CreepyLeaks: Participatory Speculation Through Demos

Irina Shklovski

Department of Computer Science, Department of Communication, University of Copenhagen, Denmark, ias@di.ku.dk

Erik Grönvall

Department of Digital Design, IT University of Copenhagen, Denmark, erig@itu.dk

ABSTRACT

Data leakage and privacy are well known but abstract terms for most people. To grant people a real-time and on-body experience of data leakage as it happens, we constructed CreepyLeaks. CreepyLeaks turns data leakage into a visceral embodied experience that augments visual information about what data are leaked, where and via which application. Conducting evaluations of CreepyLeaks we learned the value of the public demonstrations over individual encounters with privacy technologies. Rather than inspiring the audience to think positively about a design or functionality, the demo became an opportunity to develop collective ideas of concepts and problems that are difficult to grasp individually. By conducting privacy technology demos in public and semi-public events, we demonstrate how demos can create conditions for participatory speculation – a practice involving a confluence of human and non-human actors in speculative experiences, acknowledging the politics inherent in technology design and collectively considering possible futures.

CCS CONCEPTS

•Human-centered computing~Human computer interaction (HCI)~Interactive systems and tools.

KEYWORDS

Demo, Participatory speculation, Speculative experiences, Privacy, Demonstration, Creepy, Data leakage

1 Introduction

We are standing in front of a room full of people, many in fatigues and some with their sidearms, wondering how we are going to do our demo. Our demo is called CreepyLeaks and involves attaching electrodes to a person's arm and using tiny electric pulses to denote when our device detects data leaking to third parties (like an advertising server) from a mobile phone or tablet device. We had done several such demos earlier in the year, with each resulting in an engaging debate about data and privacy, so perhaps this event will go ok too even if connecting electrodes on people carrying sidearms seems odd. As the interested audience crowds our table we discover that body hair on the arms can prevent electric pulses – all the problems of live demoing in one go. Despite the minor hiccups, the demo is a success of sorts. What conspires is an active and involved discussion of what data leakage on mobile devices actually means, why this happens and what can be done about it. This discussion involves the people brave enough to try out our device and those that remain onlookers. They ask us questions but also debate among each other for the duration of the event. While not intended for everyday use, our device is an example of a privacy enhancing technology (PET) that not only provides a glimpse into the data flows on mobile devices, but also makes this experience embodied through Electrical Muscle Stimulation (EMS). The very strangeness of our demo set-up is a bit of drama, but it attracts an audience and has consistently resulted in

boisterous debates on privacy, data protection and surveillance prompted by the combined visual and visceral aspects of the experience. Where our device is just a proof of concept (see Figure 1), not something anyone might want to own, the demo of the device has its own impact and seems to attract interest precisely because of the relatively unexpected nature of its set up and the discussions that arise around it.

The term data leakage is generally defined as "accidental or unintentional distribution of private or sensitive data to an unauthorized entity" [53:5]. However, on mobile phones, researchers often term data distribution to third parties without direct owner notification as data leakage, referring to both legal (or ostensibly user permitted) and illegal (malware facilitated) types of information flows obscured from the mobile phone owner or user [47,68]. Most of the time data leakage is invisible by definition, but if it is discovered users can become concerned or even outraged. Such outrage, however, rarely translates to other kinds of action, in part because people often feel powerless to change their situation [3,55]. PETs are typically intended to improve user awareness enabling informed decision-making about data disclosure. Despite the proliferation of PETs their uptake remains limited. Users continue to ignore reading end user license agreements and even those that download privacy enhancing technologies tend to be inconsistent in their use [34]. We designed CreepyLeaks to explore an embodied approach to communicating data leakage to the users, by using EMS. By translating it into direct muscle stimulation we sought to make data leakage a feeling rather than an abstract concept.

Figure 1: CreepyLeaks demo setup. A tablet is set up to detect privacy leaks from apps and to notify our device (orange box) about these leaks. Electrodes and EMS allows a person to physically experience the leaks.

