3361863

[78] 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)*. 159–176. https://www.usenix.org/system/files/sec19-zeng.pdf

[79] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 200, 20 pages. https://doi.org/10.1145/3274469

[80] Wei Zhou, Yan Jia, Anni Peng, Yuqing Zhang, and Peng Liu. 2018. The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal* 6, 2 (2018), 1606–1616. https://arxiv.org/abs/1911.07701

[81] Yixin Zou, Kaiwen Sun, Tanisha Afnan, Ruba Abu-Salma, Robin Brewer, and Florian Schaub. 2024. Cross-Contextual Examination of Older Adults' Privacy Concerns, Behaviors, and Vulnerabilities. *Proceedings on Privacy Enhancing Technologies* 1 (2024), 133–150.

[82] Tomasz Zukowski and Irwin Brown. 2007. Examining the Influence of Demographic Factors on Internet Users' Information Privacy Concerns. In *Proceedings of the 2007 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries* (Port Elizabeth, South Africa) *(SAICSIT '07)*. Association for Computing Machinery, New York, NY, USA, 197–204. https://doi.org/10.1145/1292491.1292514

A DEFINITION OF TANGIBLE PRIVACY MECHANISMS USED FOR THE GROUP BRAINSTORMING

A tangible privacy mechanism is a privacy control and feedback mechanism that is 'tangible', i.e., manipulated or perceived by touch. This can involve touching, tilting, pushing, grabbing, squeezing, shaking, scratching, or rotating an object.

B ALL SUGGESTED REAL WORLD TANGIBLE PRIVACY MECHANISMS

Table 7. A table containing all 19 established tangible privacy mechanisms proposed in a group discussion with three usable security researchers. We grouped mechanisms based on which kind of data they protect and their location. We then selected one mechanism of each group for further evaluation in our online survey.

tangible mechanism	data protected	location	group	selected
webcam cover/sticker	identity	on device	A	X
dressing room curtain	identity	distant	B	X
floor markings of camera field of view	identity	distant	B	
sunglasses	identity	on user	C	X
newspapers	identity	on user	C	
baseball caps	identity	on user	C	
voting booth	visual	distant	D	X
privacy screens	visual	distant	D	
floor distance marking	auditory	distant	E	X
pin pad privacy shield	visual	on device	F	X
room dividers/doors	identity/visual/auditory	distant	B/D/E	
mirror foils/privacy screen foils	visual	distant	D	
devices' on/off switches	identity/visual/auditory	on device	A/F/G	
blinders	identity/visual	distant	B/D	
green screens/background screens	visual	distant	D	
remote control for volume	auditory	distant/on device	E/G	X (for G)
headphones	auditory	on user	H	X
buttons with higher resistance to avoid accidental press	-	-	-	
distraction mechanisms against shoulders surfers	visual	on device	F	

C ONLINE QUESTIONNAIRE

C.1 Overview of Questionnaire Items

Table 8. A list of all items included in our online questionnaire and the personal factors we investigated with them.

