Privacy & Safety Challenges of On-Body Interaction Techniques

Dañiel Gerhardt
daniel.gerhardt@cispa.de
CISPA Helmholtz Center for Information Security
Saarbrücken, Saarland, Germany

Divyanshu Bhardwaj
divyanshu.bhardwaj@cispa.de
CISPA Helmholtz Center for Information Security
Saarbrücken, Saarland, Germany

Ashwin Ram
ram@cs.uni-saarland.de
Saarland University, Saarland Informatics Campus
Saarbrücken, Saarland, Germany

André Zenner
andre.zenner@dfki.de
Saarland University & DFKI
Saarbrücken, Saarland, Germany

Jürgen Steimle
steimle@cs.uni-saarland.de
Saarland University, Saarland Informatics Campus
Saarbrücken, Saarland, Germany

Katharina Krombholz
krombholz@cispa.de
CISPA Helmholtz Center for Information Security
Saarbrücken, Saarland, Germany

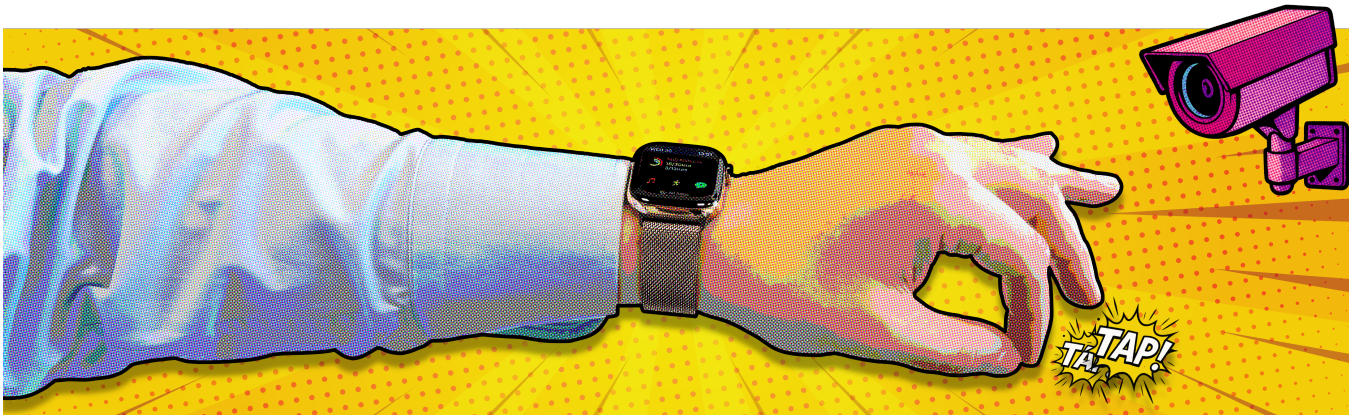

Figure 1: Visualization of an input interaction technique with repeated finger taps observed by CCTV surveillance.

Abstract

On-body computing systems offer new forms of interaction, but while they are increasingly integrated into everyday contexts, their unique privacy and safety challenges remain understudied. This paper examines these challenges through a two-round interview study with $N = 15$ experts in human-computer interaction, and privacy and safety, using speculative scenarios and adversarial roleplaying to elicit insights. Our findings reveal risks specific to on-body interactions, including over-collection of sensitive data, unwanted inferences, harm to bystanders, and threats to bodily autonomy and psychological well-being. Importantly, in the on-body context, privacy and safety concerns are deeply interconnected and cannot be addressed in isolation. We contribute an empirically grounded characterization of these entangled challenges and derive eight actionable design guidelines to support safer, more privacy-aware, on-body systems. This work informs future research and design in ubiquitous computing by highlighting the need for proactive and integrated approaches to privacy and safety in trustworthy on-body computing.

CHI '26, Barcelona, Spain

ACM ISBN 979-8-4007-2278-3/2026/04
https://doi.org/10.1145/3772318.3790403

CCS Concepts

• **Security and privacy** → **Privacy protections**; *Social aspects of security and privacy*; • **Human-centered computing** → **Interaction techniques**; **Empirical studies in HCI**; *Interaction paradigms*; **Interaction design**.

Keywords

On-Body Interaction, Privacy, Safety, Wearable Computing, Design Guidelines, Bystanders

ACM Reference Format:
Dañiel Gerhardt, Divyanshu Bhardwaj, Ashwin Ram, André Zenner, Jürgen Steimle, and Katharina Krombholz. 2026. Privacy & Safety Challenges of On-Body Interaction Techniques. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (CHI '26), April 13–17, 2026, Barcelona, Spain.* ACM, New York, NY, USA, 21 pages. https://doi.org/10.1145/3772318.3790403

1 INTRODUCTION

Advancements in computing technology have led to increasingly intimate interactions between users and devices, resulting in the emergence of on-body computers such as smartwatches, head-mounted displays (HMDs), on-skin interfaces, smart textiles, and other devices that directly interface with users' bodies to facilitate computing tasks. These devices can enable novel, intuitive, and convenient interaction techniques, potentially transforming and

enabling various application domains, from health monitoring to augmented reality experiences.

However, the intimate and personal nature of body-based interactions also amplifies the risks. Potential abuse, unauthorized access, and privacy violations take on greater significance when the technology is worn directly on the body, often for extended periods of time. Despite the growing interest and potential benefits, the privacy and safety implications of interaction techniques accompanying these on-body computing devices remain largely unexplored.

An extensive body of research addresses privacy and safety concerns related to traditional computing platforms, such as desktop PCs, laptops, and smartphones [7, 14, 15, 18, 54]. Prior work has also investigated security and privacy threats for specific mobile and ubiquitous technologies like extended and augmented reality, and smart homes [1, 32, 65], or for particular threats such as shoulder surfing and privacy risks associated with eye-tracking [17, 24].

However, as computing moves onto the body, the context fundamentally changes. The intimate, physical nature of these interactions introduces significant safety risks – spanning physical and psychological harm – that extend beyond the data-centric focus of traditional privacy research.

This paper argues that these two domains are not distinct but are deeply entangled. A privacy breach (e.g., inferring a user's habits or health status) can directly enable a safety risk (e.g., manipulation, psychological distress, or even physical harm). Despite this connection, existing research has rarely focused on safety in this context, nor on the interplay between privacy and safety as co-dependent and interconnected factors.

This paper addresses this gap by exploring the current landscape of privacy and safety challenges for emerging and proposed on-body interaction techniques with experts. Our primary goal is to understand and highlight challenges, threats, and other considerations that designers and developers must account for to ensure user safety and maintain robust privacy protection.

We position this work as an initial mapping of this critical space, providing guidelines that help interaction designers avoid common challenges we identified. Specifically, we pose the following research questions:

RQ1 What privacy and safety challenges do experts identify in on-body interactions?

RQ2 What are actionable guidelines for mitigating common privacy and safety challenges when designing on-body interactions?

To answer these questions, we first performed a comprehensive literature review, identifying and classifying novel interaction techniques proposed in the scientific literature based on regions of the human body. We then interviewed experts in Human-Computer Interaction (HCI) to map the general landscape of privacy and safety concerns associated with these interactions. Informed by insights from the HCI experts, we adapted our interview framework to conduct a deeper exploration with experts specializing in privacy and safety. Utilizing adversarial role-playing exercises, we assessed the interactions through diverse personas and threat layers, uncovering nuanced and sophisticated challenges. We used the insights from both interview rounds to develop actionable guidelines to mitigate common privacy and safety challenges when designing on-body interactions.

Our study identifies a broad spectrum of critical challenges associated with these technologies. Key findings from our expert interviews reveal critical *privacy challenges* spanning problematic data collection practices, data inference capabilities, and bystander privacy issues. Concurrently, we map distinct *safety challenges*, including risks of physical and psychological harm, compromised bystander safety, and threats to user autonomy. We argue that the subtle yet persistent erosion of personal autonomy is a significant and unique danger of on-body technologies resulting from a combination of privacy and safety challenges. A core finding is the deep interplay between these domains, where privacy breaches often directly lead to safety risks, highlighting the uniquely expanded attack surface of on-body computing.

Based on these findings, this paper makes the following contributions:

- An empirically grounded characterization of nuanced privacy and safety challenges associated with emerging on-body interaction techniques, integrating perspectives from both HCI and privacy/safety experts.
- A set of actionable design guidelines aimed at proactively guiding interaction designers in mitigating identified risks and creating trustworthy on-body systems.

This exploratory research provides foundational insights into critical privacy and safety considerations, preparing the research and interaction design communities for the inevitable challenges and opportunities in the age of intimate on-body computing.

2 RELATED WORK

We discuss related work across three key domains. We first examine prior research on privacy in HCI, which establishes the landscape of risks associated with ubiquitous and on-body computing. Next, we discuss the emerging discourse on safety risks, highlighting how the definition of harm is evolving. Finally, we review studies on the critical role of bystanders in the design and deployment of systems that operate in shared, public spaces.

2.1 Privacy in HCI

With the *third wave* of HCI, computing technologies expanded beyond traditional workplaces into diverse aspects of everyday life, including the home, social spaces, and the body itself [22]. While this broad adoption increased access to information, communication, and productivity, it also introduced significant new privacy challenges. In particular, the ubiquitous sensing capabilities of smartphones have increasingly been used to collect extensive data about their users and bystanders, often without their explicit consent or awareness [8].

These privacy issues have only intensified with the emergence of wearable and distributed personal computing devices, such as smartwatches, fitness trackers, and augmented/virtual reality (AR/VR) headsets [11, 41]. Unlike traditional mobile devices, wearables are often always-on, body-mounted, and designed to blend seamlessly into everyday environments, creating new vectors for privacy invasions. Recent work by Wu et al. [62] highlighted that the on-board

sensors on multiple popular VR platforms can be accessed without requiring any user permission, creating an opportunity for adversaries to infer sensitive information, such as keystrokes. Recent research has also highlighted the potential for *dark patterns* in wearable displays, where AR/VR systems can subtly or overtly manipulate a user's perception of reality, influencing their behavior in ways that may not align with their best interests [29].

Furthermore, the public nature of these devices introduces distinct social and visual privacy risks. Prior studies on mobile devices have characterized the prevalence of shoulder surfing [17] and proposed proxemic-aware mechanisms to detect and protect against such visual intrusions [68]. Koelle et al. [26] discussed the need for privacy notices for body-worn cameras and proposed design requirements derived from design sessions with experts.

Despite the growing awareness of privacy risks in wearable technologies, most prior work has predominantly focused on how these concerns relate to passive data collection and sharing practices [10, 38]. Less attention has been given to how emerging wearable systems create privacy risks through the novel interaction mechanisms, including how users provide input to these systems and how, when, and to whom the systems present output. In this paper, we broaden the examination of privacy in on-body computing by investigating the privacy challenges arising from user inputs and system outputs in emerging and future wearable systems, as well as the novel interaction techniques they necessitate.

2.2 Safety Risks in HCI

In this work, we adopt a broad definition of safety, as the term can be interpreted as physical safety or digital security. We define it as ensuring that systems and technologies operate without causing harm to users – both physical and psychological – to data, or infrastructure. We intentionally used this broad definition, adapted from prior work, during our expert interviews to encourage participants to explore a wide range of risks without being prematurely restricted.

Safety has become an increasingly pressing topic in HCI, particularly as technologies grow more immersive and socially embedded. Zheng et al. [67] studied safety risks in VR environments and showed that current safety designs, inherited mainly from traditional platforms, fail to address the VR-specific harms, highlighting a need for specific safety features. Similarly, Wenzel and Kaufman [60] investigated harms experienced by multicultural users interacting with voice assistants and found six physical and emotional harms.

In the physical co-presence domain, O'Hagan et al. [45] conducted in-the-wild interactions in shared spaces between VR users and bystanders, uncovering risks such as collisions, unwanted physical contact, and even abuse. At a broader level, Walker et al. [59] examined the differing definitions of safety across HCI subfields. They argued that a unified, interdisciplinary understanding of safety is necessary to build effective sociotechnical systems, particularly as new technologies emerge.

While this body of work establishes the importance of safety in specific contexts like VR or when using voice assistants, prior research has focused mainly on safety challenges arising from the application or environment, rather than from the fundamental interaction techniques themselves. Our work builds on these foundations by shifting the focus to the interaction modality. We provide a systematic investigation of the physical and psychological safety risks that are intrinsically linked to the act of interacting *on* and *with* the human body.

