# Beyond LED Status Lights - Design Requirements of Privacy Notices for Body-worn Cameras

**Marion Koelle**
University of Oldenburg
Oldenburg, Germany
marion.koelle@uni-oldenburg.de

**Katrin Wolf**
Hamburg University of Applied Sciences
Hamburg, Germany
katrin.wolf@haw-hamburg.de

**Susanne Boll**
University of Oldenburg
Oldenburg, Germany
susanne.boll@uni-oldenburg.de

**Figure 1. For bystanders it is not always easy to determine whether state-of-the-art body-worn cameras are recording them: some devices, such as Google Glass (left) or the Narrative Clip (2nd from the left) do not provide any status indicator or privacy notice. Other devices, e.g., the Snap's Spectacles (2nd from the right), provide LED indicators. However, those can be easily overlooked, misunderstood, or hidden, e.g., by applying stickers (right).**

## ABSTRACT

Privacy notices aim to make users aware of personal data gathered and processed by a system. Body-worn cameras currently lack suitable design strategies for privacy notices that announce themselves and their actions to *secondary* and *incidental* users, such as bystanders, when they are being used in public. Hypothesizing that the commonly used status LED is not optimal for this use case, due to being not sufficiently understandable, noticeable, secure and trustworthy, we explore design requirements of privacy notices for body-worn cameras. Following a two-step approach, we contribute incentives for design alternatives to status LEDs: Starting from 8 design sessions with experts, we discuss 8 physical design artifacts, as well as design strategies and key motives. Finally, we derive design recommendations of the proposed solutions, which we back based on an evaluation with 12 UX & HCI experts.

## ACM Classification Keywords

H.5.2 User Interfaces: Prototyping; H.5.2 User Interfaces: Style guides; H.5.2 User Interfaces: User-centered Design

## Author Keywords

Augmented Reality; Wearable Cameras; Lifelogging; Privacy



*TEI '18,* March 18–21, 2018, Stockholm, Sweden



ISBN 978-1-4503-5568-1/18/03...$15.00

DOI: https://doi.org/10.1145/3173225.3173234

## INTRODUCTION

The use of personal, body-worn cameras is often problematic and controversial in social situations, as it may cause discomfort and social tension. Recent work discusses bystander privacy that might be compromised by body-worn cameras [10, 12, 17, 27]. In particular, wearable cameras create a different experience for bystanders than camera phones or CCTV cameras because they are considered subtle personal devices that can enable covert recording without consent [12, 55]. As a result of the diminutive form factor, the camera's status cannot be easily inferred from the user's body posture. Thus, bystanders are often not aware they are being captured and subjectively perceive a lack of situation awareness and control.

According to Gurrin et al. [22], an essential aspect of privacy with "always-on" cameras is that bystanders have the right and ability to choose when, where, and by whom they are recorded. Privacy notices in this case are feedback (or feedthrough) [3, 16] mechanisms that make both, primary and secondary users, aware of personal data gathered and processed by a system. While privacy indicators are well researched in the context of HTTPS web browsing [48, 36], state-of-the-art body-worn cameras (c.f. Figure 1) either do not provide any indicators or rely on binary information from point lights (status LEDs) that can be easily overlooked, misunderstood, or hidden.

Non-existent or poor feedback mechanisms are an everyday, practical privacy problem [3, 13] that also deprives bystanders of the possibility to react or possibly object to being captured. Additionally, even though actual device usage might not be a privacy violation as such (e.g., having the camera turned off), the presence of a camera that is (potentially) "always-on" is perceived as a threat to privacy [30]. This has a negative effect on both, the spectator's and the user's social acceptance (c.f. [5, 41]), which can cause the user to avoid using or wearing the camera device, potentially sacrificing its assistive funtion (c.f., [47]). Thus, we base our research on the assumption that privacy notices for body-worn cameras need to deal with the following user (and bystander) concerns:

**Situation Awareness** Is the bystander aware whether a camera device is present? Is (s)he able to verify whether this device is on or off? Does (s)he know what data is being recorded, for what purpose and by whom?

**Justification** Does the device show that I (the user) do not have any dishonest intentions? Does the device communicate when the camera is worn, but not turned on? Does the device communicate when the camera is turned on (e.g., for tracking) but is not persistently storing data?

In addition to potentially conflicting with penal and civil law[1], cameras that facilitate subtle recording violate privacy or privacy-by-design guidelines that demand **Openness** (OECD, [19]), **Notice** [33], or **Visibility and Transparency** [9], such that everyone involved should be able to verify what is captured and how their data[2] is handled. Providing adequate design solutions is a timely issue, as from May 2018 a revision of the EU General Data Protection Directive[3] will obligate manufacturers to implement "privacy-by-design" for both, users and potential bystanders. The directive does not detail how this privacy-by-design requirement shall be achieved. Thus, research in industry and academia will have to fill this gap by providing well thought-out procedures and design strategies.

### Research Goals and Challenges

In order to satisfy the above-mentioned requirements, Openness [19], Notice [33], and Visibility and Transparency [9] for body-worn cameras, two design challenges need to be solved.

**Challenge 1**: Body-worn cameras should announce themselves and their actions in a noticeable, but not too obtrusive way (c.f., Flammer et al. [18]).

Conveying knowledge about usage intentions is not only demanded by existing privacy regulations, but can increase social acceptance [30]. In order to do so, privacy indicators need to show what information is used by the system [15].

**Challenge 2**: Body-worn cameras should publicly communicate their purpose of use to bystanders, but not impair the user's privacy.

Our research goal is to tackle these challenges by contributing to a better understanding of the weaknesses of established design strategies – particularly status LEDs – and by highlighting novel design opportunities. This paper makes two contributions: First, we present eight physical artifacts that embed design strategies addressing the problems *noticeability*, *understandability*, *security*, and *trustworthiness*, and suggest alternatives to LED status lights. They may serve as inspiration or critical designs [14] to spark innovative thinking about privacy notices. Second, we discuss the used design strategies and derive design recommendations for privacy notices and privacy mediating procedures for body-worn cameras.

### Related Work

While there exists an extensive body of literature on privacy notices for *primary users* while browsing the web [48, 36], or using mobile phones [29] or fitness trackers [20], only very few researchers have targeted *secondary users* (e.g., conversation partners) or third party, *incidental users* (e.g., bystanders, c.f. [28]). Systems implementing the negotiation of privacy preferences between device users and bystanders, similar to the "Privacy Dashboard" concept (c.f., [18]) have been presented by Memon et al. [38] and Aditya et al. [1]. Krombholz et al. suggest design guidelines based on three conceptual privacy-mediating technologies, a "privacy bracelet", a "privacy fabric", and a "privacy app" [32]. These conceptual scaffolds were used to better understand bystander privacy risks and explore options to communicate user-defined privacy policies. These systems all require bystanders to own a particular device (e.g., smart phone or token) and to proactively define and communicate their privacy preferences. Although the dissemination of smart phones and BLE devices is increasing, these approaches do not render notification and announcement mechanisms obsolete, as bystanders need to be made aware of potential privacy risks in the first place. Our work aims at closing this gap by investigating privacy notices that announce to the captured person if (s)he is being captured and what the captured data will be used for.