investigated factor		**scale/item**
demographics	age	How old are you?
	gender	With which gender do you identify most?
	education	What is the highest degree or level of education you have completed?
	residence	In which country do you live?
	experiences with technology	Which smart devices do you use regularly?
		Affinity for Technology Interaction (ATI) [27]
		Trust in Technology [49]
privacy concerns and attitudes	security attitudes	Security Attitudes (SA-6) [23]
	/ behavior intentions	Security Behaviour Intention Scale (SeBIS) [21]
	privacy concerns	Concern for Information Privacy (CFIP) [64]
		Internet Users' Information Privacy Concerns (IUIPC) [44]
preference for tangible interaction		Need For Touch (NFT) [56]
	general need for touch (NFT+),	I can't help touching all kinds of objects.
	derived from NFT	Touching objects can be fun.
		I place more trust in objects that can be touched before using them.
		I feel more confident using an object after touching it.
		I find myself touching or physically manipulating all kinds of objects.
perception of tangible privacy	tangible interactions	Touching privacy mechanisms can be fun. (TP-I_fun)
(7-point Likert scales,		I place more trust in privacy mechanisms that can be touched. (TP-I_trust)
if not stated otherwise)		I feel more confident using a privacy mechanism after touching it. (TP-I_confidence)
	effect on awareness	Having the object described above nearby makes me aware that my privacy could be invaded. (TP-A_aware)
		Having the object described above nearby makes me consider to use it to protect my privacy. (TP-A_consider)
	ease of verification	It is easy to understand how the presented privacy mechanisms protect my privacy from other technical devices. (TP-V_understand)
		I can easily verify myself if the presented privacy mechanisms protect my privacy from other technical devices. (TP-V_verify)
	physicalization	I would prefer using a purely digital alternatives instead of the presented privacy mechanisms to protect my privacy from other technical devices (e.g. automatically blurring my body/data on camera images, jamming of microphones). (TP-P_preference)
		The presented privacy mechanisms protect my privacy better from other technical devices than purely digital alternatives. (TP-P_performance)
		I place more trust in the presented privacy mechanisms compared to purely digital alternatives. (TP-P_trust)
	eight examples	I have used the object described above in the past. [Yes | No | I don't know]
		I have used the object described above in the past to protect my privacy from other technical devices. [Yes | No | I don't know]
		If I were to use the object described above, it would be to protect my privacy from other technical devices. (EX_use_privacy)
		It is important to me that I own the object described above. (EX_own)
		I am convinced that the object described above protects my privacy from other technical devices. (EX_confidence)
		If the object described above is not installed by default, I would try install it myself or resort to a similar alternative to protect my privacy from other technical devices. (EX_alternative)
		I would prefer using a purely digital alternative to the object described above to protect my privacy from other technical devices (e.g. automatically blurring my body/data on camera images, jamming of microphones). (EX_preference)

C.2 Complete Questionnaire

Please find our complete online questionnaire in the following. Text added to provide additional context for this paper is highlighted with squared brackets.

C.2.1 [Recruitment Message]. Real World Privacy Protection Mechanisms: In this study, we would like to collect data about your experiences and perceptions of privacy protection mechanisms.

C.2.2 Welcome to our User Study. In this study, we would like to collect data about your experiences with privacy protection mechanisms. All questions will focus on privacy-related aspects with a particular focus on smart devices (i.e., internet-connected and sensor-enhanced devices). Please complete this 30-minutes survey.

C.2.3 Definition of Privacy in the Internet of Things (IoT). Please read the following information on privacy carefully. As already mentioned, we would like to collect data about your privacy behavior. Therefore, all questions will focus on privacy and privacy-related issues. Privacy is *"the right to prevent the disclosure of personal information to others"* [72].

Please note that this questionnaire focuses on Privacy in the Internet of Things (IoT), which is the right to prevent the disclosure of personal information specifically to nearby technical devices that may include invasive sensors such as video cameras or microphones. Hence, protecting one's Privacy in IoT, does not refer to privacy invasions directly caused by persons who, for example, can listen in on conversations or read private messages.

C.2.4 [True False Quiz]. To test your knowledge, read each statement carefully and decide if it is true or false. [Answer options were: true and false.]

- Privacy in IoT is someone's right to keep their personal matters and relationships secret from nearby technical devices.
- Snooping through a friend's diary is an example of invasion of Privacy in IoT.
- Privacy in IoT means the protection of people against a possible attack or other crime.
- Privacy in IoT is the right to prevent the disclosure of personal information to nearby sensor enhanced devices.
- Privacy in IoT is the act of keeping someone or something safe from injury, damage, or loss.

C.2.5 [ATI Scale [27]]. Please indicate the degree to which you agree/disagree with the following statements. The term "technical systems" refers to apps and other software applications, as well as entire digital devices (e.g., mobile phone, computer, TV, car navigation).