2.3 Bystanders in Immersive Environments

With the rise of immersive technologies, new challenges arise regarding the presence of bystanders. These technologies extend from the user into the surrounding environment and can inadvertently expose bystanders without their consent. Existing literature has looked into the presence of bystanders and their potential interactions with users in immersive environments.

The study on interactions in shared spaces between VR users and bystanders by O'Hagan et al. [45] also revealed that bystanders often face risks of physical collisions, communication breakdowns, and even abuse due to the occlusive and immersive nature of VR. They highlighted that immersive technologies amplify power imbalances between users and bystanders. In follow-up work [44], they systematically studied user-bystander interactions in VR to understand how VR users manage awareness of bystanders, finding that users' awareness needs are not static but shift depending on social context, interaction type, and the user's desired level of immersion. Extending this into the AR setting, Corbett et al. [9] addressed the challenge of real-time bystander awareness by developing a system that uses users' eye gaze and voice cues to distinguish between users and bystanders.

While prior work has focused on bystanders in immersive interactions, not much work has been done to understand the presence of bystanders when performing on-body interactions. Our paper investigates the dynamics of bystanders in the context of on-body interactions, emphasizing privacy and safety challenges.

3 METHODOLOGY

We designed our methodology to systematically explore the privacy and safety implications of on-body interactions. Based on the results, we derive actionable guidelines to mitigate common challenges when designing future interactions.

The methodology is structured into four distinct phases (see Figure 2): (1) literature analysis and interaction selection, (2) an internal expert workshop, and (3) two rounds of interviews with experts on HCI, as well as experts on privacy and safety (RQ1). Further, (4) we derive guidelines for future interaction designs from our results (RQ2).

3.1 Literature Analysis & Interaction Selection

We conducted an extensive literature review to identify novel interaction techniques applicable to on-body computing devices. We built our initial corpus through keyword searches on the academic databases ACM Digital Library and Google Scholar, focusing on publications from relevant top-tier venues (e.g., CHI, IMWUT, UIST). Our search query strategy involved combining terms related to on-body interaction (e.g., 'input', 'output', 'interaction', 'gesture') with terms for specific body parts (e.g., 'face', 'chest', 'hand', 'leg'). A complete list of the key terms we used is available in Appendix A.

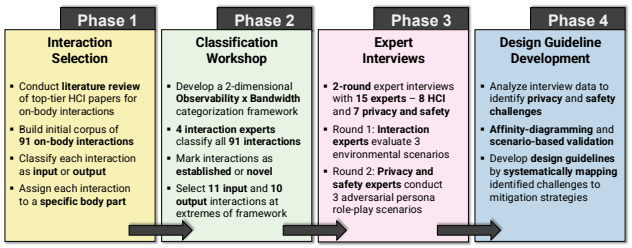

Figure 2: Overview of the four distinct phases of the methodology.

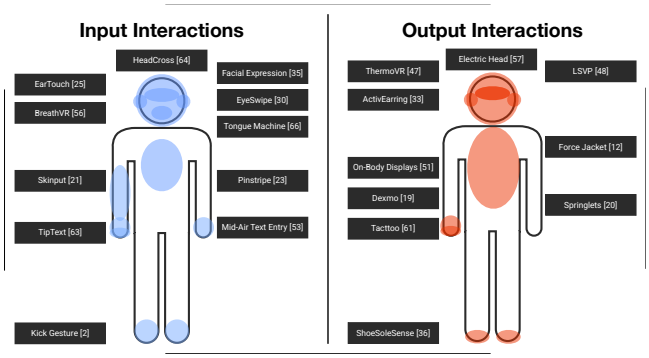

Figure 3: The 11 input and 10 output interaction techniques explored during expert interviews, illustrating their targeted body locations. The input interactions are: EarTouch [25], BreathVR [56], Skinput [21], TipText [63], Kick Gesture [2], HeadCross [64], Facial Expression [35], EyeSwipe [30], Tongue Machine [66], Pinstripe [23], and Mid-Air Text Entry [53]. The output interactions are: ThermoVR [47], ActivEarring [33], On-Body Displays [51], Dexmo [19], Tactitoo [61], ShoeSoleSense [36], Electric Head [57], LSVP [48], Force Jacket [12], and Springlets [20].

We supplemented this initial set by conducting snowball sampling from the reference lists of the already-identified publications. We performed this step to identify works that our keyword search might have missed and to ensure comprehensive coverage of the relevant literature.

To maintain a clear focus, our review concentrated on techniques involving touch and gestural input as well as visual-haptic output, excluding other modalities like voice commands or passive biometric sensing. We gathered 91 distinct interactions from existing literature, classifying them based on their input and output capabilities across different body parts, including hands, torso, head, and legs. This classification considered both the body parts involved in interaction execution (input) and the areas on the body where feedback or output was provided.

Considering the practical time constraints of expert interviews and the goal of in-depth exploration, we curated a representative subset of interactions for discussion through a two-dimensional categorization framework inspired by prior work [49] and internal expert consultations. This framework evaluated interactions across two dimensions:

- **Observability:** the extent to which external observers can perceive an interaction.
- **Bandwidth:** the amount of information (i.e., distinct states or messages) an interaction can convey.

Following this framework, we organized an in-person workshop with 4 internal interaction experts, all researchers holding postdoctoral or faculty positions, from three local research institutions. We deemed this sample size sufficient to ensure agreement on the relatively straightforward classification of interactions into the observability and bandwidth dimensions. All experts have more than 10 years of research experience. They classified each interaction individually based on our dimensions and categorized them as either established or novel based on their adoption in consumer electronics. We noted only minor disagreements during the individual classifications, primarily stemming from slight differences in interpretation of the dimensions. We resolved these disagreements through a short group discussion following the individual classification phase. From the aggregated workshop results, we selected a minimum of 2 and a maximum of 3 interactions representing the extremes of our two-dimensional classification framework for both input and output categories (e.g., selecting at least two interactions that are highly observable with low bandwidth, or classified as low in observability, but high in bandwidth). If the chosen interactions within one quadrant of our classification were conceptually similar, we included only one to avoid excessive memory load on our participants during the interviews. We deliberately chose interactions at the extremes of our classification framework to maximize the elicitation of meaningful insights from our experts. This approach makes potential vulnerabilities more apparent than they might be in more balanced techniques. To ensure diversity, we included not only a mix of established and novel techniques but also interactions targeting different body locations. For example, our experts classified Mid-Air Text Entry [53] as an established technique, and both high in observability and bandwidth. They classified Tongue Machine [66] as novel, and both low in observability and bandwidth. This yielded a total of 11 input and 10 output interactions for further exploration. The interaction techniques used during all expert interviews are listed in Figure 3.

3.2 Expert Interviews

We conducted two sequential rounds of expert interviews to iteratively deepen our understanding of privacy and safety challenges and concerns. We define the term *safety* for our context in Section 2.2. Both interview rounds were performed virtually via Zoom, with audio recordings captured for subsequent analysis.

3.2.1 *First Interview Round: Interaction Experts.*

We conducted the first set of interviews with experts in interaction design and HCI. At the beginning of each interview, we obtained informed consent. Then, we explained the study procedure and presented participants with either the set of input or output interaction techniques using slides and short illustrative videos. Each slide contained a brief text explanation of the technique alongside a

video or illustration taken from the original research paper to visually demonstrate the interaction (see Appendix 4). After explaining each interaction technique, we started an audio recording.

We asked the participants to discuss potential privacy and safety concerns for the interaction techniques we provided. To contextualize their discussion, we guided them through three predefined scenarios:

(1) **Private setting:** The interactions occur in a private space (e.g., at home), with high environmental awareness[1].
(2) **Public setting with high awareness:** The interactions occur in a public environment (e.g., at a bus stop) with high environmental awareness.
(3) **Public setting with low awareness:** The interactions occur in a public environment, but the user's environmental awareness is significantly reduced (e.g., by engaging with a virtual environment).

We purposefully omitted details about the scenarios and implementation of the techniques to avoid constraining the participants' thought processes and encourage them to think creatively. We avoided strict time-boxing, allowing them to explore deeply where insights were especially promising. We presented the techniques as a collective set (input or output) to discuss within the context of each scenario. We dedicated 10 to 15 minutes to each scenario, asking participants to identify general challenges and specific concerns associated with each scenario and interaction, which enabled us to map out the broader threat landscape and identify high-level privacy and safety issues. After completing the scenarios for the first set of techniques, we presented the remaining set and repeated the procedure. Informed by established practices in qualitative research [31], we randomized the order in which we presented the scenarios to experts and alternated the type of interaction technique we discussed first to mitigate fatigue and ordering biases. The full interview guide is provided in Appendix B.

3.2.2 *Second Interview Round: Privacy and Safety Experts.*

Using insights from the first round, we iterated our interview protocol to facilitate a deeper exploration of identified challenges with privacy and safety experts. Although the interactions presented remained unchanged, we shifted our methodological approach to an interactive, adversarial role-playing exercise, a concept central to threat modeling in security and privacy research [52]. We asked the participants to assume one of 3 carefully selected adversarial personas, each representing a distinct threat dimension with differing motives, resources, and potential attack strategies:

- **Profit-driven Corporation:** A systemic threat exploiting data for commercial benefit through large-scale collection and inference (high resources, public context).
- **Abusive Partner:** An intimate threat manipulating personal relationships for control, representing risks to social safety and targeted privacy violations (medium to low resources, private context).
- **Opportunistic Hacker:** A technical threat exploiting interactions for sabotage or personal gain, focusing on system integrity, physical safety, and malicious breaches (medium resources, ad-hoc public context).

This persona-based approach adapts established threat modeling practices for adversarial thinking to explore potential misuse and attacks. It encourages our participants to step outside a defensive or user-centric viewpoint and consider threats from specific, motivated perspectives. To enrich the adversarial thinking process, we introduced our participants to multiple potential threat layers, encouraging them to conceive sophisticated, non-obvious attacks that leverage unique aspects of each interaction type. Unlike in the first round, the scenarios were not examined sequentially; rather, we shifted the focus to detailed challenge exploration per adversarial role for each interaction. After discussing each adversarial persona for the first set of either input or output interaction techniques, we presented the remaining set and repeated the procedure. As this approach is more structured than the previous one, it allowed us to discuss more sophisticated challenges and concerns in the available time. Similar to the first interview round, we randomized the order of the adversarial personas and alternated interaction types to mitigate fatigue and ordering biases informed by established best practices [31]. Across both rounds, interviews lasted 64 minutes on average (SD = 11 min). The full interview guide is provided in Appendix C.

3.2.3 *Recruitment.*

We recruited a total of $N = 15$ experts with $N_{HCI} = 8$ specializing in HCI for the first interview round and $N_{S\&P} = 7$ specializing in safety and privacy (S&P) for the second round. For both rounds of interviews, we recruited experts based on their expertise and publication history in the fields of HCI or privacy and safety. To define our expert criterion, we set a lower-bound requirement of at least one main-author publication at a top-tier venue in their respective field. We consider the ability to publish at such venues a strong indicator of domain expertise. For HCI experts, this included venues such as CHI, IMWUT, and UIST. For S&P experts, this included venues such as IEEE S&P, CCS, USENIX Security, and NDSS. Our participants' professional experience in their respective fields ranged from 4 to 15 years (overall M = 7.2 years). While one top-tier publication was our minimum requirement, all recruited participants exceeded this criterion and had multiple publications in their field.

Experience levels were comparable across the two groups (HCI M = 7.9 years, range: 4-15; S&P M = 6.4 years, range: 4-9). Our final sample consisted of 6 women and 9 men. Further details on participant demographics can be found in Table 1.

Our author team includes researchers from both the HCI and S&P communities, which allowed us to tap into our respective professional networks to identify and recruit suitable experts from each field. We deliberately sampled experts from both communities to achieve interdisciplinary balance. We contacted potential participants individually via email, explaining the purpose of the study and why we selected them. When an expert signed up for an interview, we sent them a consent sheet containing details about the study objectives, data collection and handling.

[1]We use *environmental awareness* to mean a user's degree of perceptual access to their immediate physical surroundings [44]. High awareness implies unobscured real-world senses, low awareness implies senses are largely replaced or mediated, e.g., in immersive VR.