These kinds of announcement mechanisms have been discussed in an early work by Bellotti et al. [3] who proposed design solutions, such as the "confidence monitor" (a public display showing the captured imagery) and visual and audio signals. This work, however, is based on fixed-location cameras in a work environment and does not cover concerns triggered by today's body-worn cameras, e.g., "Is this footage going to be shared on social media?" (c.f., [27, 12]).

Moreover, our work is complementary to Schaub et al.'s [51] who propose a comprehensive design space for effective privacy notices taking into account all possible stakeholders, and account for timing, channel, modality, and control. They further discuss best practices for photo and video lifelogging. Their taxonomy, however, is based on literature research and state-of-the art consumer systems, and thus, limited to existing concepts and technologies. We extend their work by asking experts to develop and critically discuss ideas for novel approaches - that then may be classified according to their taxonomy. Flammer [18] recommends a "Peacock Design" principle where information about a device and a user's actions with it are announced to bystanders. This could be achieved using actuators or physical gestures and signs to replace the current "invisible and unobtrusive" approach. However, they also highlight that announcement mechanisms should not compromise the users' impression management (e.g., being too flashy), which will require novel design solutions. To the best

[1]Legal regulations defining whether a photograph of a person requires his/her consent vary between locales. An overview is provided at http://tinyurl.com/d6b6fco, accessed 12/06/2017

[2]Photographs potentially allow to identify depicted persons, and thus are typically considered as **personal data** under the EU Data Protection Directive 1995 and derived national regulations.

[3]EU GDPD, http://ec.europa.eu/justice/data-protection/reform/index_en.htm, accessed 12/06/2017

of our knowledge, no design strategies other than status LEDs have been suggested so far in literature or applied by industry. With our work we go beyond those conceptional considerations by presenting design artifacts to serve as inspiration or starting points, as well as concrete design recommendations.

### Problem Description

In order to meet any of the above mentioned guidelines, body-worn cameras would require effective announcement mechanisms that indicate (at least) whether the camera in question is recording or idle. It would also be ideal to inform the subject(s) about the intention of the recording and the information being saved. One commonly used design strategy is the use of light indicators (LEDs), which for example, is used by GoPro cameras. Despite being wide-spread and ubiquitously integrated in various types of devices with build-in cameras, this design strategy is not optimal for various reasons.

First, LED status indicators are **not well noticable**. Portnoff et al. [46] were able to show that, when focusing on a primary task unrelated to the recording device, participants were unlikely to notice the webcam indicator light of their computer turning on. They further note that it is particularly challenging to help people notice a LED status indicator when they are in the same room but otherwise occupied. We believe that this also applies to wearable cameras, particularly when there is no direct interaction between the camera user and the bystander.

Second, status LEDs might **not always be fully understood** as they are not mentally linked to the camera [46]. Particularly, when integrated into a novel and unfamiliar device, bystanders might be unsure what a point light indicates [30]. Despite point light displays providing a rich design space, their effectiveness is heavily influenced by learned conventions [24]. Since bystanders are not typically the primary users, they are often unaware of the meaning of a particular point light display. Therefore, colored LED indicators (e.g., red: recording, green: tracking) are unlikely to be optimal solutions.

Third, LED indicator lights are **not secure enough** as they are spoofable - i.e., they can be modified by their primary users to record secretly without signaling the bystanders. While hardware modifications, i.e., removing or de-wiring the LED require technical skills, LED indicators can also simply be masked[4] or painted over. In addition, malicious software might aim to take over the device and secretly record with the status LED turned off. Depending on the actual device's hardware, status LEDs are typically controlled through software, and thus could potentially be deactivated without simultaneously disabling the recording capabilities. Sophisticated counter strategies have been covered by IT Security research [40], but do not provide hundred percent protection. Aiming to prevent software attacks, other devices have the status LED hardwired in the same logical connection as the webcam. However, recent research has shown that attacks on hardwired status LEDs have also been successful [6].

Since LED indicator lights are prone to various kinds of spoofing, they are often perceived as **untrustworthy** from a user's or bystander's point of view. Prior studies have indicated that users are often unsure about the actual mode of operation of the status lights [46], and due to the perceived risk of a security breach, users often cover the camera's lens [34]. In addition, even though actual device usage might not be a privacy violation as such (e.g., having the camera turned off), the presence of a camera that is (potentially) "always-on" is perceived as a threat to privacy: a turned-off indicator light does not entirely eliminate bystander concerns of being recorded [30].

Summing up, LED status lights are not ideal for the design of effective privacy notices for body-worn cameras. Designing effective alternatives is challenging, as they would have to be *noticeable*, *understandable* without prior device-specific knowledge, *secure*, i.e. unspoofable and therefore also both, objectively and subjectively *trustworthy*.

## EXPERIMENT 1: EXPERT DESIGN STUDY

To address the research challenges (1) camera presence and status, and (2) communication of the intention of use, we asked teams of experts to create concepts and design artifacts that support the user's need for *justification* and the bystander's need for *situation awareness*. This approach aims to explore requirements of privacy notices for body-worn cameras, which we believe is essential to reduce the lack of social acceptance of those devices. We do not limit privacy notices to the visual modality, but - following Schaub et al [51] - understand privacy notices as information output of interactive systems using any modality, including audio [31] and haptics [49].

### Experiment Design & Participants

Design solutions developed in participatory design can produce solutions relevant to users' existing needs and desires, but may be less effective at producing innovative ideas that answer users' future or latent needs [50]. In addition, privacy notices are an abstract, non-tangible concept, and body-worn cameras not (yet) widely adopted, which makes it too challenging for non-experts to come up with novel design strategies for privacy notices. Thus, we decided to recruit experts instead of potential users for our experiments.

Working with experts promises not only to involve people that are able to reflect on needs that users are unaware of, experts also know the needs of many users from a survey perspective. Therefore, one expert can bring in the expertise of many users. In consequence, we deemed in-depth design exercises with a limited number of experts more suitable than for the particular design challenge (privacy notices of body-worn cameras) than large scale surveys, and conducted 8 design sessions (2-3h) with 2 expert participants each.