- I like to occupy myself in greater detail with technical systems.
- I like testing the functions of new technical systems.
- I predominantly deal with technical systems because I have to.
- When I have a new technical system in front of me, I try it out intensively.
- I enjoy spending time becoming acquainted with a new technical system.
- It is enough for me that a technical system works; I don't care how or why.
- I try to understand how a technical system exactly works.
- It is enough for me to know the basic functions of a technical system.
- I try to make full use of the capabilities of a technical system.

C.2.6 [CFIP Scale [64]]. Please indicate the degree to which you agree/disagree with the following statements.

- It usually bothers me when companies ask me for personal information.

- All the personal information in computer databases should be double-checked for accuracy-no matter how much this costs.
- Companies should not use personal information for any purpose unless it has been authorized by the individuals who provided the information.
- Companies should devote more time and effort to preventing unauthorized access to personal information.
- When companies ask me for personal information, I sometimes think twice before providing it.
- Companies should take more steps to make sure that the personal information in their files is accurate.
- When people give personal information to a company for some reason, the company should never use the information for any other reason.
- Companies should have better procedures to correct errors in personal information.
- Computer databases that contain personal information should be protected from unauthorized access-no matter how much it costs.
- It bothers me to give personal information to so many companies.
- Companies should never sell the personal information in their computer databases to other companies.
- Companies should devote more time and effort to verifying the accuracy of the personal information in their databases.
- Companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.
- Companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.
- I'm concerned that companies are collecting too much personal information about me.

C.2.7 [IUIPC Scale [44]]. Please indicate the degree to which you agree/disagree with the following statements.

- Consumer online privacy is the consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
- Consumer control of personal information lies at the heart of consumer privacy.
- I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.
- To show that you are paying attention, please select "strongly disagree" option as your answer.
- Companies seeking information online should disclose the way the data are collected, processed, and used.
- A good consumer online privacy policy should have a clear and conspicuous disclosure.
- It is very important to me that I am aware and knowledgeable about how my personal information will be used.
- It usually bothers me when online companies ask me for personal information.
- When online companies ask me for personal information, I sometimes think twice before providing it.
- It bothers me to give personal information to so many online companies.
- I'm concerned that online companies are collecting too much personal information about me.

C.2.8 [TIT Scale [49]]. Please indicate the degree to which you agree/disagree with the following statements.

- My typical approach is to trust new technologies until they prove to me that I shouldn't trust them.
- I usually trust a technology until it gives me a reason not to trust it.
- I generally give a technology the benefit of the doubt when I first use it.

- I believe that most technologies are effective at what they are designed to do.
- A large majority of technologies are excellent.
- Most technologies have the features needed for their domain.
- I think most technologies enable me to do what I need to do.

C.2.9 [SBIS Scale [21]]. Please indicate the degree to which you agree/disagree with the following statements.

- When I'm prompted about a software update, I install it right away.
- I try to make sure that the programs I use are up-to-date.
- I manually lock my computer screen when I step away from it.
- I set my computer screen to automatically lock if I don't use it for a prolonged period of time.
- I use a PIN or passcode to unlock my mobile phone.
- I use a password/passcode to unlock my laptop or tablet.
- If I discover a security problem, I continue what I was doing because I assume someone else will fix it.
- When someone sends me a link, I open it without first verifying where it goes.
- I verify that my anti-virus software has been regularly updating itself.
- When browsing websites, I mouseover links to see where they go, before clicking them.
- I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar.
- I do not change my passwords, unless I have to.
- I use different passwords for different accounts that I have.
- I do not include special characters in my password if it's not required.
- When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.
- I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon).

C.2.10 [SA-6 Scale [23]]. Please indicate the degree to which you agree/disagree with the following statements.

- Generally, I diligently follow a routine about security practices.
- I always pay attention to experts' advice about the steps I need to take to keep my online data and accounts safe.
- I am extremely knowledgeable about all the steps needed to keep my online data and accounts safe.
- I am extremely motivated to take all the steps needed to keep my online data and accounts safe.
- I often am interested in articles about security threats.
- I seek out opportunities to learn about security measures that are relevant to me.

C.2.11 [NFT scale [56] and Additional Items]. Please indicate the degree to which you agree/disagree with the following statements.