Our initial evaluation of CreepyLeaks applied a traditional individual user-trial approach where people were asked to wear the device for a period of time and then debriefed. The findings largely replicated prior studies as participants learned to ignore the EMS notifications relatively quickly [4,43]. See for example work by Knibbe et al. that describes how users get accustomed to EMS, requiring stronger and stronger signals [35]. However, when we moved to public demonstrations we noticed a pattern of intense engagement and joint discussions between the demo participants and curious onlookers. In their seminal work on technology as experience, McCarthy and Wright propose *recounting* as a sense-making process through which "we enjoy storytelling and make sense of experience in stories" [44:43]. Our demo, CreepyLeaks, made the moment of data leakage in the course of technology use an uncomfortable,

punitive experience played out in public, in front of others. During demonstrations, CreepyLeaks offered both participants and onlookers a glimpse of the existing data extraction and exchange infrastructures that underlie any interaction with digital technology. As a result, the demo opened a space for discussion and recounting that offered a new way for our audience to collectively grasp some of the problems of data and technology. We saw this as an opportunity to create what Frauenberger calls *participatory speculation* – a practice involving a conglomeration of human and non-human actors in speculative experiences that help to acknowledge the politics inherent in technology design and to collectively consider possible futures [29].

In this paper we explore the potential and the value of staged public technology demonstrations performed with a purpose that goes beyond the "demo or die" expectation. We show here how a demo can open up a space for discussion – where the technology becomes a prop, a vehicle for generating much needed debate, about topics as complex and hard to grasp as data, data security and privacy. We argue that there can be a dual purpose to public technology demos and that there is space to expand our understanding of what a demo can be. Demonstrating our work of privacy and security research with a deliberate addition of spectacle to the proceedings has allowed us to not only show off and allow the audience to test the technology, but also produced conditions for people to reason about technology in new ways. Whatever the goals of the technology in question, at least in the area of privacy it is possible to reframe the public demo as a critical design intervention [49] that can encourage users to consider alternative relationships to familiar and new technical systems. In this world of digital resignation [64] and surveillance capitalism [70] there is an opportunity for technology researchers to use demos not only to entrance with new ideas but also to engage in a critical dialogue about the implications of our inventions.

In what follows below we present related work on Privacy and PETs, the demo in HCI, consider issues of critical design, discuss what a shift from participatory design toward participatory speculation might entail and briefly review work on uncomfortable interactions. We then present our CreepyLeaks device and describe the initial evaluation of CreepyLeaks and how we moved towards the demo configuration. We detail demo experiences from four public demos with radically different audiences ranging from an audience at a small suburban community library to the crown princess of Denmark and then discuss the implications of our work.

2 RELATED WORK

Although this research took its departure in research on privacy and data leakage, our process lead to questions about the broader meaning of public demonstrations of new technologies and their role in HCI. Our technology was not intended as a critical design exploration but shared some features typically attributed to such. The EMS aspect of our design evoked some disorientation and discomfort, capitalizing on the uncomfortable and the physically visceral to communicate abstract ideas. All of these concerns together became actionable in the spectacle of the demo and in the communal, participatory sense-making that it inspired. Below we present related work that contributed to our analysis and understanding.

2.1 Privacy and PETs

As computerization moved into increasingly diverse areas of life, concerns about new visibilities, power dynamics and control over disclosure of information multiplied [28]. Many researchers have attempted to address the issue by developing a range of privacy enhancing technologies (PETs), engaging the problem of unfettered data collection from different angles [18,27]. Many

PETs are explicitly intended to intervene in, breakdown, and challenge the data extractive relationships that support contemporary software systems [33,34,36,69]. Despite occasional success (PETs such as AdBlock, Ghostery or PrivacyBadger have become fairly common and an increasing number of instant messaging applications are considering end-to-end encryption following the relative success of Signal and WhatsApp), the vast majority of PETs do not find an audience [18,27,58].