In a successful and complete product design process, iterating through analyzation, design, evaluation and redesign phases requires a lot of time [8]. In contrast, our experiments aim for incomplete, but interesting design artifacts that each address a few perspectives of the complex design challenges described beforehand. There are two reasons for this approach: first, the time frame of a single design session is too short for a fully-developed product. Second, by deliberately aiming for the incomplete and imperfect, we also allow not-fully thought out, not (yet) realizable and exaggerated or visionary ideas to

[4]How to modify & Black out Snapchat Spectacles, https://www.youtube.com/watch?v=GRN3rRqol98, accessed 12/06/2017

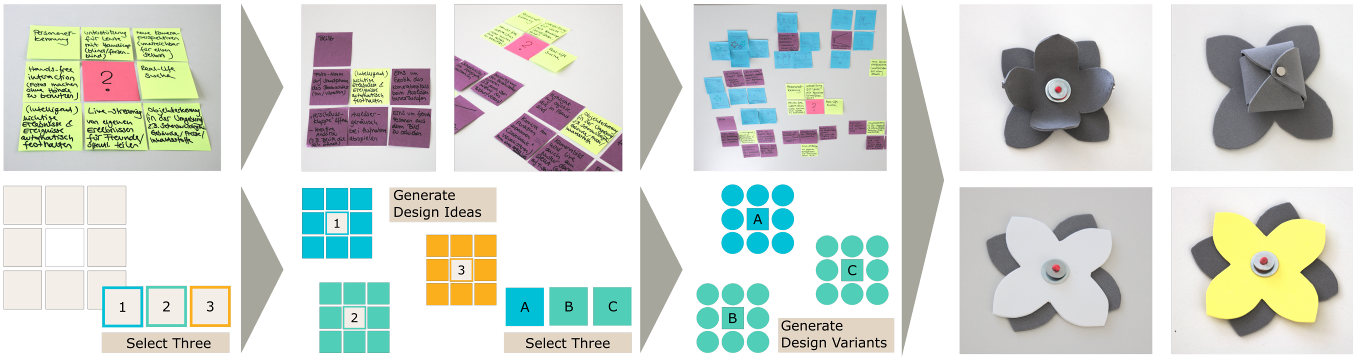



**Figure 2. The design sessions were organized following the Lotus Flower Method: schematic explanation at the bottom, documentation of the design session at the top. [From left to right:] Participants started out from applications that can be enabled with wearable cameras, of which they then selected three. In two subsequent iterations they generated design ideas, selected their three favorites and elaborated on those by designing different variants. Finally, one selected idea was visualized as low-fidelity prototype (here: Prototype A, "Status Flower").**

be part of the created artifacts. Thus, the design artifacts' perspectives are extended towards abstract and creative thinking.

Referring to the constructivism paradigm [21, 52], which assumes that novel solutions are constructed from the learner's (here: expert's) previous knowledge, we expected the potential perspectives on the design challenges to be diverse. Thus we intentionally recruited experts with different research focuses. Each pair of experts contributes one or multiple perspectives on privacy notices of body-worn cameras from which the underlying design strategies are then reconstructed. To more holistically understand strengths and weaknesses of each design strategy, we use the design artifacts created by experts to stimulate a discourse around our research topic [56], which, in our case, is the question how the design of body-worn smart cameras can address *justification* and *situation awareness*. This discourse will be twofold. First, the experts themselves will reflect on their designs, which happens right after they finish the design process. Second, UX experts will analyze the design artifacts, which will be described in greater detail in the section on *Experiment 2: UX Evaluation*.

We conducted 8 design sessions with 2 experts participating in each session as a design team. They were teamed up, as design is usually done in teams, and discussion often fruitfully enforces creativity [2]. To generate design artifacts that embed a wide scope of design perspectives, we recruited design research teams from our community that were covering the following expertise: (1) information retrieval (2) wearable computing (3) shape changing interfaces (4) notifications (5) ambient light displays (6) social context technologies (7) integrated media, and (8) cognitive science. They were recruited from different groups at four universities and one research institute. Our 16 experts (8 females, 8 males) were between 23 and 43 years (mean = 30, SD = 5).

### Procedure & Task

Our design sessions were similarly structured like the design thinking phases [7]. Design thinking could, of course, not fully be applied as the temporal limitation of our sessions did not allow for iteration and readdressing previous phases.

First, tackling the phases *empathy* and *design*, we started with a presentation about the state of the art as well as trends and challenges of current Augmented Reality (AR) smart glasses and body-worn cameras. We also gave an overview of related research and clearly articulated our targeted problems of users' justification and bystanders' situation awareness referring to the work of Portnoff et al. [46]. Summarizing previous work's conclusions, we highlighted that LEDs do neither work for user justification nor for bystanders situation awareness, as they show significant weaknesses regarding *noticeability*, *understandability*, *security*, and *trustworthiness*.

Second, participants were instructed to ideate alternatives in a guided design process, starting from the *ideation* phase. We guided our experts through a 3-step ideation session applying the Lotus Flower Method (see Figure 2). The Lotus Flower Method [39] – or Lotus Blossom Technique [54] – is a method for group brainstorming that originated in the 1990ies. It is a problem-solving approach where each successive step provides a more in-depth look at potential solutions to the problem. Although highly structured, it fosters imagination and innovative thinking while it is at the same time easy to use and explain [25, 26, 53]. Balancing structure and flexibility, the Lotus Flower Method was ideal for our research intentions.

All experts were provided with post-its and pens. Then, using a top-down approach, we asked in step 1 *"What applications can be enabled with wearable smart cameras?"* In step 2, each team selected 3 to 4 applications and answered for them the following question: *"How and where could a smart camera communicate to spectators whether they are being captured and what the images are being used for?"*. In step 3, again 3 ideas should be selected and be brought into the next design level through developing different variations of selected ideas. The focus of that task was on *"How could the UI communicate the application kind and how the camera mode?"* For each step, we reminded the design teams to be aware of all kinds of modalities and to avoid status LEDs.

Third, we arranged a *prototype* phase. Here, each expert team chose one of their ideas generated in step 3 of the *ideation* phase. That idea was then prototyped using a material box equipped with all kinds of materials and making tools inspired by the IDEO's Tech Box[5].

[5]A curated collection of various technologies, materials and mechanisms, source of inspiration when designers are being stuck. C.f., https://tinyurl.com/yayvbpvq, accessed 12/06/2017

Forth, we tackled the Test phase through encouraging our experts to evaluate their prototypes. The experts rated in a 7 item Likert scale *"How well the prototyped idea communicate the camera status?"* as well as *"How well does it communicate the kind of application?"* The ratings were intended to get the experts in the mood of critical reflecting on their ideas. Followed by that, we gathered qualitative feedback through asking for specific design elements of their prototypes. In a semi-structured interview, they were asked to name those elements particularly important/beneficial respectively problematic to situation awareness, and those elements particularly important/beneficial respectively problematic for justification. Sessions lasted 2 to 3 hours. Participants were served with sweets and beverages. There was no monetary compensation.

### Measurements

We recorded the *ideation* phase by photographing the arranged post-its. Results of the *prototype* phase were captured on video and with still images of the prototypes. Ratings and answers of the *test* phase were filled in and saved in Google docs.