Table 1: Overview of expert participant demographics by expertise area.

ID	Years Exp.	No. Publications	Gender
HCI Experts			
HCI_1	6	9	W
HCI_2	5	11	W
HCI_3	5	2	M
HCI_4	12	30	M
HCI_5	10	12	M
HCI_6	6	9	M
HCI_7	4	11	M
HCI_8	15	12	W
S&P Experts			
$S\&P_1$	9	7	M
$S\&P_2$	5	9	W
$S\&P_3$	8	6	M
$S\&P_4$	6	5	M
$S\&P_5$	9	28	W
$S\&P_6$	4	2	M
$S\&P_7$	4	7	M

3.3 Data Analysis

Our data analysis consisted of two main phases: (1) a systematic analysis of the expert interviews, and (2) the development of design guidelines for interaction techniques.

3.3.1 Thematic Analysis.

We employed a qualitative thematic analysis approach outlined by Braun and Clarke [6] to explore our expert participants' responses. We began by having a GDPR-compliant third-party service produce an orthographic transcript of all interviews, with participants providing consent for this step. Following an inductive, bottom-up approach informed by open coding, two researchers independently coded 7 interviews spanning both expert groups to create the initial codes. They then met to compare their findings, work through any discrepancies, and collaboratively build a single codebook for both interview rounds. They further refined the codebook by resolving variations in code nomenclature and occasional oversights in code application. After confirming that they had no substantive disagreements in their interpretation of the interview content, one researcher applied the refined codebook to the remaining interviews. As coding progressed, the researchers wrote summaries and analytical memos to help organize and track early themes.

We ensured reliability and consistency without calculating inter-rater reliability, with the two primary researchers meeting regularly to discuss the data, mitigate coding drift, and resolve differences until consensus was reached, in line with recommended qualitative practices [3, 37, 46].

After completing all coding, both researchers met again to identify emerging patterns, relationships between codes, and higher-order themes [6, 58].

3.3.2 Guideline Development.

In a subsequent session, two doctoral researchers conducted a workshop to translate the findings from RQ1 into practical design recommendations for RQ2. The process began with a systematic review of every challenge identified by the expert participants. The researchers employed affinity diagramming to synthesize these challenges, clustering them based on their underlying nature and the types of risks they represented. This structured approach enabled them to identify common themes and corresponding mitigation strategies, which formed the basis of an initial set of guidelines.

The researchers primarily derived the mitigation strategies and the resulting actionable guidance from the solutions proposed by the experts during the interviews. This was supplemented by established best practices from prior privacy and safety research, leveraging the researchers' own expertise in these domains.

To ensure the robustness and practical applicability of the guidelines, the researchers then engaged in an iterative refinement process using scenario-based validation exercises. For a given challenge-interaction pair identified by the experts, they would apply the guidelines to conceptually adapt the interaction technique. They would then simulate using this adapted technique within different scenarios to assess whether the guideline effectively mitigated the challenge without introducing new problems. The researchers repeated this validation cycle until the guidelines reached a stable state where they consistently addressed the identified privacy and safety risks without needing further modification.

3.4 Supplementary Materials

We provide supplementary materials for increased transparency and replicability that are available for download. These materials consist of the two expert interview guides, the initial list of representative interaction techniques, and the curated list used for the interviews. It also includes the threat layers shown during interviews, a visual overview of the results from the internal expert workshop, and the codebook used for data analysis.

3.5 Ethical Considerations

All participants provided informed consent before participating. We ensured ethical data handling by anonymizing transcripts and safeguarding sensitive information, adhering strictly to ethical guidelines. Throughout the study, we minimized the collection of personally identifiable information and limited the number of people with access to participant data. We stored and processed all our data in line with the General Data Protection Regulation.

4 RESULTS OF EXPERT INTERVIEWS

We discuss the findings of our expert interviews to identify the privacy and safety challenges associated with the selected on-body interaction techniques. We first examine the privacy challenges related to these techniques, emphasizing issues of data over-collection, data inference, and the privacy of bystanders. Subsequently, we explore the potential safety issues that may arise from these techniques, which include physical and psychological harm, threats to bystander safety, and concerns related to conditioning and control.

4.1 Privacy Challenges

On-body interaction techniques rely on sensors and processors that continuously collect and process data to detect and respond to user input. However, as highlighted by our expert participants, this reliance on pervasive sensing introduces significant privacy challenges. These challenges extend beyond general data collection and include concerns about the excessive gathering of sensitive information, such as biometric and health data, emotional states, and personal habits. They also encompass risks related to unauthorized access to this data and the potential for inferred insights that go far beyond what users knowingly share. The dual-use capabilities of sensors (i.e., serving their intended function and a secondary, often unintended one) and increasingly sophisticated inference techniques further add to these privacy challenges. Moreover, the privacy of bystanders may be affected when these sensors capture data beyond that of the primary user. In the following, we explore the key privacy concerns associated with on-body interactions, focusing on issues related to data over-collection, data inference, and their implications for both user and bystander privacy.

4.1.1 Data Over-Collection.

Many on-body interaction techniques for input rely on extensive amounts of data collected by different sensors. The interactions we discussed with experts incorporate cameras operating in different spectra (such as visible or infrared), motion sensors, bio-acoustic sensors, and EMG sensors, to name a few. Multiple sensors are often incorporated within a single device to enable a given interaction.

While data collection is essential, our participants pointed out that an inherent challenge arises from the fact that these devices often collect more data than is required for their intended purpose, resulting in potential privacy violations. A camera intended to track head movements records everything in its field of view, and a bio-acoustic sensor intended to detect finger taps on the skin can localize taps and other skin interactions beyond a given body area. Additional data collected by such vast arrays of sensors can reveal personal and sensitive information about the user that goes far beyond their intended goal. Our expert participants identified this data over-collection through sensor dual-use as a potential concern. One expert gave an example explaining that an HMD with a built-in accelerometer for head tracking can use the same hardware to track general body movement.

> *"I'm assuming that it uses [...] gyroscopes or something to measure the acceleration of the head. But you can also measure the acceleration of the user himself or herself."* — S&P$_4$

The data gathered *"on-body"* is typically sensitive in nature, encompassing personal medical records, biometric data, and other forms of confidential information. With on-body computing devices becoming more integrated and complex, it can be difficult for users to understand what data is collected and processed and how it is used. Given this lack of understanding, various stakeholders with different motives might be interested in over-collecting data. This includes corporations with monetary interests, malicious actors, and other unauthorized individuals, including friends and family.

While direct observation poses a significant threat, the data collected by on-body devices is also susceptible to more technically sophisticated attacks targeting the data stream and device integrity. As mentioned by our experts, Man-in-the-Middle (MitM) attacks targeting wireless communication links (e.g., Bluetooth) can allow adversaries to intercept or eavesdrop on sensitive sensor data streams.

> *"If you're an active attacker, [...] you can use sensors or [...] you can read the wire or use other channels to observe and attack."* — HCI$_7$

Furthermore, the integrity of the device itself presents critical vulnerabilities. Attackers might compromise devices through malware, supply chain attacks, or firmware manipulation. This could enable hidden data collection backdoors, where devices might alter their data collection behavior when not under audit, making it harder to detect:

> *"When something is audited, you see, okay. This is all fine, all encrypted. [...] And once the audit mode [...] is off, they could still collect the data [...] in secret."* — S&P$_5$

Such compromises could involve sabotaging devices to force unintended data recording or injecting additional covert sensors like GPS or microphones.

Ultimately, the goal of many advanced attacks is the unauthorized extraction and exploitation of sensor data. The experts highlighted risks, including the sale of collected personal data for profit. A significant concern is that this captured data could be used to undermine authentication systems that increasingly rely on behavioral and biometric factors, effectively creating a potential market for stolen biometric profiles or *'Biometrics as a service' offered by hackers.'* [S&P$_5$] The increasing density of sensors also raises concerns about cross-device spying, where *'If one device is malicious/collects a lot of unnecessary data, it could spy on input of other devices nearby.'* [S&P$_4$] The increased amount and sensitivity of collected data, combined with these advanced attack vectors, significantly increase the privacy risks associated with on-body interaction techniques.

4.1.2 Data Inference.

Data from on-body sensors can yield substantial insights into user behavior and preferences, potentially leading to severe privacy violations if such data is accurately inferred. As one expert highlighted, the sensors enabling interaction often allow for much broader interpretation:

> *"So, you're loading the user with a lot of sensors that can be used to not only measure what they are designed to measure, but you can infer more information from that."* — S&P$_4$

Inference mechanisms vary widely, from easily detectable techniques to more discreet and subtle approaches. Similar to data collection, data inference can be carried out by any entity with access to collected sensor data, including corporations seeking commercial advantage, malicious actors, or other unauthorized individuals.

Among the various inference strategies, direct observation attacks stand out as both straightforward and among the most commonly exploited. These include line-of-sight viewing, shoulder surfing, and video recording, all of which can capture user inputs for subsequent replication. The study participants noted that

'Everything like [...] Skinput, or EarTouch [...] and all of that [...] can be easily observed and thus they are not private.' [S&P$_1$] On-body displays are a prime example of observable outputs particularly susceptible to such visual attacks.

More discreet inference techniques leverage side-channel cues such as auditory and vibrational leaks. These may include subtle sounds produced by devices, like one expert noting *'Force Jacket might [...] be audible.'* [S&P$_1$], as well as other minute vibrations, which can disclose the nature of user interactions. Additionally, sophisticated data inference attacks can employ technologies like thermal cameras to detect temperature changes or microphones to discreetly gather data enabling inferences without the user's awareness.

The success of data inference is influenced by the subtlety of user interaction and the situational context. Subtle, low-profile interactions are inherently more challenging to observe and, therefore, less likely to be accurately inferred. The experts frequently cited examples like TipText and Tongue Machine, stating *'[It is] very private because it's not observable.'* [S&P$_1$], enabling covert usage. This contrasts sharply with larger, more expressive interactions. At the same time, public environments inherently elevate the risk of observation attacks, while contexts with low user situational awareness, such as being immersed in the virtual world, further heighten vulnerability due to the user's limited ability to monitor their surroundings. Conversely, in high-awareness settings, users can more strategically time their interactions to mitigate the risk of being observed.

Beyond inferring user's interactions, data inference could reveal various aspects of a person's life, such as health status, emotional state, physical activities, routines, and demographic details. For instance, one expert explained that gait patterns from shoe sensors might reveal daily routines, indoor/outdoor activity, and demographics. This information can enable detailed behavioral profiling and tracking, identifying user habits, preferences, activities, and locations while potentially linking these behaviors to underlying beliefs. Such data could be exploited for purposes like highly targeted advertising, selling user profiles, re-identification, and influencing decisions, all of which raise serious privacy concerns. In more troubling cases, inferred data (e.g., about health conditions or habits like smoking) might even be shared with entities like health insurance companies or placed behind paywalls for financial gain, further harming users.

> *"It's like a premium feature, but here, [...] I would get an advertisement which says 'Hey, you've been diagnosed with something severe. You wanna know what it is? Pay $100.'"* — S&P$_5$

However, it is crucial to acknowledge that data inference is not infallible. The experts cautioned against the risks of over-inference and inaccurate conclusions drawn from sensor data. One participant noted the danger of assuming causality from correlation, especially for sensitive attributes. Such false positives can lead to significant harm, for instance, if data from a borrowed device leads to incorrect assumptions about the primary user's habits or health status.

The privacy risks associated with inference also extend temporally. Some of the experts raised concerns about data hoarding – the practice of collecting sensor data now for potential analysis with more sophisticated algorithms in the future. This temporal dimension means users might consent to data collection without fully understanding the potential future inferences that could be drawn as machine learning techniques advance.

Furthermore, the advanced data collection attacks discussed previously directly exacerbate inference risks. Data intercepted via MitM attacks or extracted from compromised devices provides adversaries with richer, raw sensor feeds, potentially enabling more accurate or invasive inferences than possible through external observation alone. Compromised firmware could even perform complex inferences directly on-device, potentially exfiltrating only the derived sensitive insights rather than raw data, making detection harder.

In summary, data inference transforms raw sensor readings into potentially revealing insights, posing a profound privacy risk. This risk is amplified by the variety of inference methods, the potential for inaccurate conclusions, the prospect of future analysis using advanced techniques, and the underlying vulnerabilities in data collection itself.