- When walking through stores, I can't help touching all kinds of products.
- Touching products can be fun.
- I place more trust in products that can be touched before purchase.
- I feel more comfortable purchasing a product after physically examining it.
- When browsing in stores, it is important for me to handle all kinds of products.
- If I can't touch a product in the store, I am reluctant to purchase the product.
- I like to touch products even if I have no intention of buying them.
- I feel more confident making a purchase after touching a product.

- When browsing in stores, I like to touch lots of products.
- The only way to make sure a product is worth buying is to actually touch it.
- There are many products that I would only buy if I could handle them before purchase.
- I find myself touching all kinds of products in stores.
- To make sure that you are paying attention, please select "slightly agree" option as your answer.
- I can't help touching all kinds of objects.
- Touching objects can be fun.
- I place more trust in objects that can be touched before using them.
- I feel more confident using an object after touching it.
- I find myself touching or physically manipulating all kinds of objects.

C.2.12 [General Instructions on Tangible Mechanisms]. In the next section, you will see a few examples of objects, that protect your privacy against other devices such as cameras or microphones (aka. privacy mechanisms). Please focus only on how these mechanisms protect your privacy from technical devices, rather than other persons. Please read the description of each mechanism carefully, click on the example to see how it works and finally answer the questions.

C.2.13 [Description of Each Mechanism].

- Voting booth: A voting booth is a room or cabin in a polling station that protects the secrecy of the ballot. No camera can therefore record your vote.
- Distance markings: Distance markings are markings placed at certain intervals on the floor to keep people a distance apart from each other. Such markings prevent eavesdropping: from a certain distance a microphone is not able to record your conversation (e.g. with a pharmacist).
- Dressing room curtain: Dressing room curtains are a piece of material which creates a barrier between you changing clothing and nearby cameras.
- Privacy shield on PIN pad: A privacy shield is a cover placed around a keypad. It prevents cameras from recording your PIN.
- Remote control: A remote control allows you to manipulate the volume of a device, such as a TV or speakers. You can increase the volume of your device to make sure that a nearby microphone is not able to record your conversation.
- Webcam cover: A webcam cover is a small sliding mechanism that is attached to your webcam. It allows you to cover the webcam and avoid being recorded by it.
- Headphones: Headphones are small speakers which you wear over your ears. With headphones, you can listen to private voice messages and no nearby microphone can record them.
- Sunglasses: Sunglasses are glasses with tinted lenses. By wearing sunglasses, you can prevent your face from being recognized by nearby cameras.

C.2.14 [Questions for Each Mechanism]. Please focus on how the object described above protects your privacy from technical devices, rather than other persons. [Answer options were: Yes, No, and I don't know.]

- I have used the object described above in the past.
- I have used the object described above in the past to protect my privacy from other technical devices.

To what extent do you agree with the following statements. [Answer options were: strongly disagree, disagree, slightly disagree, neither agree nor disagree, slightly agree, agree, and strongly agree]

- If I were to use the object described above, it would be to protect my privacy from other technical devices.
- It is important to me that I own the object described above.
- I am convinced that the object described above protects my privacy from other technical devices.
- If the object described above is not installed by default, I would try install it myself or resort to a similar alternative to protect my privacy from other technical devices.
- I would prefer using a purely digital alternative to the object described above to protect my privacy from other technical devices (e.g. automatically blurring my body/data on camera images, jamming of microphones).

C.2.15 [General Question on Tangible Privacy Mechanisms]. The following questions all refer to the eight privacy mechanisms we presented to you in this questionnaire (voting booth, distance markings, dressing room curtains, PIN-pad privacy shield, remote control, webcam cover, headphones, and sunglasses). Please indicate the degree to which you agree/disagree with the following statements. [Answer options were: strongly disagree, disagree, slightly disagree, neither agree nor disagree, slightly agree, agree, and strongly agree]