## EXPERIMENT 2: UX EVALUATION

Nikander et al. [44] demonstrate that the outcome of concept evaluations tends to be biased, and not objective when designers evaluate a set of designs including their own concepts or ideas. For this reason, we supplement the design team's evaluations of their own prototypes (experiment 1) with a second idea evaluation, where we invited UX and HCI experts that had not taken part in our design session. The major goal of the evaluation was analyzing the meta-concepts underlying the designs from the first session and gather opinions on how well they solve the problems *noticeability*, *understandability*, *security*, and *trustworthiness*. However, as explained above, the generated design artifacts cannot take the place of ready-made product ideas. We understand them as truly subjective, and high-quality perspectives on the research challenges, which – during the design session – became physical artifacts.

### Experiment Design & Participants

We conducted expert interviews aiming to capture a meta-perspective on the generated design strategies and how they target our research challenges (again, rather than aiming for finding a real product design). Hence, we interviewed UX as well as HCI experts and asked them to analyze the design artifacts created in the first experiment. We invited 12 HCI and UX experts (6 m / 6 f), aged 25 to 40 ($M = 30, SD = 4$) who had in average 7 years of experience (SD = 4).

### Procedure, Task & Measurements

There are no established usability principles (heuristics) or evaluation criteria for body-worn or Augmented Reality smart cameras (yet). Nevertheless, general criteria for privacy notices, such as presented by Cranor et al. [11], Dourish et al. [13], and Bellotti et al. [3] are available and had provided the theoretical groundwork for the design requirements that were given to the experts during the first iteration of design sessions. For this reason, we re-used the design requirements and transferred them into open interview questions.

For each of the 8 design artifacts, we prepared a printed A4 design explanation card containing 3-4 pictures and a descriptive text. A short version of the explanations is shown in Table 1. To encourage our interview partners to judge the design artifacts, we asked them for rating each design regarding the pre-defined requirements, e.g. "How noticeable is the camera's status in the described design?". The ratings were measured in a 7 item Likert scale (1: "very poorly" to 7: "very well"). Again, through the provision of a numerical rating, the expert participants should be directed towards re-thinking the concepts and establishing a consolidated opinion, before elaborating. Making a decision about the rating was only used as an "opinion builder" to serve as starting point to reflect on the ideas. Then, in a second step, the participants were asked to explain their rating, which we later used as basis for analysis and discussion. The design artifacts were presented in randomized order. Ratings and interview answers were recorded using Google docs.

## RESULTS

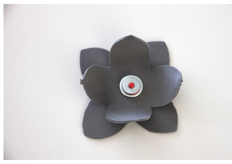
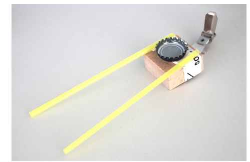
This section jointly presents results of the expert design study (Experiment 1) and the UX evaluation (Experiment 2). Each design team visualized their favorite concept from the ideation phase as a low-fidelity prototype. We denote qualitative statements and ideas by the design teams as "DT". An overview of the resulting prototypes is given in Table 1. The prototypes represent iteratively developed interaction concepts that are made physically using material and low-fi prototyping techniques. As result, we got 8 design artifacts that address the issues previously mentioned with AR and smart cameras. The design artifacts serve as base for identifying design strategies that make AR and smart cams more usable in public.

In addtion to the prototypes, we analyzed the ideas of step 2 and 3 of the *ideation* phase (Lotus Flower) using inductive category development, as suggested by Mayring [37] and extracted design ideas. Then, we compared the developed prototypes amongst each other and to the extracted ideas, and worked out overarching approaches to solve the research problem, that we subsequently present as design strategies.

Discovered design strategies were analyzed qualitatively. We carefully selected suitable qualitative comments from our expert evaluation that help reflecting on the design strategies from a meta-perspective. As explained earlier, the expert rating of the prototypes served as "opinion builder" so that the experts have a starting point from where they can explain their opinion about the ideas. Hence, we selectively report ratings that have clear scoring when describing the design strategies to show what concepts were found most or least promising. Here, we present the design strategies and substantiate them through expert ratings as well as through expert comments (denoted as "E") explaining their critical and promising aspects.

### Physical Occlusion

A concept that, in contrast to software solutions, was rated trustworthy is the occlusion of the camera lens with opaque material (Prototype A & C) which is reflected by the highly rated security (Mdn=6, SD=1.8) and trustworthiness (Mdn=5, SD=1.7) of Prototype A. This idea is inspired by traditional camera lens covers ("irises"), which prevents image capturing even if the software would still be in recording state.

| | Prototype A - DT1 | Prototype B - DT2 | Prototype C - DT3 | Prototype D - DT4 |
|---|---|---|---|---|
| Prototype Depiction |  |  |  |  |
| Short Description | A flower-shaped camera enclosure covers the lens with an opaque material when no recording takes place ("closed bud" metaphor). Different types of recordings (video, still images) are visualized through color changing petals. | The camera device has an embedded printer that displays the captures as physical artifacts. The artifacts also serve as controls that can be used by the bystander to delete the recording or adjust the audience it may be shared to. | A kid's camera shaped as a character with the lens embedded in the eye. Eyelid and ears close when no video/audio is captured ("eyelid" metaphor). The necks tilting angle indicates the angle of vision. | The camera device is projecting a frustum on the floor, indicating what area is being captured. Additionally, icons are projected that indicate the nature of the recording, e.g., video/still images as well as whether (and where) the imagery might be shared. |
| **Design Strategies** | physical occlusion<br>color-coding | transfer of control<br>displayed camera image | physical occlusion<br>indicated angle of vision | indicated angle of vision<br>indicate captured area<br>visible device actions<br>text & icon |

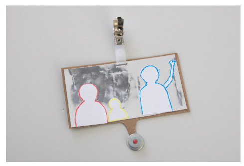
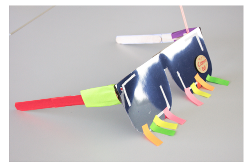
| | Prototype E - DT5 | Prototype F - DT6 | Prototype G - DT7 | Prototype H - DT8 |
|---|---|---|---|---|
| Prototype Depiction |  |  |  |  |
| Short Description | The camera device integrates two icons, one for "analysis only" and one for "persistent storage"/"recording" associated with a color ("red" and "blue") as well as a textual label. The corresponding color is repeated as circling point light on a LED circle surrounding the lens. | The camera device depicts or "mirrors" the camera's view of the scene when the device is turned on. Its image is shown in an abstract way to visualize object or person detection/recognition (here: 3 persons) and where detected entities are located in the field of view. | The camera device (here: glasses) "mirrors" the camera view on its frame and lenses. If a face is recognized, the frame on the glasses front lights up (for the detected bystander to see) and vibrates (for the user to feel the event). | This smart glasses device for blind people acts as normal (dark) sunglasses when turned off. When turned on it shows the camera image on one side and an icon and textual description of the usage intention on the other side. |
| **Design Strategies** | text & icon<br>color-coding<br>visible device actions | displayed camera image<br>visible device actions | displayed camera image<br>visible device actions | text & icon<br>color-coding<br>displayed camera image |