4.1.3 Bystander Privacy.

In addition to concerns surrounding the primary user, on-body interaction techniques also raise significant challenges for bystander privacy. Sensors integral to these devices, such as cameras, microphones, or even motion trackers operating within a specific range, may inadvertently capture data about nearby individuals without their knowledge or consent. This presents a distinct and potentially more severe privacy challenge compared to the primary user, who actively chooses to wear the device and is typically aware, at least nominally, of its intended function. Bystanders, in contrast, may be entirely unaware they are being sensed, giving them no opportunity to consent, object, or take evasive action. One HCI expert highlighted how privacy considerations can make the design and implementation of interactions more difficult.

> *"I think that bystanders are worried about being filmed. [...] On the other hand, building input methods or techniques using cameras is super easy."* — HCI$_4$

Consequently, many previously discussed data collection and inference risks – such as excessive data gathering, sensitive inferences, and behavioral profiling – extend beyond the user and also affects the people nearby. Data captured from bystanders could be aggregated and analyzed by various actors. For instance, our experts noted that companies might leverage the sensors on users' devices for dual-use to understand the user and potentially gather data on bystanders, effectively profiling crowds or analyzing public spaces.

Malicious actors could also exploit compromised devices or intercept data streams to spy on conversations or activities involving bystanders, gathering contextual information beyond the primary user. Furthermore, in interpersonal contexts, bystander data can be exploited for surveillance. For example, tracking a primary user's device location can inadvertently reveal the location and movements of their companions. The proliferation of such sensor-equipped devices could enable broader environmental monitoring or even forms of crowd surveillance if data is aggregated centrally or accessed

illicitly by state actors or other powerful entities. While not the focus of the interactions studied, the potential integration of more advanced environmental sensors could intensify these bystander privacy risks in the future.

Summary

On-body interactions rely on various sensors that can pervasively collect extensive, sensitive personal data, enabling inferences far beyond user intent. This inferred information poses significant risks, including behavioral profiling, exploitation, and unforeseen threats from future analysis, while also being susceptible to inaccuracies. Further, on-body devices face advanced technical threats like communication interception, firmware compromise, and illicit data extraction. Additionally, these systems create substantial privacy risks for bystanders by inadvertently capturing their data without their awareness or consent.

4.2 Safety Challenges

Our expert participants noted that the safety implications become increasingly paramount as the interactions move closer to the body. Our analysis additionally revealed that privacy challenges directly influence the potential safety risks associated with on-body interactions.

The experts explained that these safety challenges span both physical and psychological dimensions. In addition, they raised concerns about the safety of bystanders, who may inadvertently be at risk due to their proximity to primary users or the unintended activation of sensors. Furthermore, experts noted that repeated engagement with these systems could gradually influence user behavior, leading to concerns around conditioning and loss of autonomy. In the following sections, we examine these dimensions of safety in more detail, focusing on the broader implications for the well-being of users and bystanders.

4.2.1 Physical Harm.

On-body interaction techniques present physical safety challenges due to their proximity to the body. These risks extend beyond discomfort, potentially escalating to device-induced strain, acute injury, or long-term physical damage.

Interaction-induced physical harm can arise directly from performing on-body gestures or responding to outputs presented on the body. The study participants highlighted that harm can manifest in various forms. Interactions demanding significant user attention, such as responding to complex notifications or following navigation prompts, can lead to dangerous distractions, diverting attention from the immediate environment. This is particularly concerning in high-risk contexts, as one expert explained when talking about LSVP.

> *"It partially obstructs your view, so you need to be careful when there could be some cars or [...] construction work around you."* — HCI_3

The experts also raised concerns about the danger of specific interactions, such as systems relying on precise navigation guidance (e.g., ShoeSoleSense). If such systems provide incorrect or poorly timed cues, they might lead users into hazardous environments. Additionally, the experts noted that sensory overload from multiple haptic, auditory, or visual outputs could further reduce situational awareness and impair judgment.

Interactions requiring large, expressive, or awkward bodily movements introduce musculoskeletal strain or injury risks, especially with prolonged or repetitive use. The study participants frequently noted that the size and nature of gestures impact safety. Large movements like kick gestures increase the likelihood of accidental collisions with surrounding objects or people, particularly when spatial awareness is limited, such as when being immersed in the virtual environment.

> *"The kick gesture could also cause harm, especially if you're in VR because you could be kicking an object or another person [...] this could really hurt yourself or others."* — $S\&P_2$

This lack of awareness can also lead users to trip over or collide with obstacles accidentally. In contrast, smaller, more subtle interactions were generally perceived as physically safer regarding direct motion-related harm.

Hardware issues and device characteristics contribute significantly to physical risks. Due to the proximity to the body, malfunctions or miscalibrations can have severe consequences. The participants expressed concerns about potential burns from thermal output devices, injury from excessive electrical stimulation, restricted blood flow or breathing from constricting wearables, or even hearing damage from poorly regulated audio output.

Beyond accidental harm or standard malfunctions, the experts emphasized the potential for intentional physical harm inflicted through the exploitation of on-body systems. The close integration with the body and the ability of some devices to deliver potent physical stimuli (heat, electricity, force) create a significant attack surface for malicious actors. One expert described a scenario where an attacker threatens physical harm to a user unless demands are met, calling it "ransomware for the body".

> *"If the user is wearing multiple [on-body devices], you can combine a lot of them to send a message. Like, think about ransomware, but for your body."* — $S\&P_4$

In interpersonal contexts, abusive partners with device control could abuse the device's capabilities in a similar way.

The technical vulnerabilities discussed under privacy challenges (Section 4.1) have direct physical safety implications. Attacks like MitM or device compromises (malware, firmware exploitation) could allow adversaries to intercept and modify legitimate commands sent to output devices. For example, a safe level of electrical muscle stimulation could be maliciously amplified to unsafe levels. Similarly, safety limits designed to prevent overheating or excessive force could be deliberately overridden via exploited firmware or compromised components resulting from supply chain attacks.

These findings indicate that physical safety risks associated with on-body interactions can arise from unintended user behavior (e.g., distraction, collisions), design oversights or hardware failures, and intentional exploitation by adversaries leveraging technical vulnerabilities. These risks are compounded as interactions move closer to the body, amplifying the potential physical consequences of failure or misuse.

4.2.2 Psychological Harm.

As on-body interaction techniques become more immersive and tightly integrated with the user's sensory experience, the potential for psychological harm increases significantly.

Our expert participants highlighted several ways interactions can impact mental and emotional well-being. They explained that psychological harm often stems from how users experience and interpret feedback from their bodies. Increased immersion can heighten the emotional impact, leading to fear, anxiety, or discomfort.

> *"[Create] an uncomfortable and fearful situation to control the person. [...] In theory, you can always take the device off, but sometimes [...], even if you know it wasn't real, you have a tricky situation in there. It takes time to adjust."* — S&P$_5$

Another expert provided an example by saying *'[It] could scare me for sure [when] somebody else projects a spider on my body.'* [HCI$_7$] Furthermore, users could face social embarrassment from performing awkward gestures in public or if devices actuate unexpectedly. Such harm may arise unintentionally from system design or be deliberately inflicted by various actors, including corporations leveraging mood influence, attackers, or abusive partners. A participant raised concerns about gaslighting through manipulated outputs, where systems could distort a user's perception of reality in an interpersonal context.

Long-term psychological effects were another primary concern. The participants warned that extended usage could blur the boundaries between real and virtual experiences, making it harder for users to distinguish reality from simulated sensations over time. This might extend beyond visual confusion in VR/AR and potentially include persistent phantom tactile alerts after using haptic devices or difficulty interpreting real-world thermal cues after prolonged exposure to artificial ones. The participants also pointed out that corporate-driven "attention engineering" could impact cognitive functions or brain development, raising concerns about the vulnerabilities of children and adolescents using such technologies.

4.2.3 Bystander Safety.

On-body interaction techniques not only impact the primary user but can also pose risks to the safety of nearby bystanders. Interactions involving large, expressive body movements increase the potential for accidental physical harm to others, notably when users have reduced spatial awareness, for instance, when immersed in virtual reality. Collisions and accidental touching can occur, especially in crowded or constrained environments. One expert described their concern about accidentally touching strangers when using mid-air text entry.

> *"If you really have to reach out for 40 centimeters, I would be afraid to [...] awkwardly [grab] someone else. That would not be safety with regards to 'I hurt someone,' but I inappropriately touched someone."* — HCI$_4$

Conversely, the social perception of on-body interactions can create discomfort or provoke undesired reactions from bystanders, potentially compromising the user's safety. Interactions that appear strange, rude, or confusing may draw negative attention. Bystanders *'might get angry [...] if you behave very weirdly'* [HCI$_7$] when they feel threatened or annoyed observing certain gestures, potentially leading to verbal or even physical confrontation. The novelty of these techniques can intensify such reactions, making users conspicuous and vulnerable, as evidenced by prior experiences with camera glasses and Google Glass [5, 16]. Furthermore, cultural and contextual factors significantly shape bystander reactions, influencing what is considered acceptable interaction.

Beyond physical interactions and social perceptions, device outputs can also impact bystanders. Publicly visible outputs, such as on-body displays or visible augmented reality projections, may expose nearby individuals to unwanted or inappropriate content without their consent. For example, companies might push intrusive advertisements into a bystander's visual field via a user's device. Alternatively, malicious actors could exploit visible outputs to broadcast offensive messages or display disturbing content, creating an uncomfortable or unsafe environment for those nearby.

4.2.4 Conditioning & Control.

Beyond immediate physical or psychological impacts, our expert participants highlighted a distinct category of safety concerns related to conditioning and control. This involves the potential for on-body systems to be used to subtly influence or overtly manipulate user behavior and autonomy, often driven by external actors. While related to psychological effects, this theme focuses specifically on the mechanisms undermining user agency.

The experts worried that repeated exposure to subtle sensory feedback – haptic pulses, gentle electrical stimulation, or thermal cues – could lead to Pavlovian conditioning, gradually shaping user preferences, habits, or even physiological responses, potentially without conscious awareness [50]. This could be exploited commercially. One expert described how a corporation could be interested in guiding user behaviors using such methods, associating positive feelings with specific products or guiding attention via attention engineering that becomes more potent with intimate on-body feedback.

> *"The corporation could maybe have an interest in basically teaching you certain behaviors [...] using these subtle outputs to slowly condition participants. So, this is like the Pavlovian or classical conditioning experiments."* — S&P$_4$

In interpersonal contexts, particularly intimate partner violence (IPV), these mechanisms could be weaponized for control. An abusive partner might exploit device capabilities to condition the victim's responses or directly manipulate their behavior. As described by an expert, this could range from conditioning *'[so] subtle, the target would not be aware of it'* [S&P$_4$] to more overt control.

For example, the ability of some systems to directly actuate the user's body opens possibilities for external control and coercion, not only from partners but also from external actors. While we previously discussed the potential for causing physical harm via such mechanisms (see Section 4.2.1), the ability for an attacker to remotely compel movement or physically constrain the user also fundamentally undermines their autonomy and safety. This enables scenarios akin to the previously mentioned "ransomware for the body", where control itself becomes the leverage or harm.

These concerns about conditioning and control underscore a profound safety risk inherent in tightly coupled on-body systems: the potential erosion of user agency and autonomy through interfaces designed to influence behavior and physiology directly.

Summary

On-body interactions introduce significant safety risks, including direct physical harm from user distraction, collisions, hardware failures, or exploitation, enabling remote attacks like "ransomware for the body." Psychologically, users face potential impact on their mental and emotional well-being. Increased immersion can evoke negative emotional responses such as anxiety or lead to uncomfortable social consequences. Our experts also warned of long-term cognitive impacts blurring the boundaries between real and virtual experiences. Safety concerns extend to bystanders, who are at risk of accidental physical harm and unwanted exposure to visible outputs, while negative bystander reactions can compromise user safety. Further, some systems pose fundamental threats to user autonomy through the potential for subtle behavioral conditioning or direct external control over bodily actions.

5 DESIGN GUIDELINES FOR INTERACTION TECHNIQUES

Drawing from our findings, we propose a set of design guidelines to mitigate the privacy and safety challenges of on-body interaction techniques. The guidelines are grounded in the risks identified by our experts, building upon established privacy and safety principles to address the unique challenges of on-body computing. They are intended to assist interaction designers by directly addressing the challenges detailed in our RQ1 findings (see Sections 4.1 and 4.2).