For PETs to be successful they must first interest and persuade regular technology users that renegotiating their existing relationships with stable data systems is something they want to and should do. However, this is a difficult challenge for two reasons. First, the practice of ongoing massive data collection has rendered many technology users feeling so powerless that existing solutions seem ineffective given the incomprehensible scale of personal data disclosure [3]. While users may find the behavior of their devices downright creepy they are also paralyzed by the immensity of the system [64], often experiencing a kind of "learned helplessness" when faced with decisions about disclosure [55]. Second, the concepts of privacy and data leakage themselves may just be too abstract to have enough relevance in daily practice [17,54]. After all, what are the practical consequences of having your location or your phone ID leaked to a third party advertiser? How can users be expected to care about data disclosure if it is difficult to know whether handing location data to an advertiser is something to worry about in concrete terms. Addressing either of these problems directly is difficult despite attempts to simplify decision-making through cognitive nudges, creative notifications [2,65] or by giving privacy scores to phone apps [37] or websites [60].

If, as McCarthy and Wright argue [45], technology use is a form of experience, then PETs are tools that are intended to help people make sense of their data worlds in new ways. Since privacy is generally conceived of as an individual or at most an interpersonal problem, PETs are typically designed for individual use. In essence, PETs are intended to prejudice technology users towards caution and greater reflection on the content and data involved in contemporary interactions with technology. Although the McCarthy and Wright framework is comprised of six inter-connected sense-making processes, it is in the reflection, appropriation and recounting processes where we can observe conscious decision-making at play. Of these, recounting is the only one that is explicitly interpersonal, involving those around us in helping us make sense of our experiences. Following this, we may argue that the more complex the initial experience, the more important the interpersonal process of recounting may be. After all, discussion and collective debate are key to human thought and development across a variety of domains [16]. Thus while McCarthy and Wright are mostly concerned with the effects that storytelling and recounting have on subsequent individual experiences with technology, we focus on the communal aspect of recounting and the importance of collective sense-making that it makes possible.

2.2 The demo in HCI

The demo is a staple of HCI practice where innovative prototypes are presented to various publics. The "demo or die" principle, legendary at the MIT Media Lab, became a common idea in technical research [9,25]. The intention of the demo is to present, inform, entice and communicate. Most often this is a one-way interaction from the researcher (i.e. presenter) to the public. Although a demo is always a kind of spectacle or performance, it can also become a site of politics, a way to convene discussion, reflection and communal experience especially for topics that can be difficult to grasp. Beyond using the format of the demo to inspire the audience to think positively about this or that design or functionality, the demo can also embed an opportunity for the

audience to develop a shared idea of concepts and problems that are difficult to grasp individually. The participatory and, often, communal nature of the public demo is perhaps its most important and overlooked aspect. In any demo that attracts sufficient attention some people might engage with the demonstrated technology directly while others remain onlookers thus creating shifting roles of audience and performance.

A demo is a powerful format that not only demonstrates what is possible, but can also invite the audience to imagine potential futures through storytelling communicated with the demo setup and the involvement of the researchers. Moving research results beyond the enclosed confines of research spaces, demos invite witnessing of progress, innovation and ingenuity, where the emphasis can be placed on the future possibilities of what interim research artefacts might imply or represent [25]. How to imagine future possibilities and how to engage non-designers and non-technologies in productively imagining different and alternative technological futures has become an important question in HCI as researchers struggle to find ways to design responsibly [8,29,31]. Frauenberger argues for a rethinking of the traditional user-centred design practice, and proposes the need to "create spaces and processes that enable humans and non-humans to come together in the creative, political, controversial *Participatory Speculation* and mattering of future socio-technical configurations" [29:19].

We propose that the familiar format of the demo as a whole can be reframed and recast as a participatory engagement rather than a one-way performative act, offering a way to create conditions for convening a kind of collective participatory speculation that can eventually move beyond the demo itself.

2.3 Critical design - making things visible

The idea that designing things is more than merely finding a solution to problems but a form of ethical and political encounters is not new [29]. Many design strands in HCI such as critical, adversarial and speculative design, focus on creating provocative artefacts that question the social and political contexts of technology in different ways. Many computational artistic expressions are also intended as critical or political statements, designed as disturbances to intervene into existing discourses about topics such as privacy or ethics and the role technologies play in our lives [5].