**Table 1. Physical design artifacts created during the design sessions of Experiment 1. Each artifact is presented along with characteristic design strategies obtained from inductive category development and comparative analysis. Further imagery is included with the supplementary material.**

The occlusion ideas show that that approach allows for playfulness and physical design of, for example, a flower metaphor with opening and closing leaflets (Prototype A), or a physical "eye lid" metaphor as used in Prototype C. Both serve to reassure bystanders of what a camera can capture and what is impossible to be recorded through. This effect can also be leveraged by playing around with other physically limiting attributes of the camera, for example the FOV (through tilting the camera or using glare shields or blenders). The simplicity of that concept was very much appreciated by E10 who stated *"Metaphors ... for everybody. With open eyes, you can see, with closed eyes you can't. Same with the direction of the eye."*

### Indicated Capture Area and Angle of Vision

Depicting the camera's frustum in the environment (see Prototype D) leads to high noticeability (Mdn=6, SD=1.6). Variants had been proposed also during the phases of *ideation*, where participants suggested metaphors such as "Aura", "Shine" or "Halo" to indicate capturing angle and distance or projecting an area on the floor. Consequently, if inside the captured frame, a bystander could step out of it knowing where to stand without being captured. While this concept can be easily seen (E3) and is a *"good way of giving context to other people"* (E4), the projector could be masked (E4, 5, 6, 8), and therefore, E12 even *"won't trust the projector operation"*.

### Displayed Camera Image

In their final prototype, four out of eight design teams (DT) suggested to communicate to bystanders what the camera was recording by displaying the camera image (Prototypes B, F, G, H). This strategy follows a "What-you-see-is-what-you-get" approach, as appreciated by E8: *"The device is feeding back what it captures."* In consequence, this strategy becomes very understandable, which is emphasized by the two highest ratings for understandability, the understandable camera status of Prototype H (Mdn=6.5, SD=0.8) as well as of the understandable application purpose of Prototype F and H (F: Mdn=6.5, SD=1.5, H: Mdn=6.5, SD=2.0). Even though displaying the camera image may be intuitive as that method is building on what users know about digital cameras, remote display locations (e.g. on the chest) may be a problem as the connection of the camera and the camera image might not always be obvious:

*"[The prototype] does not really link image and camera on a first glance."* (DT6) Moreover, even though the camera could be recording, *"The display can still be covered if I just put the camera upside down in my shirt pocket."* (E5 about Prototype F) Another problem of this strategy (as of any but the physical occlusion) is a lack of trustworthiness. Experts mention that the device could be capturing even, despite a software controlled display indicating the opposite: *"If the displayed video was paused, it [the camera] could still capture."* (E2) However, E10 noted that *"an abstraction of the image increases the trustworthiness"*, but E8 raised the concern that it was unclear whether *"the raw image [was] saved somewhere?"*.

### Visible Device Actions

While the previously discussed strategy ("displaying the camera image") replicates the captured image, other suggestions aimed to make usage intentions visible to provide a better understanding of what the image will be used for. DT6 suggested, for instance, displaying the result of image processing to both the user and the bystander, through displaying emojis on smart glasses when performing emotion detection to communicate to the bystander which sentiment has been recognized. That would allow to better show what kind of application is used (E1). Further design ideas made use of abstractions (Prototype F, G) to symbolize that objects or persons were detected, e.g., highlighting a "view finder" on successful face recognition. However, this only communicates that something has been recognized but not for what purpose (E11). The proposed solutions have been criticized for a lack of understandability (E8, E9), which could potentially be achieved better using application icons (E2), as explained in the next paragraph.

### Color-coding, Text & Icon

The experts proposed established methods to visualize information, especially concepts that require only little display space, were proposed. Colors can be used to symbolize (or "code") different kinds of stati or meanings. Color-coding of some sort has been used in Prototype A, E and H. However, using color codes is easier to implement than other design strategies, experts have doubts about the understandability of such visualization as, for example, *"Blossom color change / flash does not inform us exactly of what is happening"* (E7). Such concern was already stated from the design team itself when reflecting on their prototype: *"We're not sure whether the glowing, blinking, and steady colour is intuitive."* (DT1)

Textual displays, e.g., "recording" have been suggested in Prototypes E and H, which may be easier to get but hard to read from greater distance. Moreover, various icons or pictograms were proposed to illustrate the camera's status and the purpose of recording, persistence of data storage or the targeted platform for sharing (Prototype D). Although, icons are widely-used, they *"can have different meanings if the audience is not trained for it"* (E11), and hence, *"[i]conic design could be unintuitive"* (DT5). Using well-known icons, e.g., associated with applications (E5) or social media (E6, E8), can communicate what application is accessing the image. Nevertheless, there is some vagueness, e.g., where or to whom social media would share an image (E9, E11), which would require a new consent vocabulary of icons (E5).

### Transfer of Control

During *ideation*, different mechanisms to transfer control over the image to the bystander, were proposed, e.g., using gesture or voice commands such as "camera off" to disable a third party camera. Prototype B suggests to put the bystander in control and to enable him/her to consent (or object) to being recorded, for example, through deleting the image. Alternatively, (s)he can allow the user to share it via a social network. This idea also embodies the notion of a person's ownership of his/her image. While it is difficult to fully control the distribution of digital media, this is truly possible with analog media. Protoype B encapsulates the control into an analog artifact and hands the picture over to the captured person. While this idea lacks in transparency whether the camera is recording or not (E5, E6, E7), and the feedback about the recording might be given too late to be rejected by the bystander (E8), Prototype 2 presents an interesting and truly novel approach for a transfer of control over the image usage from user to bystander. However, experts also noted a lack of trust regarding both, user and used technology: *"I don't trust human beings, and this is a big factor here."* (E10), *"I cannot verify what has been recorded and if the bubble really was pressed."* (E9), The *"camera could still store images."* (E6) However, it is appreciated by E9 that – after handing over the physical control – the captured person can decide about her/his likeness. In summary, experts liked the principle of handing over control, but criticized how this aim was implemented in the Low-Fi prototype.

## DISCUSSION

To derive design recommendations and to close the loop on the evaluation criteria, noticeability, understandability, security, and trustworthiness, presented in the section on *Problem Description*, we discuss how the identified design strategies address the criteria as well as how they relate to previous work.

### Improving Noticeability

Noticeability, i.e., whether user's notice a privacy indicator or not is an important quality criteria [11] of privacy notices. Design strategies that made a device most noticeable were those that display the camera image or the ones indicating the capture area. A reason for the good noticeability of these strategies is surely the visual dominance of the shown content and its well visible placement. In the case of body-worn cameras, its status, e.g, recording, idle, or off, but also the camera's presence and location has to be communicated. The latter fails, if the camera is not recognized as such, as e.g, criticized for Prototype C: *"Having [a] hidden camera is not socially acceptable."* (DT3). On the other hand, privacy notices that merely inform bystanders – e.g., "Warning: CCTV in use" signs or Protoype D's "recording", but do not offer actionable and meaningful choices are not effective [51].