We recognize that interaction designers may not always have the authority to implement all guidelines, particularly when other stakeholders make core decisions about data collection or business models. In such cases, the guidelines should serve as best practices and be used for advocacy, empowering designers to articulate the importance of responsible design to decision-makers. Maintaining a high level of privacy and safety for users and bystanders serves the long-term interests of all stakeholders.

Previous work expressed concerns regarding the intimacy of biometric data, such as *kinematic fingerprints* [55], and provided recommendations for strict data minimization and anonymization [13]. This guideline emphasizes the need to restrict sensor data capture to the absolute minimum necessary for interaction, based on prior literature and our experts' concerns about over-collection, sensor dual-use, and the sensitivity of on-body data.

G1 Minimize Data Collection

Responsible data governance mitigates privacy risks by deliberately reducing *potential* data capture (via sensor choice) and *actual* data processed. This directly impacts hardware selection, algorithm design (using only necessary data), and data handling architecture (favoring local processing).

Actionable Guidance:

- **Select Minimal Sensors:** Implement only the essential sensor suite capable of reliably enabling the core interaction. Justify the inclusion of each sensor.
- **Configure Minimal Capture:** Operate sensors at the minimum required fidelity, sampling rate, and duration necessary for the interaction. Avoid continuous capture if event-based sensing suffices.
- **Process Locally:** Prioritize on-device or local processing (e.g., on a paired smartphone) to minimize raw sensor data transmission and external exposure where feasible.
- **Enforce Purpose Limitation:** Strictly define and technically enforce the specific purpose(s) for collecting and using data. Prevent function creep [28].
- **Communicate Data Practices:** Clearly inform users about what sensors are active and what data is being collected, processed, or shared (related to G5).

Our participants identified the observability of interactions as a key concern, creating privacy risks through inference and safety risks through negative social attention or misinterpretation. Building on established tenets of tangible interaction [43], this guideline emphasizes the importance of peripheral and discreet interaction styles that allow users to manage privacy without social disruption or unnecessary intrusion [39].

G2 Manage Interaction Observability

Managing interaction perceivability (e.g., visual, auditory, thermal) requires balancing usability and expression against privacy and safety risks. This impacts gesture, output, and form-factor design, as well as context adaptation. While discretion is often key, higher observability may be acceptable for non-sensitive interactions or specific contexts (e.g., gaming) if risks are carefully weighed.

Actionable Guidance:

- **Default to Discretion:** Design for discretion (e.g., micro-gestures, localized haptics) as a default for sensitive inputs/outputs or common public use contexts.
- **Provide Perceivability Control:** Offer clear user controls to manage output perceivability (e.g., haptic intensity, distinct modes for public/private environments).
- **Minimize Side-Channel Leakage:** Reduce unintentional information leakage through side-channels (e.g., noise from actuators, vibrations, or visible heat signatures).
- **Consider Context & Sensitivity:** Explicitly evaluate the trade-offs between observability and function based on the typical use contexts and the sensitivity of the information involved.

Physical safety is paramount due to the intimate proximity of devices. Our findings highlight risks from distraction, accidental harm (including collisions and strain), hardware failures (such as burns and shocks), and intentional attacks. Drawing on established safety

standards for electrical stimulation [27] and risk mitigation strategies for autonomous haptics [40], this guideline mandates strict hardware limits and robust fail-safe mechanisms to prevent injury.

G3 Ensure Physical Safety & Reliability

Preventing physical harm requires validated safety limits, ergonomic design, and rigorous testing due to amplified on-body failure consequences. The criticality of safety measures (like overrides) increases with the device's potential to inflict harm. Choices made for other guidelines interact with physical safety (e.g., less expressive gestures as described in G2), often reducing collision and strain risks. Ensuring safety influences material selection, power management, actuation limits, feedback mechanisms, and failure mode analysis.

Actionable Guidance:

- **Implement Safety Limits:** Enforce and validate strict hardware and software limits (e.g., thermal, electrical, force) appropriate to the harm potential.
- **Include Fail-Safes:** Incorporate context-appropriate and robust fail-safe mechanisms and accessible user overrides (e.g., physical buttons), especially for high-risk devices (e.g., high-powered or body-actuating).
- **Optimize Ergonomics:** Minimize repetitive strain, awkward postures, and collision risks (related to the discretion described in G2).
- **Mitigate Environmental Hazards:** Minimize distraction potential in critical situations. Account for reduced awareness risks (e.g., during VR use).
- **Verify Reliability:** Extensively test system reliability under realistic on-body conditions, verifying safety limits and failure modes of body-interfacing components.

Experts highlighted risks to users' mental and emotional states, ranging from fear and embarrassment to manipulation like gaslighting and long-term concerns like cognitive strain or blurred reality boundaries. Consistent with ethical frameworks for virtual environments, this guideline stresses the need to manage the intensification of experience and potential *reentry* difficulties that blur the distinction between virtual and physical reality [4].

G4 Safeguard Psychological Comfort & Integrity

Protecting psychological integrity requires designing comfortable, non-manipulative interactions respectful of user cognition and emotion. This impacts feedback design (content, modality, intensity), immersion management, and interaction pacing, and it necessitates proactively considering misuse potential for psychological harm.

Actionable Guidance:

- **Prioritize Comfort & Control:** Avoid startling and distressing feedback without explicit user opt-in and providing granular intensity and frequency controls.
- **Ensure Output Clarity & Verifiability:** Design outputs to be clearly interpretable and verifiably linked to system state to reduce confusion and manipulation potential. Provide status indicators.
- **Manage Immersion Effects:** Clearly differentiate simulated and augmented stimuli from reality, where ambiguity could cause distress. Consider potential long-term adaptation effects.
- **Minimize Cognitive Burden:** Avoid unnecessary cognitive load or excessive attentional demands, especially for continuous use or vulnerable users (e.g., children).
- **Consider Misuse Potential:** Anticipate misuse scenarios causing psychological distress (e.g., targeted fear stimuli) and implement preventative design choices or safeguards.

The high complexity of on-body systems and opaque data practices can disempower users, making meaningful control and understanding essential for effectively navigating privacy and safety risks. Frameworks for privacy management emphasize the centrality of both awareness and control, advocating for interactions that are direct, intuitive, and granular to ensure users remain empowered rather than overwhelmed [39].

G5 Empower User Control & Understanding

Trustworthy interaction requires transparent systems that empower users with meaningful agency over device operation, data, and settings. This impacts user interface (UI) design for settings and status, feedback clarity, consent mechanisms, and how system functionality is communicated.

Actionable Guidance:

- **Provide Clear Information:** Offer accessible explanations of system functionality, data practices (related to G1), risks, and settings.
- **Implement Granular Controls:** Design easily discoverable and usable controls for settings, permissions, sharing preferences, and output behavior.
- **Employ Meaningful Consent:** Use contextual, informed, and reversible consent mechanisms for data processing and risky operations. Avoid dark patterns.
- **Enable User Intervention:** Provide accessible ways to interrupt, pause, modify, or override operations, especially in critical contexts (related to G3).

The experts highlighted potential technical vulnerabilities that could severely impact privacy and safety, stressing the need for foundational security. While established cybersecurity principles apply to all information technologies [42], the intimate nature of on-body interactions amplifies the potential severity of adverse events. This guideline emphasizes the necessity of established cybersecurity best practices to safeguard the confidentiality, integrity, and availability of these highly sensitive systems.

G6 Ensure System Security & Integrity

Protecting the system and data requires integrating strong security principles throughout the design, often necessitating collaboration with security and privacy experts. Security impacts architecture, hardware and software choices, communication, authentication, and update strategies.

Actionable Guidance:

- **Secure Communication Channels:** Implement standard, validated security protocols (e.g., authenticated encryption) for all data exchange.
- **Enforce Access Control:** Apply the principle of least privilege. Implement strong authentication/authorization for accessing sensitive data or triggering potentially hazardous functions.
- **Protect Device Integrity:** Employ secure software/firmware development practices, secure updates, and consider hardware security features (e.g., tamper detection) against unauthorized modification.
- **Leverage Hardware Limits:** Incorporate hardware safeguards (e.g., actuator limits) to mitigate the impact of software exploits.
- **Use Appropriate Authentication:** Select user authentication methods suitable for the context, considering usability and threat resistance (e.g., observation, replay).

A distinct concern raised by the experts was the potential for on-body systems to manipulate users intentionally or undermine their autonomy through conditioning or direct control. This guideline focuses on preserving user agency, as immersive technologies can threaten personal autonomy by manipulating emotions and behaviors [43] or inducing a sense of detachment and loss of agency known as depersonalization [55]. Designers must therefore implement safeguards against coercive influences to ensure users remain the authors of their own actions.

G7 Protect User Agency

Respecting user autonomy requires actively designing against coercive or manipulative uses of the technology's influence on perception, physiology, or action. This impacts the design of feedback loops, actuation capabilities, and persuasive elements, and it requires explicit consideration of adversarial manipulation.

Actionable Guidance:

- **Ensure Transparency of Influence:** Any features that influence user behavior (e.g., nudges) must be fully transparent regarding their mechanism and purpose, be opt-in, and easily controllable/disabled.
- **Prevent Unauthorized Control:** Design systems that can control or influence body movements with strong safeguards (see G6) against unauthorized external control. Limit capabilities based on misuse potential.
- **Mitigate Interpersonal Manipulation:** Explicitly consider and mitigate misuse for interpersonal manipulation and control (e.g., conditioning) via technical or UI means (e.g., status indicators, discreet modes).
- **Indicate Subtle Outputs:** Provide salient feedback for system actions, especially subtle outputs (e.g., heating, low-intensity vibration), reducing the potential for unnoticed conditioning.

The experts highlighted that the impacts of on-body technology extend beyond the primary user, affecting bystanders and raising broader ethical questions about misuse and fairness. Addressing these implications requires a proactive ethical perspective that anticipates the *dual use* of technology for malicious purposes [34] and considers the long-term social hazards of widespread adoption [55]. Designers must strive for fairness by evaluating systems against potential biases that could disproportionately affect vulnerable populations [13].

G8 Ensure Ethical & Societal Responsibility

Addressing wider implications, such as responsibilities to non-users and society, requires a broad ethical perspective during design. This impacts decisions about sensor scope (G1), public perceivability of outputs (G2), accessibility, fairness, and anticipating misuse (G4, G7). While minimizing the sensor suite helps reduce the amount of data captured from bystanders, residual risks (e.g., from necessary cameras) must still be managed.

Actionable Guidance:

- **Minimize Impact on Bystanders:** Actively design sensor capture and system operation to minimize unintentional collection of bystander data. Design outputs to avoid exposing non-users to unwanted content or harm.
- **Anticipate & Mitigate Misuse:** Proactively identify potential misuse scenarios during design (e.g., via threat modeling), particularly risks disproportionately affecting vulnerable groups.
- **Maximize Fairness & Accessibility:** Evaluate and mitigate potential biases in sensors, algorithms, or interaction requirements that could create barriers or inequities.

6 DISCUSSION

This paper explored the landscape of privacy and safety challenges associated with emerging on-body interaction techniques through expert interviews. Our findings, detailed in Section 4, reveal a complex interplay of risks demanding careful consideration by designers, developers, and researchers. We position this work as an initial mapping of this critical space, offering foundational guidelines in Section 5 to assist interaction designers navigate the development of future intimate computing technologies.

Shifting Landscape of Computing Risks. As computing technology moves from our desks and pockets directly onto our bodies and integrates deeply with our senses, the potential for harm increases significantly. While privacy concerns associated with excessive data collection have grown over the past decades with regard to mobile computing, our findings suggest that concerns about safety – physical, psychological, and societal – are becoming equally, if not more, important. In this context, safety is not just about preventing devices from causing physical harm. It also means protecting people from being emotionally manipulated, losing control over their bodies, or being pushed into uncomfortable or unwanted experiences. The intimate nature of interactions amplifies the consequences of failure, misuse, or malicious exploitation.