Critical design can be categorized in two ways: the objects and experiences produced are either mock-ups that are not working or they are so polished that they can seem otherworldly, focused on the aesthetics and the performative in appearance [6,49]. It is no wonder that interpreting and drawing useful conclusions for practical design work requires new frameworks for interpretation and for supporting discussions about the futures of technology that may be provoked through critical design [7]. If the HCI professional community needs help with interpretation of critical design, how can we expect people outside this academic community to be able to engage with and debate technological futures?

Bardzell et al. provide a framework for scholarly reading of objects as provocations about the future, potentially supporting reasoned debates in the aftermath [7]. Yet this approach still focuses on a deep engagement with the object where the reflections provoked by the object are solitary and individual. Our experience with the CreepyLeaks demo points to a missing piece in potential critical engagements with technology: the importance and value of creating an environment for a collective and communal discussion of technology, focusing on the discussion itself as a valuable outcome, where the object fades into the background.

As Dourish and colleagues have previously argued, "technology development is not simply an end in itself, but also becomes a means to reflectively explore the assumptions and attitudes that underpin ideas about technology and humanity" [22:1727]. The idea of creating common and shared experiences appears

often in artistic and interventional projects. For example, Westenberg's art piece called Routes and Routines [66] enabled people to come together and explore the usually invisible digital infrastructures of the city through collective activities with sensors and DIY tools. Rather than privileging particular types of technology creation or focusing on particular kinds of fictional or future imaginaries, we consider the role of the demo as an opportunity for an exploration offered by the spectacle that new technologies can engender. The demo, by virtue of its public nature, creates conditions for such an exploration to be a collective and participatory endeavor on the part of the audience, with the researcher occasionally recruited as a facilitator and a source of expert knowledge.

In their discussion of different flavours of critical design, Pierce et al. note that "some scholars take critical design as a starting point for discussing how social issues and political themes might enter design practice." [49:2084]. While this is a worthwhile goal, we note that a focus on social issues and political themes may not need to be focal throughout every design process. Yet even where these issues are not central at the outset, we suggest that the demo can offer ways to engage with political themes and social issues alongside technological research endeavours. In essence the demo format offers a way to interrogate the existing design politically and socially at points in time. The conversations and discussions during the demo can inform the presented design itself, but it is important to acknowledge that there is an inherent politics to the demo whether intended or not.

2.4 Participatory design, speculation and convening conversations

Participatory design (PD) is known for its use of mock-ups, early prototypes and workshops in design [12] and has a long track-record of facilitating participatory and democratic design processes where future users have a voice in technology design [57]. The early focus on technology design in PD practices has in the later years been complemented by a broader look at processes of community technology appropriation [13], power-structures and negotiations that take place in design [24], infrastructuring and ongoing design in use [11,19], and the creation and use of shared resources through commons [42]. The broader contemporary PD research community also shows interest in the role technology may have in shaping society, or even in helping us understand the now of society and its potential futures, rather than developing tools to sustain predefined or specific activities. Additionally, researchers have explored how design fiction and speculative design can be used in PD. For example, Elsden and colleagues proposed a practice of speculative enactments to engage carefully selected groups in speculations about technology futures from within carefully constructed environments [26]. Desjardins and colleagues developed a notion of co-speculation as a collaborative method that involved non-designers in envisioning alternative technological presents and futures by individually engaging with pre-made booklets [20]. Similarly, participatory speculation draws on speculative design while inviting different actors, stakeholders and community members to workshop-style speculative design events, co-designing and discussing alternative futures [30]. Instead of focusing on individual user needs, participatory speculation creates conditions for communal explorations for what kinds of futures we want and what kinds of species we want to be. After all, designing things is a form of 'ethical and political encounters' [29].