However, procedures or technologies realizing choice of consent or mediation of privacy preferences (c.f., [38, 45]) also need to appropriately notify bystanders of the necessity of choice in the first place. Procedures that ask for consent without prior notice, might satisfy the need for *justification*, but not the need for *situation awareness*. A lack of notice was also criticized by the UX experts: *"It's a Kinder Surprise*[6] *- only*

[6] Popular sweet, a chocolate egg containing a small plastic toy, https://en.wikipedia.org/wiki/Kinder_Surprise, accessed 12/06/2017

*when you have been captured you can choose what you do."* (E7 about Prototype B) While the control card (Prototype B) provided the bystander with control over the captured imagery and the option to withdraw his/her consent to recording, this was only after (s)he had already been recorded. Thus, the request for consent was not coupled with an appropriately timed notice: ideally, consent and notice complement each other.

**Recommendation:** Combine consent and notice in a meaningful way; First notify and make both, user and bystander aware of the situation, then ask for consent.

### Improving Understandability

Bystanders of body-worn cameras encounter them incidentally and potentially without preparation. Hence, privacy notices targeted at bystanders need to be understandable without prior knowledge. Egelman et al. [15] note that a lack of familiarity with e.g., face detection and recognition, video recording and visual tracking, makes it difficult to design distinguishable icons presenting those concepts, which is suggested through the design strategy: visible device action. This is problematic, as according to Moyes et al. "an icon [that] is not guessable it is not necessarily an unsuccessful icon" [42]. In consequence, while icons, related techniques (e.g., earcons [4], and also color codes can be beneficial for primary users that had the opportunity to learn their meaning, they do not achieve the goal of *situation awareness* on the bystanders' side. In addition, they might be inaccessible to users suffering from color blindness. Textual displays can only partially overcome this problem, as the bystander would need to be able to see it under readable conditions (lighting conditions, glare, scale), and understand, both used language and the notices meaning. Metaphors, such as e.g., the "eye lid" (Prototype C), "iris", or "bud" (Prototype A) might be a promising approach, whose effectiveness will have to be proven by future work. Approaches from cinematography [35] could also inspire non-iconic, but simple 2D visualizations of captured regions (c.f., Gustafson et al. [23]), as outlined by Prototype D.

**Recommendation:** Privacy notices targeting bystanders, should avoid any element that has to be known (written language), learned (color codes) or cannot be guessed easily (complex, unfamiliar icons), as well as consider accessibility.

### Improving Security & Trustworthiness

Concerning privacy notices, security and perceived trustworthiness are closely interconnected. However, an unspoofable, i.e., objectively secure technique, is not necessarily perceived as fully trustworthy. A design strategy that can achieve both is to physically block the camera lens. Evidence about webcam covering behavior [34] as well as homemade camera covers[7], suggest that this might be an intuitive and higly trustworthy option (also noted by Bellotti et al. [3]). In the context of body-worn cameras this strategy could act reassuringly by justifying both needs, *situation awareness* and *justification*. However, noticeability and understandability might largely depend on the visual design of the shutter or switch, particularly whether the camera is still recognizable as such.

[7]John Biehler, Google Glass Privacy Cover, https://www.thingiverse.com/thing:182763, accessed 12/06/2017

Shutters and switches, but also any other enabling/disabling function of a body-worn cameras can be operated manually or automatic. Manual operation by the user might be easy to realize, but also prone to human error and dishonesty, as noted during the UX evaluation: *"If you have trustworthy users, the system is trustworthy. Utopia."* (E10 about Prototype B). For this reason, manually disabling a camera might not be predictable enough from a bystander's perspective, as they cannot be sure whether the user will actually remember or be willing to disable the camera, when e.g., entering a public bathroom or swimming pool. Moreover, notifying displays could be deliberately hidden by camera users. Hence, the location of the camera lens and of the notifying display should be at the same position, which ensures that of the display is occluded that lens is occluded as well.

Due to the mistrust in users as outlined above, automatic, software-controlled solutions, e.g., based on sensors[8] that ensure bystander privacy might be preferable. This is a challenge for future research, as they would require sensing procedures that, unlike e.g., microphones, do not infringe with the users privacy and that are robust enough to reliably react to changes regarding the privacy sensitivity of a situation.

**Recommendation:** Privacy notices should provide bystanders with a reassuring mechanism to rule out false positives (recording without indication), and automatically react to privacy sensitive situations in a predictable and reliable way.

### Limitations

With their relatively small scale our studies do not provide a generalizable cross section of opinions. However, we believe that, as stated by Jakob Nielsen [43] that specialists can act as "double experts" with their expertise covering the kind of interface being evaluated, as well as its users, thus providing a survey perspective. Nevertheless, particularly creative or extraordinary solutions might have been missed. On the provision of their informed consent for experiment one, participants were informed that they will be asked to prototype in the end. Thus, they might have been biased towards rejecting concepts that are hard to build, e.g., the "odor emitting camera" (DT6).

## CONCLUSION

LED status lights are an established option to signal whether a wearable camera is recording, but lack *noticeability*, *understandability*, *security* and *trustworthiness*. In this work, we investigated alternative announcement mechanisms in the context of body-worn cameras addressing those problems. From a UX analysis of design strategies based on 8 physical artifacts designed by experts, we derive design recommendations for privacy notices and privacy mediating technologies for body-worn cameras. Providing potential starting points for product design, our recommendations address a timely issue, as the increasing dissemination of wearable consumer cameras and the projected EU legislation (GDPD) demand effective solutions for privacy notices, that realize privacy-by-design and that are acceptable from the perspectives of all stakeholders, including users, bystanders and manufacturers.

[8]Patent for a computing device camera view controller and shutter, https://www.google.com/patents/WO2016090351A1, accessed 12/06/2017

## ACKNOWLEDGMENTS

This work has been supported by the BMBF project ChaRiSma under grant number 16I1665.