Rethinking Frameworks for On-body Computing. Addressing these challenges requires moving beyond established frameworks. Prior work has laid a crucial foundation, such as investigating privacy on traditional computing platforms [7, 14, 15, 18, 54], exploring safety risks in specific applications like VR [45, 67], and examining bystander privacy in immersive settings [9, 44]. While our findings confirm the continued relevance of these concerns, our expert interviews highlighted that the unique context of on-body interaction demands extending or adapting established frameworks and assumptions. Factors such as continuous body contact, novel sensor modalities capturing intimate physiological or behavioral data, direct bodily actuation, and deeply immersive experiences fundamentally alter the risk landscape.

Crucially, our findings reveal a deep interconnection between privacy and safety. As demonstrated in Section 4, compromising privacy through pervasive data collection and inference directly creates safety threats. Knowledge inferred about a user's habits, emotional state, health, or vulnerabilities can be leveraged to manipulate their behavior, trigger psychological distress, or even facilitate targeted physical harm or control. This link demands approaches that consider privacy and safety not in isolation but as intertwined facets of trustworthy system design.

Expanding Attack Surface. The attack surface for on-body systems is increased compared to conventional devices. The proliferation of cheaper, smaller, and more diverse sensors integrated directly into on-body computers increases the potential avenues for data collection. Our study participants worried that sensors might be included beyond necessity or enabled later without clear user awareness, amplifying risks of over-collection and dual-use.

This extensive data capture fuels increasingly powerful inference capabilities, allowing actors to deduce sensitive information about health, emotions, habits, and identity. This is compounded by the threat of data hoarding for future analysis. Data collected today could yield unforeseen, potentially harmful insights years later as analysis techniques evolve. Combined with technical vulnerabilities, this creates numerous channels through which adversaries – be they corporations, criminals, or state actors – can potentially access, infer from, or exploit highly intimate data, leading to more severe privacy violations and safety harms. These risks are no longer hypothetical but are becoming structurally incorporated into emerging business models. On-body systems must be treated not only as technical systems but also as infrastructure of power and surveillance, requiring a precautionary design stance.

User Burden & Societal Impact. Increasing technological complexity places a significant burden on end-users. As devices become more integrated and data practices more opaque, it becomes questionable whether average users can reasonably be expected to understand the full extent of data collection, potential inferences, vulnerabilities, or long-term consequences of using such technologies. Relying solely on user vigilance, configuration, or consent becomes increasingly untenable. Systems must make their presence and purpose clear to users and those around them.

Further, societal norms and individual ethics, which provide some checks on misuse of technologies like smartphones (e.g., social stigma against constant filming), may prove less effective for on-body devices where sensing can be less conspicuous or even invisible. While ethical use should be encouraged, the primary responsibility for mitigating risks cannot fall solely on the user. It must be embedded within the design process itself.

Proactive & Collaborative Design. Therefore, addressing the multifaceted challenges of on-body interaction necessitates shifting towards proactive, integrated, and interdisciplinary design approaches. Privacy and safety cannot be afterthoughts but must be core considerations from the earliest stages of concept development. Our study with experts highlights the value and necessity of this cross-disciplinary discourse. Effectively navigating the trade-offs between usability, privacy, and safety requires combining expertise in various fields, including interaction design, human factors, security, privacy, and ethics. The guidelines proposed in Section 5 represent a first step in translating the concerns raised by experts into actionable principles intended to support designers in this complex endeavor.

Limitations. While this study provides foundational insights, we acknowledge its limitations and suggest avenues for future research. Our findings are based on a qualitative study with a targeted sample of $N = 15$ experts. We justify the sample size by the significant depth of our participants' expertise (see Section 3.2.3) and by reaching thematic saturation within both the HCI and S&P groups, with final interviews yielding no significantly new high-level challenges. Although their expertise provided rich insights, the perspectives may not fully represent all viewpoints, such as those of industry practitioners or end-users from diverse cultural backgrounds, which tempers the generalizability of our findings.

Furthermore, the scenarios we used in our interviews were intentionally abstract to encourage broad, creative thinking. A limitation of this approach is that the identified risks are speculative and may not capture all the context-specific nuances that would emerge from deploying and observing these interactions in real-world situations.

Finally, our design guidelines were systematically derived from our expert data and validated internally using scenario-based exercises. However, their practical effectiveness and usability when applied by interaction designers have not yet been evaluated. Future work is needed to validate these guidelines in practice and to conduct situated, in-the-wild studies of on-body systems to observe how these privacy and safety challenges manifest and evolve.

7 CONCLUSION

As on-body interaction techniques continue to push interactions closer to the body, they demand a deeper reflection on how privacy and safety are entangled in physical, intimate spaces. Our study reveals that addressing these risks cannot rely on traditional paradigms that separate privacy concerns from safety considerations. Instead, designers must recognize how data privacy, bodily safety, and bystander dynamics converge into a single, expanded threat surface. Our paper outlines this expanded threat surface by empirically bringing all three dimensions together, highlighting their mutual dependencies and offering actionable paths for design. Moving forward, creating trustworthy on-body systems will require more than technical solutions. It will demand a cultural shift toward proactively anticipating harm, accommodating diverse vulnerabilities, and embedding safeguards directly into the interaction techniques. Privacy and safety must be treated as core principles of on-body computing, supported by stronger collaboration and discourse between HCI researchers, and security and privacy experts to ensure that future systems protect users and pave the way for secure on-body interactions.

Acknowledgments

This work would not have been possible without the expert participants who contributed their time and insights. We thank Avian Krämer from CISPA's Scientific Writing and Presentation team for proofreading this paper. Lastly, we thank the anonymous reviewers for their valuable and constructive feedback that substantially improved our paper. This research was funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) - 521601028.

References

[1] Melvin Abraham, Pejman Saeghe, Mark Mcgill, and Mohamed Khamis. 2022. Implications of XR on Privacy, Security and Behaviour: Insights from Experts. In *Nordic Human-Computer Interaction Conference*. ACM. doi:10.1145/3546155.3546691

[2] Jason Alexander, Teng Han, William Judd, Pourang Irani, and Sriram Subramanian. 2012. Putting Your Best Foot Forward: Investigating Real-World Mappings for Foot-Based Gestures. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12)*. Association for Computing Machinery. doi:10.1145/2207676.2208575

[3] Rosaline S. Barbour. 2001. Checklists for Improving Rigour in Qualitative Research: A Case of the Tail Wagging the Dog? *The BMJ* 322, 7294 (2001).

[4] Katharina-Maria Behr, Andreas Nosper, Christoph Klimmt, and Tilo Hartmann. 2005. Some Practical Considerations of Ethical Issues in VR Research. *Presence: Teleoper. Virtual Environ.* 14, 6 (Dec. 2005). doi:10.1162/105474605775196535

[5] Divyanshu Bhardwaj, Alexander Ponticello, Shreya Tomar, Adrian Dabrowski, and Katharina Krombholz. 2024. In Focus, Out of Privacy: The Wearer's Perspective on the Privacy Dilemma of Camera Glasses. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems (CHI '24)*. Association for Computing Machinery. doi:10.1145/3613904.3642242

[6] Virginia Braun and Victoria Clarke. 2006. Using Thematic Analysis in Psychology. *Qualitative Research in Psychology* 3, 2 (2006).

[7] Jeff K. Caird, Kate A. Johnston, Chelsea R. Willness, Mark Asbridge, and Piers Steel. 2014. A Meta-Analysis of the Effects of Texting on Driving. *Accident Analysis & Prevention* 71 (Oct. 2014). doi:10.1016/j.aap.2014.06.005

[8] Erika Chin, Adrienne Porter Felt, Vyas Sekar, and David Wagner. 2012. Measuring User Confidence in Smartphone Security and Privacy. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12)*. Association for Computing Machinery. doi:10.1145/2335356.2335358

[9] Matthew Corbett, Brendan David-John, Jiacheng Shang, Y. Charlie Hu, and Bo Ji. 2023. BystandAR: Protecting Bystander Visual Data in Augmented Reality Systems. In *Proceedings of the 21st Annual International Conference on Mobile Systems, Applications and Services*. ACM. doi:10.1145/3581791.3596830

[10] Enrico Costanza, Samuel A. Inverso, Elan Pavlov, Rebecca Allen, and Pattie Maes. 2006. Eye-q: Eyeglass Peripheral Display for Subtle Intimate Notifications. In *Proceedings of the 8th Conference on Human-computer Interaction with Mobile Devices and Services (MobileHCI '06)*. Association for Computing Machinery. doi:10.1145/1152215.1152261

[11] Prerit Datta, Akbar Siami Namin, and Moitrayee Chatterjee. 2018. A Survey of Privacy Concerns in Wearable Devices. In *2018 IEEE International Conference on Big Data (Big Data)*. doi:10.1109/BigData.2018.8622110

[12] Alexandra Delazio, Ken Nakagaki, Roberta L. Klatzky, Scott E. Hudson, Jill Fain Lehman, and Alanson P. Sample. 2018. Force Jacket: Pneumatically-Actuated Jacket for Embodied Haptic Experiences. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. Association for Computing Machinery. doi:10.1145/3173574.3173894

[13] Sarah Delgado Rodriguez, Radiah Rivu, Ville Mäkelä, and Florian Alt. 2023. Challenges in Virtual Reality Studies: Ethics and Internal and External Validity. In *Proceedings of the Augmented Humans International Conference 2023 (AHs '23)*. Association for Computing Machinery. doi:10.1145/3582700.3582716

[14] Paula Delgado-Santos, Giuseppe Stragapede, Ruben Tolosana, Richard Guest, Farzin Deravi, and Ruben Vera-Rodriguez. 2022. A Survey of Privacy Vulnerabilities of Mobile Device Sensors. *ACM Comput. Surv.* 54, 11s (Sept. 2022). doi:10.1145/3510579

[15] Biruk Demissie, Eniyew Tegegne Bayih, and Alelign Alemu Demmelash. 2024. A Systematic Review of Work-Related Musculoskeletal Disorders and Risk Factors among Computer Users. *Heliyon* 10, 3 (Feb. 2024). doi:10.1016/j.heliyon.2024.e25075

[16] Brian L. Due. 2015. The Social Construction of a Glasshole: Google Glass and Multiactivity in Social Interaction. *PsychNology Journal* 13, 2 (Dec. 2015).

[17] Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding Shoulder Surfing in the Wild: Stories from Users and Observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. Association for Computing Machinery. doi:10.1145/3025453.3025636

[18] Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior. *Computers & Security* 77 (Aug. 2018). doi:10.1016/j.cose.2018.04.002

[19] Xiaochi Gu, Yifei Zhang, Weize Sun, Yuanzhe Bian, Dao Zhou, and Per Ola Kristensson. 2016. Dexmo: An Inexpensive and Lightweight Mechanical Exoskeleton for Motion Capture and Force Feedback in VR. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. Association for Computing Machinery. doi:10.1145/2858036.2858487

[20] Nur Al-huda Hamdan, Adrian Wagner, Simon Voelker, Jürgen Steimle, and Jan Borchers. 2019. Springlets: Expressive, Flexible and Silent On-Skin Tactile Interfaces. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery. doi:10.1145/3290605.3300718

[21] Chris Harrison, Desney Tan, and Dan Morris. 2010. Skinput: Appropriating the Body as an Input Surface. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. Association for Computing Machinery. doi:10.1145/1753326.1753394

[22] Steve Harrison, Deborah Tatar, and Phoebe Sengers. 2007. The Three Paradigms of HCI. *Alt. Chi. Session at the SIGCHI Conference on human factors in computing systems* (2007).