- Touching privacy mechanisms can be fun.
- I place more trust in privacy mechanisms that can be touched.
- I feel more confident using a privacy mechanism after touching it.
- Having the object described above nearby makes me aware that my privacy could be invaded.
- Having the object described above nearby makes me consider to use it to protect my privacy.
- It is easy to understand how the presented privacy mechanisms protect my privacy from other technical devices.
- I can easily verify by myself if the presented privacy mechanisms protect my privacy from other technical devices.
- I would prefer using a purely digital alternative instead of the presented privacy mechanisms to protect my privacy from other technical devices (e.g. automatically blurring my body/data on camera images, jamming of microphones).
- I think that the presented privacy mechanisms protect my privacy better from other technical devices than purely digital alternatives.
- I place more trust in the presented privacy mechanisms compared to purely digital alternatives.

C.2.16 Demographics. Finally, a few questions about yourself.

- With which gender do you identify most? [Answer options were: female, male, other, prefer not to say]
- How old are you? I am ... years old.
- What is the highest degree or level of education you have completed? [Answer options were: No schooling completed; Some High School, no diploma; High School; University Entrance Qualification; Professional Education; Bachelor's Degree; Master's Degree; Ph.D. or higher; Other:]
- In which country do you live? Country:
- Which smart devices do you use regularly? Select all the devices you use on a regular basis. [Answer options were: smartphone; smart headphones (i.e., internet-connected or voice controlled); smart watch (e.g., Apple Watch, Samsung Galaxy Watch); tablet; fitness tracker (e.g., FitBit, Koretrak, Garmin); smart digital camera (i.e., internet-connected or voice controlled); smart speaker; smart TV (i.e., internet-connected or voice controlled); current generation gaming console (i.e., internet-connected or voice controlled); smart hub with screen (e.g., Amazon Echo Show, Facebook Portal); smart video doorbell (i.e., internet-connected or voice controlled); smart indoor/outdoor

security cameras (i.e., internet-connected or voice controlled); laptop/desktop PC; smart printer (i.e., internet-connected or voice controlled); smart garage door opener (i.e., internet-connected or voice controlled); smart thermostat (i.e., internet-connected or voice controlled)]

D RESULTS

D.1 Participants'Demographics

Table 9. Table showing the demographics of our participants ($N = 444$) recruited as a representative sample for the US population via Prolific.

gender		age		education	
female	230	mean	46.47	Bachelor's Degree	184
male	206	std	16.14	High School	97
other	5	min	18	Master's Degree	60
prefer not to say	3	max	85	University Entrance Qualification	42
				Professional Education	34
				Ph.D. or higher	13
				Other:	9
				Some High School, no diploma	5

D.2 Perception of Established Tangible Privacy Mechanism

Table 10. This table shows participants' overall feedback on the eight tangible privacy mechanisms.

item		descriptives		
		mean	std	median
EX_use_privacy	If I were to use the object described above, it would be to protect my privacy from other technical devices.	4.51	1.96	5.0
EX_own	It is important to me that I own the object described above.	4.36	1.98	5.0
EX_confidence	I am convinced that the object described above protects my privacy from other technical devices.	4.32	1.91	5.0
EX_alternative	If the object described above is not installed by default, I would try install it myself or resort to a similar alternative to protect my privacy from other technical devices.	3.91	2.01	4.0
EX_preference	I would prefer using a purely digital alternative to the object described above to protect my privacy from other technical devices (e.g. automatically blurring my body/data on camera images, jamming of microphones).	3.31	1.86	3.0

Table 11. Participants' feedback on each tangible privacy mechanism. Participants could select from a 7-point Likert scale ranging from strongly disagree (1) to strongly agree (7).