## REFERENCES

1. Paarijaat Aditya, Rijurekha Sen, Peter Druschel, Seong Joon Oh, Rodrigo Benenson, Mario Fritz, Bernt Schiele, Bobby Bhattacharjee, and Tong Tong Wu. 2016. I-pic: A platform for Privacy-compliant Image Capture. In *Annual International Conference on Mobile Systems, Applications, and Services (MobiSys)*. ACM, 235–248. DOI:http://dx.doi.org/10.1145/2906388.2906412

2. Ernesto Arias, Hal Eden, Gerhard Fischer, Andrew Gorman, and Eric Scharff. 2000. Transcending the Individual Human Mind – Creating Shared Understanding through Collaborative Design. *ACM Transactions on Computer-Human Interaction (TOCHI)* 7, 1 (2000), 84–113. DOI: http://dx.doi.org/10.1145/344949.345015

3. Victoria Bellotti and Abigail Sellen. 1993. Design for Privacy in Ubiquitous Computing Environments. In *European Conference on Computer-Supported Cooperative Work (ECSCW)*. 77–92. http://dl.acm.org/citation.cfm?id=1241940

4. Meera M Blattner, Denise A Sumikawa, and Robert M Greenberg. 1989. Earcons and Icons: Their Structure and Common Design Principles. *Human–Computer Interaction* 4, 1 (1989), 11–44. DOI: http://dx.doi.org/10.1207/s15327051hci0401_1

5. Stephen Brewster, Roderick Murray-Smith, Andrew Crossan, Yolanda Vasquez-Alvarez, and Julie Rico. 2009. The GAIME project: Gestural and Auditory Interactions for Mobile Environments. *BRIT COMP S* (2009). http://eprints.gla.ac.uk/34242/

6. Matthew Brocker and Stephen Checkoway. 2014. iSeeYou: Disabling the MacBook Webcam Indicator LED. In *USENIX Security*. 337–352. http://dl.acm.org/citation.cfm?id=2671247

7. Tim Brown. 2009. Change by Design. (2009).

8. Tim Brown and Jocelyn Wyatt. 2010. Design Thinking for Social Innovation IDEO. *Development Outreach* 12, 1 (2010), 29–31. DOI: http://dx.doi.org/10.1596/1020-797X_12_1_29

9. Ann Cavoukian. 2009. Privacy by Design – The 7 Foundational Principles. (2009). https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf accessed 12/06/2017.

10. Soumyadeb Chowdhury, Md Sadek Ferdous, and Joemon M Jose. 2016. Bystander Privacy in Lifelogging. In *British Human Computer Interaction Conference*. DOI: http://dx.doi.org/doi:10.14236/ewic/HCI2016.62

11. Lorrie Faith Cranor. 2006. What do they indicate?: Evaluating Security and Privacy Indicators. *Interactions* 13, 3 (2006), 45–47. DOI: http://dx.doi.org/10.1145/1125864.1125890

12. Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. 2014. In situ with Bystanders of Augmented Reality Glasses: Perspectives on Recording and Privacy-mediating Technologies. In *Conference on Human Factors in Computing Systems (CHI)*. ACM, 2377–2386. DOI: http://dx.doi.org/10.1145/2556288.2557352

13. Paul Dourish, E. Grinter, Jessica Delgado de la Flor, and Melissa Joseph. 2004. Security in the Wild: User Strategies for Managing Security As an Everyday, Practical Problem. *Personal Ubiquitous Comput.* 8, 6 (Nov. 2004), 391–401. DOI: http://dx.doi.org/10.1007/s00779-004-0308-5

14. Anthony Dunne and Fiona Raby. 2001. *Design Noir: The Secret Life of Electronic Objects*. Birkhauser.

15. Serge Egelman, Raghudeep Kannavara, and Richard Chow. 2015. Is This Thing On?: Crowdsourcing Privacy Indicators for Ubiquitous Sensing Platforms. In *Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 1669–1678. DOI: http://dx.doi.org/10.1145/2702123.2702251

16. Barrett Ens, Tovi Grossman, Fraser Anderson, Justin Matejka, and George Fitzmaurice. 2015. Candid interaction: Revealing hidden mobile and wearable computing activities. In *Annual ACM Symposium on User Interface Software & Technology (UIST)*. ACM, 467–476. DOI:http://dx.doi.org/10.1145/2807442.2807449

17. Md Sadek Ferdous, Soumyadeb Chowdhury, and Joemon M Jose. 2017. Analysing Privacy in Visual Lifelogging. *Pervasive and Mobile Computing* (2017). DOI:http://dx.doi.org/10.1016/j.pmcj.2017.03.003

18. Ivo Flammer. 2016. Genteel Wearables: Bystander-Centered Design. *IEEE Security & Privacy* 14, 5 (2016), 73–79. DOI: http://dx.doi.org/10.1109/MSP.2016.91

19. Organisation for Economic Co-operation and Development. 2013. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. OECD Publishing. http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=114&InstrumentPID=312&Lang=en accessed 12/06/2017.

20. Joshua Gluck, Florian Schaub, Amy Friedman, Hana Habib, Norman Sadeh, Lorrie Faith Cranor, and Yuvraj Agarwal. 2016. How Short Is Too Short? Implications of Length and Framing on the Effectiveness of Privacy Notices. In *Symposium on Usable Privacy and Security (SOUPS)*. https://www.usenix.org/node/197281

21. Egon G Guba, Yvonna S Lincoln, and others. 1994. Competing Paradigms in Qualitative Research. *Handbook of Qualitative Research* 2, 163-194 (1994).

22. Cathal Gurrin, Rami Albatal, Hideo Joho, and Kaori Ishii. 2014. A Privacy by Design Approach to Lifelogging. *Digital Enlightenment Yearbook* (2014), 49–73. http://doras.dcu.ie/20505/

23. Sean Gustafson, Patrick Baudisch, Carl Gutwin, and Pourang Irani. 2008. Wedge: Clutter-free Visualization of off-screen Locations. In *Conference on Human Factors in Computing Systems (CHI)*. ACM, 787–796. DOI: http://dx.doi.org/10.1145/1357054.1357179

24. Chris Harrison, John Horstman, Gary Hsieh, and Scott Hudson. 2012. Unlocking the Expressivity of Point Lights. In *Conference on Human Factors in Computing Systems (CHI*. ACM, 1683–1692. DOI: http://dx.doi.org/10.1145/2207676.2208296

25. James M Higgins. 1994. *101 creative problem solving techniques: The handbook of new ideas for business*. New Management Publishing Company.

26. James M Higgins. 1996. Innovate or evaporate: creative techniques for strategists. *Long Range Planning* 29, 3 (1996), 370–380.