[23] Thorsten Karrer, Moritz Wittenhagen, Leonhard Lichtschlag, Florian Heller, and Jan Borchers. 2011. Pinstripe: Eyes-Free Continuous Input on Interactive Clothing. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. Association for Computing Machinery. doi:10.1145/1978942.1979137

[24] Christina Katsini, Yasmeen Abdrabou, George E. Raptis, Mohamed Khamis, and Florian Alt. 2020. The Role of Eye Gaze in Security and Privacy Applications: Survey and Future HCI Research Directions. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Association for Computing Machinery. doi:10.1145/3313831.3376840

[25] Takashi Kikuchi, Yuta Sugiura, Katsutoshi Masai, Maki Sugimoto, and Bruce H. Thomas. 2017. EarTouch: Turning the Ear into an Input Surface. In *Proceedings of the 19th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '17)*. Association for Computing Machinery. doi:10.1145/3098279.3098538

[26] 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 (TEI '18)*. Association for Computing Machinery. doi:10.1145/3173225.3173234

[27] Michinari Kono, Takumi Takahashi, Hiromi Nakamura, Takashi Miyaki, and Jun Rekimoto. 2018. Design Guideline for Developing Safe Systems That Apply Electricity to the Human Body. *ACM Trans. Comput.-Hum. Interact.* 25, 3 (June 2018). doi:10.1145/3184743

[28] Bert-Jaap Koops. 2021. The Concept of Function Creep. *Law, Innovation and Technology* 13, 1 (Jan. 2021). doi:10.1080/17579961.2021.1898299

[29] Veronika Krauss, Pejman Saeghe, Alexander Boden, Mohamed Khamis, Mark McGill, Jan Gugenheimer, and Michael Nebeling. 2024. What Makes XR Dark? Examining Emerging Dark Patterns in Augmented and Virtual Reality through Expert Co-Design. *ACM Transactions on Computer-Human Interaction* (April 2024). doi:10.1145/3660340

[30] Andrew Kurauchi, Wenxin Feng, Ajjen Joshi, Carlos Morimoto, and Margrit Betke. 2016. EyeSwipe: Dwell-free Text Entry Using Gaze Paths. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. Association for Computing Machinery. doi:10.1145/2858036.2858335

[31] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. 2017. *Research Methods in Human-Computer Interaction* (2 ed.). Morgan Kaufmann.

[32] Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. 2018. Towards Security and Privacy for Multi-user Augmented Reality: Foundations with End Users. In *2018 IEEE Symposium on Security and Privacy (SP)*. doi:10.1109/SP.2018.00051

[33] Minkyeong Lee, Seungwoo Je, Woojin Lee, Daniel Ashbrook, and Andrea Bianchi. 2019. ActivEarring: Spatiotemporal Haptic Cues on the Ears. *IEEE Transactions on Haptics* 12, 4 (Oct. 2019). doi:10.1109/TOH.2019.2925799

[34] Michael Madary and Thomas K. Metzinger. 2016. Real Virtuality: A Code of Ethical Conduct. Recommendations for Good Scientific Practice and the Consumers of VR-Technology. *Frontiers in Robotics and AI* 3 (Feb. 2016). doi:10.3389/frobt.2016.00003

[35] Katsutoshi Masai, Yuta Sugiura, Masa Ogata, Kai Kunze, Masahiko Inami, and Maki Sugimoto. 2016. Facial Expression Recognition in Daily Life by Embedded Photo Reflective Sensors on Smart Eyewear. In *Proceedings of the 21st International Conference on Intelligent User Interfaces (IUI '16)*. Association for Computing Machinery. doi:10.1145/2856767.2856770

[36] Denys J. C. Matthies, Franz Müller, Christoph Anthes, and Dieter Kranzlmüller. 2013. ShoeSoleSense: Proof of Concept for a Wearable Foot Interface for Virtual and Real Environments. In *Proceedings of the 19th ACM Symposium on Virtual Reality Software and Technology (VRST '13)*. Association for Computing Machinery. doi:10.1145/2503713.2503740

[37] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-Rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. In *Proc. CSCW*.

[38] 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 (CHI EA '16)*. Association for Computing Machinery. doi:10.1145/2851581.2892475

[39] 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 (Feb. 2021). doi:10.1145/3430506

[40] Soroosh Mortezapoor, Mohammad Ghazanfari, Khrystyna Vasylevska, Emanuel Vonach, and Hannes Kaufmann. 2025. Safety for Mobile Encountered-Type Haptic Devices in Large-Scale Virtual Reality. *Frontiers in Virtual Reality* 6 (Oct. 2025). doi:10.3389/frvir.2025.1648019

[41] Vivian Genaro Motti and Kelly Caine. 2015. Users' Privacy Concerns About Wearables. In *Financial Cryptography and Data Security*, Michael Brenner, Nicolas Christin, Benjamin Johnson, and Kurt Rohloff (Eds.). Springer. doi:10.1007/978-3-662-48051-9_17

[42] National Institute of Standards and Technology. 2024. *The NIST Cybersecurity Framework (CSF) 2.0*. Technical Report NIST CSWP 29. National Institute of Standards and Technology. doi:10.6028/NIST.CSWP.29

[43] Fiachra O'Brolcháin, Tim Jacquemard, David Monaghan, Noel O'Connor, Peter Novitzky, and Bert Gordijn. 2016. The Convergence of Virtual Reality and Social Networks: Threats to Privacy and Autonomy. *Science and Engineering Ethics* 22, 1 (Feb. 2016). doi:10.1007/s11948-014-9621-1

[44] Joseph O'Hagan, Julie R. Williamson, Florian Mathis, Mohamed Khamis, and Mark McGill. 2023. Re-Evaluating VR User Awareness Needs During Bystander Interactions. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*. Association for Computing Machinery. doi:10.1145/3544548.3581018

[45] Joseph O'Hagan, Julie R. Williamson, Mark McGill, and Mohamed Khamis. 2021. Safety, Power Imbalances, Ethics and Proxy Sex: Surveying In-The-Wild Interactions Between VR Users and Bystanders. In *2021 IEEE International Symposium on Mixed and Augmented Reality (ISMAR)*. doi:10.1109/ISMAR52148.2021.00036

[46] Anna-Marie Ortloff, Matthias Fassl, Alexander Ponticello, Florin Martius, Anne Mertens, Katharina Krombholz, and Matthew Smith. 2023. Different Researchers, Different Results? Analyzing the Influence of Researcher Experience and Data Type During Qualitative Analysis of an Interview and Survey Study on Security Advice. In *Proc. CHI*.

[47] Roshan Lalintha Peiris, Wei Peng, Zikun Chen, Liwei Chan, and Kouta Minamizawa. 2017. ThermoVR: Exploring Integrated Thermal Haptic Feedback with Head Mounted Displays. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. Association for Computing Machinery. doi:10.1145/3025453.3025824

[48] Ashwin Ram and Shengdong Zhao. 2021. LSVP: Towards Effective On-the-go Video Learning Using Optical Head-Mounted Displays. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 5, 1 (March 2021). doi:10.1145/3448118

[49] Stuart Reeves, Steve Benford, Claire O'Malley, and Mike Fraser. 2005. Designing the Spectator Experience. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '05)*. Association for Computing Machinery. doi:10.1145/1054972.1055074

[50] Robert A. Rescorla. 1988. Pavlovian Conditioning: It's Not What You Think It Is. *American Psychologist* 43, 3 (1988). doi:10.1037/0003-066X.43.3.151

[51] Stefan Schneegass, Sophie Ogando, and Florian Alt. 2016. Using On-Body Displays for Extending the Output of Wearable Devices. In *Proceedings of the 5th ACM International Symposium on Pervasive Displays (PerDis '16)*. Association for Computing Machinery. doi:10.1145/2914920.2915021

[52] Adam Shostack. 2014. *Threat Modeling: Designing for Security*. John Wiley & Sons.

[53] Marco Speicher, Anna Maria Feit, Pascal Ziegler, and Antonio Krüger. 2018. Selection-Based Text Entry in Virtual Reality. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. Association for Computing Machinery. doi:10.1145/3173574.3174221

[54] Chad Spensky, Jeffrey Stewart, Arkady Yerukhimovich, Richard Shay, Ari Trachtenberg, Rick Housley, and Robert K. Cunningham. 2016. SoK: Privacy on Mobile Devices – It's Complicated. *Proceedings on Privacy Enhancing Technologies* (2016).

[55] James S. Spiegel. 2018. The Ethics of Virtual Reality Technology: Social Hazards and Public Policy Recommendations. *Science and Engineering Ethics* 24, 5 (Oct. 2018). doi:10.1007/s11948-017-9979-y

[56] Misha Sra, Xuhai Xu, and Pattie Maes. 2018. BreathVR: Leveraging Breathing as a Directly Controlled Interface for Virtual Reality Games. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. Association for Computing Machinery. doi:10.1145/3173574.3173914

[57] Yudai Tanaka, Jun Nishida, and Pedro Lopes. 2022. Electrical Head Actuation: Enabling Interactive Systems to Directly Manipulate Head Orientation. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22)*. Association for Computing Machinery. doi:10.1145/3491102.3501910

[58] Mojtaba Vaismoradi and Sherrill Snelgrove. 2019. Theme in Qualitative Content Analysis and Thematic Analysis. *Forum Qualitative Social Research* 20, 3 (2019).

[59] Ashley Marie Walker, Michael Ann DeVito, Karla Badillo-Urquiola, Rosanna Bellini, Stevie Chancellor, Jessica L. Feuston, Kathryn Henne, Patrick Gage Kelley, Shalaleh Rismani, Renee Shelby, and Renwen Zhang. 2024. "What Is Safety?": Building Bridges Across Approaches to Digital Risks and Harms. In *Companion Publication of the 2024 Conference on Computer-Supported Cooperative Work and Social Computing (CSCW Companion '24)*. Association for Computing Machinery. doi:10.1145/3678884.3681824

[60] Kimi Wenzel and Geoff Kaufman. 2024. Designing for Harm Reduction: Communication Repair for Multicultural Users' Voice Interactions. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems (CHI '24)*. Association for Computing Machinery. doi:10.1145/3613904.3642900

[61] Anusha Withana, Daniel Groeger, and Jürgen Steimle. 2018. Tacttoo: A Thin and Feel-Through Tattoo for On-Skin Tactile Output. In *Proceedings of the 31st Annual ACM Symposium on User Interface Software and Technology (UIST '18)*. Association for Computing Machinery. doi:10.1145/3242587.3242645

[62] Yi Wu, Cong Shi, Tianfang Zhang, Payton Walker, Jian Liu, Nitesh Saxena, and Yingying Chen. 2023. Privacy Leakage via Unrestricted Motion-Position Sensors in the Age of Virtual Reality: A Study of Snooping Typed Input on Virtual Keyboards. In *2023 IEEE Symposium on Security and Privacy (SP)*. doi:10.1109/SP46215.2023.10179301

[63] Zheer Xu, Pui Chung Wong, Jun Gong, Te-Yen Wu, Aditya Shekhar Nittala, Xiaojun Bi, Jürgen Steimle, Hongbo Fu, Kening Zhu, and Xing-Dong Yang. 2019. TipText: Eyes-Free Text Entry on a Fingertip Keyboard. In *Proceedings of the 32nd Annual ACM Symposium on User Interface Software and Technology (UIST '19)*. Association for Computing Machinery. doi:10.1145/3332165.3347865

[64] Yukang Yan, Yingtian Shi, Chun Yu, and Yuanchun Shi. 2020. HeadCross: Exploring Head-Based Crossing Selection on Head-Mounted Displays. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 4, 1 (March 2020). doi:10.1145/3380983

[65] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security and Privacy Concerns with Smart Homes. In *Proceedings of the 13th Symposium on Usable Privacy and Security (SOUPS '17)*.

[66] Qiao Zhang, Shyamnath Gollakota, Ben Taskar, and Raj P.N. Rao. 2014. Non-Intrusive Tongue Machine Interface. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. Association for Computing Machinery. doi:10.1145/2556288.2556981

[67] Qingxiao Zheng, Shengyang Xu, Lingqing Wang, Yiliu Tang, Rohan C. Salvi, Guo Freeman, and Yun Huang. 2023. Understanding Safety Risks and Safety Design in Social VR Environments. *Proc. ACM Hum.-Comput. Interact.* 7, CSCW1 (April 2023). doi:10.1145/3579630

[68] Huiyuan Zhou, Khalid Tearo, Aniruddha Waje, Elham Alghamdi, Thamara Alves, Vinicius Ferreira, Kirstie Hawkey, and Derek Reilly. 2016. Enhancing Mobile Content Privacy with Proxemics Aware Notifications and Protection. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. Association for Computing Machinery. doi:10.1145/2858036.2858232

A Academic Database Keyword Search

We built our initial corpus of interaction techniques by combining terms related to on-body interaction with terms for specific body parts. We conducted keyword searches on the academic databases ACM Digital Library and Google Scholar, focusing on publications from top-tier venues relevant to our research (e.g., CHI, IMWUT, UIST).