question	feedback on presented established tangible privacy mechanisms sorted by mean							
EX_use_privacy	sunglasses	remote control	distance markings	headphones	dressing room curtains	voting booth	privacy shield	webcam cover
mean	2.98	3.18	3.91	4.25	5.17	5.29	5.55	5.73
std	1.69	1.82	1.83	1.91	1.73	1.58	1.43	1.4
median	2.0	3.0	4.0	5.0	6.0	6.0	6.0	6.0
EX_own	distance markings	voting booth	privacy shield	dressing room curtains	sunglasses	remote control	webcam cover	headphones
mean	2.98	3.18	3.91	4.25	5.17	5.29	5.55	5.73
std	1.69	1.82	1.83	1.91	1.73	1.58	1.43	1.4
median	2.0	3.0	4.0	5.0	6.0	6.0	6.0	6.0
EX_confidence	sunglasses	remote control	distance markings	headphones	privacy shield	dressing room curtains	voting booth	webcam cover
mean	2.93	3.16	3.39	4.56	4.98	5.01	5.06	5.48
std	1.62	1.69	1.77	1.77	1.62	1.74	1.59	1.5
median	2.0	3.0	3.0	5.0	5.0	6.0	5.0	6.0
EX_alternative	sunglasses	distance markings	remote control	voting booth	privacy shield	dressing room curtains	headphones	webcam cover
mean	3.05	3.11	3.51	3.86	4.14	4.2	4.3	5.11
std	1.7	1.79	1.85	2.02	2.01	2.07	1.9	1.86
median	3.0	3.0	4.0	4.0	4.0	4.0	4.0	6.0
EX_preference	dressing room curtains	voting booth	webcam cover	headphones	privacy shield	sunglasses	remote control	distance markings
mean	2.64	3.02	3.05	3.24	3.35	3.48	3.81	3.86
std	1.72	1.76	1.77	1.75	1.8	1.94	1.89	1.92
median	2.0	2.0	2.0	3.0	3.5	4.0	4.0	4.0

D.3 Euclidean Distances Between Feedback on Different Tangible Privacy Mechanisms

Table 12. Overview of the calculated Euclidean distances between participants' feedback for the eight presented purely tangible privacy mechanisms.

	voting booth	distance markings	dressing room curtains	privacy shield	remote control	webcam cover	headphones
voting booth							
distance markings	2.542						
dressing room curtains	0.655	2.844					
privacy shield	0.611	2.761	0.812				
remote control	3.172	2.024	3.123	3.186			
webcam cover	1.822	3.987	1.468	1.424	3.881		
headphones	2.067	2.967	1.728	1.904	2.079	1.994	
sunglasses	3.346	1.785	3.348	3.481	0.772	4.329	2.603

D.4 Correlations of Standard Scales

Table 13. Overview of Pearson's correlation coefficient between all standard scales.

scale 1	scale 2	correlation
NFT	NFT+	0.963
IUIPC	CFIP	0.805
SeBIS	SA	0.600
ATI	SA	0.418
ATI	SeBIS	0.360
ATI	TIT	0.334
CFIP	SA	0.296
IUIPC	SA	0.287
IUIPC	SeBIS	0.270
CFIP	SeBIS	0.241
CFIP	NFT	0.081
TIT	SA	0.076
CFIP	NFT+	0.065
TIT	NFT+	0.051
TIT	NFT	0.047
IUIPC	NFT+	0.022
IUIPC	NFT	0.018
ATI	CFIP	0.012
TIT	SeBIS	0.007
SA	NFT+	-0.017
SA	NFT	-0.028
ATI	IUIPC	-0.030
ATI	NFT+	-0.046
ATI	NFT	-0.093
SeBIS	NFT+	-0.131
SeBIS	NFT	-0.147
CFIP	TIT	-0.166
IUIPC	TIT	-0.234

D.5 Correlations of Personal Attributes with Properties of Tangible Privacy

Table 14. Overview of Pearson's correlation coefficient between investigated personal attributes and participants' perception of the investigated properties of tangible privacy mechanisms.

	regularly used IoT devices	age	generally used	used to protect privacy	ATI	TIT	SBIS	SA	information privacy concerns	extended need for touch
tangible interaction	0.078	-0.212	0.086	0.275	0.159	0.111	-0.053	0.100	-0.056	0.467
awareness/verification	0.163	-0.117	0.109	0.233	0.202	0.214	0.103	0.209	0.086	0.229
physicalization	-0.0017	-0.198	0.154	0.217	0.156	0.119	0.036	0.029	-0.044	0.068