27. Roberto Hoyle, Robert Templeman, Steven Armes, Denise Anthony, David Crandall, and Apu Kapadia. 2014. Privacy Behaviors of Lifeloggers using Wearable Cameras. In *International Joint Conference on Pervasive and Ubiquitous Computing (Ubicomp)*. ACM, 571–582. DOI:http://dx.doi.org/10.1145/2632048.2632079

28. Giovanni Iachello, Khai N Truong, Gregory D Abowd, Gillian R Hayes, and Molly Stevens. 2006. Prototyping and Sampling Experience to Evaluate Ubiquitous Computing Privacy in the Real World. In *Conference on Human Factors in Computing Systems (CHI)*. ACM, 1009–1018. DOI: http://dx.doi.org/10.1145/1124772.1124923

29. Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. 2013. Privacy as Part of the App Decision-making Process. In *Conference on Human Factors in Computing Systems (CHI)*. ACM, 3393–3402. DOI: http://dx.doi.org/10.1145/2470654.2466466

30. Marion Koelle, Matthias Kranz, and Andreas Möller. 2015. Don't look at me that way!: Understanding User Attitudes Towards Data Glasses Usage. In *International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI)*. ACM, 362–372. DOI: http://dx.doi.org/10.1145/2785830.2785842

31. Gregory Kramer. 1993. *Auditory Display: Sonification, Audification, and Auditory Interfaces*. Westview Press.

32. Katharina Krombholz, Adrian Dabrowski, Matthew Smith, and Edgar Weippl. 2017. Exploring Design Directions for Wearable Privacy. In *Network and Distributed System Security Symposium (NDSS)*. DOI: http://dx.doi.org/10.14722/usec.2017.23001

33. Marc Langheinrich. 2001. Privacy by Design – principles of Privacy-aware Ubiquitous Systems. In *International conference on Ubiquitous Computing (Ubicomp)*. Springer, 273–291. http://www.vs.inf.ethz.ch/publ/papers/privacy-principles.pdf

34. Dominique Machuletz, Henrik Sendt, Stefan Laube, and Rainer Böhme. 2016. Users Protect Their Privacy If They Can: Determinants of Webcam Covering Behavior. In *European Workshop on Usable Security (EuroUSEC)*. DOI:http://dx.doi.org/10.14722/eurousec.2016.23014

35. Tim Marsh and Peter Wright. 2000. Using cinematography conventions to inform guidelines for the design and evaluation of virtual off-screen space. In *AAAI 2000 Spring Symp. Ser. Smart Graphics*. 123–127.

36. Max-Emanuel Maurer, Alexander De Luca, and Tobias Stockinger. 2011. Shining Chrome: Using Web Browser Personas to Enhance SSL Certificate Visualization. In *IFIP TC 13 International Conference on Human-Computer Interaction (Lecture Notes in Computer Science)*, Vol. 6949. Springer, 44–51.

37. Philipp Mayring. 2014. Qualitative content analysis: theoretical foundation, basic procedures and software solution. (2014). http://nbn-resolving.de/urn:nbn:de:0168-ssoar-395173

38. Mohsin Ali Memon and Jiro Tanaka. 2014. Ensuring Privacy during Pervasive Logging by a Passerby. *Journal of Information Processing* 22, 2 (2014), 334–343. DOI: http://dx.doi.org/10.2197/ipsjjip.22.334

39. Michael Michalko. 2014. *Thinkpak: a Brainstorming Card Deck*. Ten Speed Press.

40. Saeed Mirzamohammadi and Ardalan Amiri Sani. 2016. Viola: Trustworthy Sensor Notifications for Enhanced Privacy on Mobile Systems. In *Annual International Conference on Mobile Systems, Applications, and Services (MobiSys)*. ACM, 263–276. DOI: http://dx.doi.org/10.1145/2906388.2906391

41. Calkin S. Montero, Jason Alexander, Mark T. Marshall, and Sriram Subramanian. 2010. Would You Do That?: Understanding Social Acceptance of Gestural Interfaces. In *International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI)*. ACM, New York, NY, USA, 275–278. DOI: http://dx.doi.org/10.1145/1851600.1851647

42. Jackie Moyes and Patrick W Jordan. 1993. Icon Design and its Effect on Guessability, Learnability, and Experienced User Performance. *People and Computers* 8 (1993), 49–60.

43. Jakob Nielsen. 1992. Finding Usability Problems Through Heuristic Evaluation. In *Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 373–380. DOI: http://dx.doi.org/10.1145/142750.142834

44. Jan B Nikander, Lassi A Liikkanen, and Miko Laakso. 2014. The Preference Effect in Design Concept Evaluation. *Design Studies* 35, 5 (2014), 473–499. DOI: http://dx.doi.org/10.1016/j.destud.2014.02.006

45. Sarah Pidcock, Rob Smits, Urs Hengartner, and Ian Goldberg. 2011. Notisense: An Urban Sensing Notification System to Improve Bystander Privacy. *PhoneSense* (2011). DOI: http://dx.doi.org/10.1.1.390.599

46. Rebecca S Portnoff, Linda N Lee, Serge Egelman, Pratyush Mishra, Derek Leung, and David Wagner. 2015. Somebody's Watching Me?: Assessing the Effectiveness of Webcam Indicator Lights. In *Conference on Human Factors in Computing Systems (CHI)*. ACM, 1649–1658. DOI:http://dx.doi.org/10.1145/2702123.2702164

47. Halley Profita, Reem Albaghli, Leah Findlater, Paul Jaeger, and Shaun K Kane. 2016. The AT Effect: How Disability Affects the Perceived Social Acceptability of Head-Mounted Display Use. In *Conference on Human Factors in Computing Systems (CHI)*. ACM, 4884–4895. DOI:http://dx.doi.org/10.1145/2858036.2858130

48. Kenneth Radke, Colin Boyd, Juan Gonzalez Nieto, and Laurie Buys. 2013. Who decides?: Security and Privacy in the Wild. In *Australian Computer-Human Interaction Conference (OzCHI)*. ACM, 27–36. DOI: http://dx.doi.org/10.1145/2541016.2541043

49. Diego C. Ruspini, Krasimir Kolarov, and Oussama Khatib. 1997. The Haptic Display of Complex Graphical Environments. In *Annual Conference on Computer Graphics and Interactive Techniques (SIGGRAPH)*. ACM Press/Addison-Wesley Publishing Co., New York, NY, USA, 345–352. DOI: http://dx.doi.org/10.1145/258734.258878

50. Elizabeth BN Sanders. 2001. Virtuosos of the Experience Domain. In *IDSA Education Conference*. Boston, USA. http://echo.iat.sfu.ca/library/sanders_01_virtuosos.pdf

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

52. Thomas A Schwandt and others. 1994. Constructivist, Interpretivist Approaches to Human Inquiry. *Handbook of Qualitative Research* 1 (1994), 118–137.

53. Gerald F Smith. 1998. Idea-generation techniques: A formulary of active ingredients. *The Journal of Creative Behavior* 32, 2 (1998), 107–134.

54. Sheridan Tatsuno. 1990. *Created in Japan: From imitators to world-class innovators*. Ballinger Pub Co.

55. Katrin Wolf, Albrecht Schmidt, Agon Bexheti, and Marc Langheinrich. 2014. Lifelogging: You're Wearing a Camera? *IEEE Pervasive Computing* 13, 3 (2014), 8–12. DOI:http://dx.doi.org/10.1109/MPRV.2014.53

56. John Zimmerman, Jodi Forlizzi, and Shelley Evenson. 2007. Research through Design as a Method for Interaction Design Research in HCI. In *Conference on Human Factors in Computing Systems (CHI)*. ACM, 493–502. DOI: http://dx.doi.org/10.1145/1240624.1240704