We limited our search to paper titles and abstracts to avoid unrelated results that contain our search terms in their main text. We used the following terms to construct our search queries:

- **On-Body Interaction Terms:** input, output, feedback, interaction, interface, gesture, on-body, wearable
- **Body Part Terms:** skin, face, head, forehead, neck, eye, ear, nose, mouth, tongue, lip, teeth, cheek, chin, upper body, chest, back, arm, forearm, elbow, hand, wrist, backhand, palm, fingers, lower body, hip, buttocks, leg, thigh, knee, calf, foot, ankle, heel, toes, full body, whole body, textiles, fabrics, clothing

The following is an example of a search query we used on ACM Digital Library:

```
[[Abstract: input] OR [Title: input] OR
[Abstract: output] OR [Title: output]] AND
[[Abstract: gesture] OR [Title: gesture] OR
[Abstract: interaction] OR [Title: interaction] OR
[Abstract: interface] OR [Title: interface]] AND
[[Abstract: face] OR [Abstract: head] OR
[Abstract: neck] OR [Abstract: eye] OR
[Abstract: ear] OR [Abstract: nose] OR
[Abstract: mouth] OR [Abstract: lip]] AND
[Published in: Proceedings of the CHI Conference on
Human Factors in Computing Systems OR
Proceedings of the ACM on Interactive, Mobile,
Wearable and Ubiquitous Technologies OR
Proceedings of the ACM Symposium on User Interface
Software and Technology]
```

We supplemented the initial set obtained through keyword searches by conducting snowball sampling from the reference lists of the already-identified publications. We performed this step to identify works that our keyword search might have missed and to ensure comprehensive coverage of the relevant literature.

B Expert Interview Guide (Round 1)

B.1 Introduction

Greet participant, **introduce** yourself and introduce the topic: *"Hello, my name is (name). I am a researcher at (institution). Thank you for taking the time for this interview! We are currently looking at privacy and safety problems of interactions with on-body computers.*

This is also what we want to talk to you about in this interview since you are an expert in the field of HCI."

B.2 Consent

If the participant already sent back the consent form, skip this part.

Otherwise, ask the participant if they have read and signed the consent form.

"Have you read and signed the consent form I sent you? If you have any questions about it feel free to ask them now!"

B.3 Procedure Explanation

Explain the study procedure to the participant and answer potential questions.

"What we want to do today is present you with a list of certain interaction techniques with on-body computing devices; some you may already be familiar with, and some are rather novel and only proposed in literature (but not used commercially yet).

We will then give you three scenarios in which we ask you to imagine using these interactions."

"Finally, we ask you to think specifically about potential concerns in regards to privacy and safety that these interactions could suffer from in those scenarios."

"With privacy we broadly mean the discipline of having control over one's personal data and keeping data safe against improper access, theft, or loss.

By safety we are referring to the discipline of ensuring that systems and technologies operate without causing harm to users, data, or infrastructure. This harm can be both physical or psychological. "

"We will do this for a set of input and a set of output interactions. In total, this should take about one hour (+ 15 minutes)."

"We keep the scenarios and instructions somewhat **vague on purpose**. You are allowed (and encouraged) to consider different details and situations yourself.

Please share as much as you want to with us. We appreciate any input no matter how obvious or out there you think it is. There are no right or wrong answers, we only want to hear your perspective!"

B.4 Scenarios & Interactions

[START RECORDING AFTER ASKING FOR CONSENT]

"I will start the recording now if there are no more questions and you're ready!"

Introduce interactions first [go to either INPUT or OUTPUT].

"Let's start by going through the first set of interactions. We chose this set of interactions together with a panel of experts in interactions and privacy. We'll quickly go through them to make sure you understand them all, but you don't need to remember them. We will keep them on-screen while we talk."

"Let us imagine using these interactions in the first/second/third scenario…"

- PRIVATE, AWARE: "a rather private situation, e.g., when you are at home or another private space. Your awareness of reality is high in this scenario meaning you can see and hear the world around you well."

Give a more specific scenario if the participant asks for more context: *"Imagine a situation where you are at home in your apartment in a room by yourself. There are no unknown bystanders, at most someone living with you who you trust or a pet. There are no trivial or obvious ways to observe you by outsiders. You can see and hear everything around you well."*

- PUBLIC, AWARE: "a public setting, e.g., at a bus stop where there might be things happening around you and there might be bystanders. Your awareness of reality is high in this scenario meaning you can see and hear the world around you well."

Give a more specific scenario if the participant asks for more context: *"Imagine a situation where you are at a busy bus stop located on the sidewalk in the city. The bus stop is next to a street with other cars and buses driving past regularly. Other people are waiting at the bus stop, and more are walking past it. There are many bystanders, and you have no control over the people and objects around you. You can see and hear everything around you well."*

- PUBLIC, UNAWARE: "a public setting where there might be things happening around you and there might be bystanders. However, your awareness of reality is low now meaning your senses could be overwritten, e.g., when you are in a virtual world."

Give a more specific scenario if the participant asks for more context: *"Imagine a situation where you are at a busy bus stop located on the sidewalk in the city. The bus stop is next to a street with other cars and buses driving past regularly. Other people are waiting at the bus stop, and more are walking past it. There are many bystanders, and you have no control over the people and objects around you. The difference here is that you are using a virtual reality headset that fully overwrites your visual sense of the real world and also your auditory sense to some degree while you are using the interactions."*

"Please take your time to think and talk to me about potential concerns in regards to privacy and safety that these interactions could suffer from in this scenario. (For example) Is there an interaction that jumps out to you as particularly concerning in regards to privacy and safety?"

NOTE TO INTERVIEWER: We are not concerned with viability, commercialization, or how much participants like interactions. Our sole focus is privacy and safety.

Let the participant talk and ask them follow-up questions or encourage them to think about more interactions and situations.

Move on to the remaining set of interactions: Introduce them, go through scenarios again.

B.5 Farewell

Answer final questions and say goodbye.

"Once again: Thank you so much for taking the time to do this with us and your great insights. This is everything from our side, and if you have any questions, feel free to ask them now. Otherwise, I'll say goodbye and hope to see you in the future!"

C Expert Interview Guide (Round 2)

C.1 Introduction

Greet the participant, **introduce** yourself, and introduce the topic:

"Hello, my name is (name). I am a researcher at (institution). Thank you for taking the time to do this interview! We are currently looking at privacy and safety concerns related to interactions with on-body computers.

This is what we want to talk to you about in this interview since you are an expert in the field of privacy."

C.2 Consent

If the participant already sent back the consent form, skip this part.

Otherwise, ask the participant if they have read and signed the consent form.

"Have you read and signed the consent form I sent you? If you have any questions, feel free to ask them now!"

C.3 Procedure Explanation

Explain the study procedure to the participant and answer potential questions.

Introduction

"What we want to do today is use certain novel interactions with on-body computers to compromise a user's privacy and safety (in a role-playing exercise)." Interaction Techniques

"A core element of everything we discuss today will be 21 interaction techniques with on-body computing devices we curated. We selected these from the scientific literature of the HCI community and divided them into input and output interactions. In this interview, we will go through these two groups separately (to maintain an overview and structure)."

Structure I/O

"As it is necessary to know the interactions and how they work, we will go through one set of them first and then discuss them for a while. After, I will present the second set, and we will discuss those as well."

Procedure Overview

*"The way I want to approach our discussion is by *you* putting yourself in the shoes of a specific adversary, e.g., a profit-driven corporation."*

"I then want you to try to find ways to compromise a user's privacy and/or safety by looking at different threat layers such as technical exploits, social exploits, etc. I will also provide you with certain environments in which to consider these threats."

Privacy/Safety Explained

Explain the **terminology** for privacy and safety.

"With privacy, we broadly mean the discipline of having control over one's personal data and keeping data safe against improper access, theft, or loss."

"By safety, we are referring to the discipline of ensuring that systems and technologies operate without causing harm to users - both physical or psychological, to data, or infrastructure."

Semi-structured Interview

"While we prepared personas, threat layers, and environments for you, you are not required or even asked to always adhere to these. They are mostly meant to guide our conversation but not constrain it."

"After I have presented all interactions, I will assign you an adversary role, and then I want you to discuss how you could compromise the safety and/or privacy of a user in that role using the given interaction techniques. Don't worry, we will have everything you need to know on screen, and you can always ask questions."

Beyond Surface-Level

"One disclaimer before we get started: in this interview, we are trying to identify concerns that go beyond surface-level concerns - like observation attacks or accidental collisions - and instead, we are interested in novel threats that might emerge from the interaction's design itself."

"We encourage you to take your time and think creatively — even if it feels speculative! The goal is to uncover risks that haven't been widely considered yet."

Timeframe

"In total, this meeting is set up to take **about one hour**, but if we end up needing more time and you have time, I would be happy to finish our discussions before concluding."

C.4 Scenarios & Interactions

[START RECORDING AFTER ASKING FOR CONSENT]

Participant is assigned order for Interaction Techniques and Adversary Roles. Adhere to those.

"I will start the recording now if there are no more questions and you're ready!"

Introduce interactions first [go to INPUT or OUTPUT].

"Let's start by going through the first set of interactions. We chose this set of interactions together with a panel of experts in interactions and privacy. We'll quickly go through them to make sure you understand them all, but you don't need to remember them. We will keep them on-screen while we talk."

[PRESENT THE **TECHNIQUES** USING SLIDES, JUMP TO TECHNIQUES TABLE]

Confirm participant understands all interactions. **Answer** potential **questions**.

"Please now assume the role of the following adversarial persona trying to compromise a user's privacy & safety. Take your time to think about potential approaches and concerns that come to your mind."

[PRESENT THE **PERSONA**]

"On the screen, you see different threat layers — so angles you could use to compromise a user — and different environments — so circumstances that change in how public they are and how much awareness you have, e.g., you being inside a virtual world in a public place is different from seeing and hearing the world around you unobstructed in a private place. You can use these threat layers and environments as inspiration, but they may not fully apply to every persona and interaction."

"Let's get started on our discussion. So, considering this persona, how would you go about compromising a user's privacy and/or safety?"

NOTE TO INTERVIEWER: We are not concerned with viability, commercialization, or how much participants like interactions. Our sole focus is privacy and safety.

Let the **participant** talk, ask them follow-up questions, and ensure they go through different ideas and approaches. [max. 10 minutes per persona]

Provide a **different persona** and repeat until all personas were discussed.

Repeat for the remaining set of interactions: Introduce interactions, re-iterate unchanged elements (personas, threat layers, environments).

C.5 Farewell

After going through all interactions and discussing them extensively for every persona.

Answer final questions and say goodbye.

"Once again: Thank you so much for taking the time to do this with us and your great insights. This is everything from our side, and if you have any questions, feel free to ask them now. Otherwise, I'll say goodbye and hope to see you in the future!"

D Examples of Interaction Presentation

We show two examples of how we introduced the on-body interaction techniques to our participants, before discussing them as described in the Methodology (see Section 3).

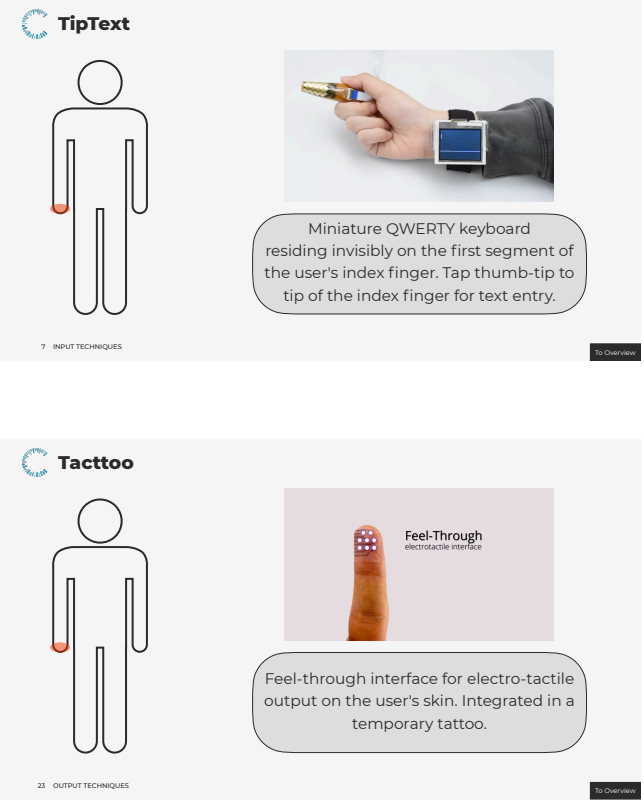

Figure 4: Two examples of how we presented the on-body interaction techniques to participants.