What stands out in the above examples is the interest of promoting participation to shape communities and societal visions, rather than limiting activities to design of explicit interactions with technology. The speculative nature of participatory speculation sets it apart from the use of drama in PD workshops, while the emphasis on group experiences with relatively limited

structure and scripting distinguishes it from efforts such as co-speculation and speculative enactments [14]. Participatory speculation can be used to create debate, challenge norms, create consensus, give an informed voice to people, thus allowing them to participate in shaping desirable futures that goes beyond technology development. Still, as exemplified in the cited papers above the result is often externalised in the form of mock-ups, sketches, visions and prototypes. A demonstration event may not be a traditional design method but can promote participation, facilitating public debate and discussions across society. Indeed, the demo is set apart from a typical co-design encounter as there is no 'design' to be made or physical content (being storyboards, sketches or design ideas) to be produced. The demo allows people to come together and to communally experience, question, debate and reflect based on the lived experience of the demonstration. From that perspective, the demo aligns with PD thinking and Frauenberger's suggestion to "…move towards design practices that feed off controversies, that are participatory, involving human and non-human actors, that are speculative to create spaces in which we negotiate desirable futures, that are agonistic to recognise the creation of technology as a political arena and that reach across design and use." [29:21].

2.5 Uncomfortable and visceral interactions

The demo as a spectacle can bring people together and expose them to experiencing something new. Given the public nature of a demo, individual experiences can be shared collectively through observation, recounting and participating in discussions and dialogues. Mollon and Gentes have discussed how an 'uncanny feeling' or 'uncanny enough' artefact can trigger conversations and that design is a form of communication, a dialogue enabler of sort, between the designer and an audience, focusing in particular on "how to convert people from being viewers to questioners" [46:2].

An everyday but potentially uncanny technology that has recently gained some momentum in HCI is Electrical Muscle Stimulation (EMS) devices (see for example [38,40,50,63]. Before finding its way into HCI research, EMS devices have traditionally been used in rehabilitation and sports training [39,41,62] as well as in art (see the very performative and speculative work by Stelarc [61]). Due to its direct and often visual effect on the body, EMS-based notifications can be uncomfortable, visceral and spectacular all in one, making it an interesting design material when seeking to establish a spectacular and 'uncanny enough' demonstration event. As we use EMS to transmit a sensation, a notification, rather than for controlling specific muscles, our use of EMS is different from the main body of EMS-related work in HCI. A notable exception is the work by Grönvall et al. on FeltRadio [32], a WiFi signal strength detector that translates the signal strength of intercepted radio activity on the 2,4GHz band (where much WiFi traffic is located) to EMS. The stronger the radio-signal, the stronger is the EMS sent into the body. FeltRadio, like CreepyLeaks, uses EMS to make something that is normally hidden (i.e. WiFi activity mid-air or a privacy leak from a person's phone) perceivable to our senses rather than as a means to achieve a specific and controlled muscle reaction. This is an opportunity for a different way of reading the world through embodied perception.

The idea of visceral experience with data intensive technologies has been explored by Benford and colleagues in their work on uncomfortable interaction, seeking to understand the role of discomfort in creating a range of experiences with technology [10]. Where drama and performativity have typically been linked to emotional states and responses, Shklovski et al. studied creepiness and a sense of unease as experiences with data leakage [55]. Norman has traditionally relegated the visceral experience of technology and design to shape, form and materiality of an artefact [48], yet there is an inherent viscerality to a privacy violation [59] that has no material shape and yet can elicit a physical

shiver as part of an emotional response. Shklovski et al. have previously proposed a kind of visceral design to highlight design of potentially threatening data flows in technological systems that we may want users to seriously consider and reflect upon [55]. The use of EMS as a way to signal data leakage moves in this direction by making the experience of a potential privacy violation embodied and visceral in its tinge of an unpleasant muscle twitch.

3 THE CREEPYLEAKS DEVICE

CreepyLeaks is built around a common concept of a privacy enhancing technology (PET) and was designed to turn data leakage into a visceral embodied experience. Typical PETs are oriented towards individuals and their experience with technologies - the attempts to nudge or inform assume the individual to be in a position to make decisions and the need to support that decision-making in a particular direction [27]. CreepyLeaks started out with the same idea, playing with the concept of embodiment for the abstractions of privacy and data leakage. CreepyLeaks challenges people's perceptions of data leakage through sensorial augmentation, by making users feel data leakage through electro-muscle stimulation. Our original goal was to explore whether making data leakage an embodied experience could change how people think about personal data and what they are willing to do about data leakage as a potential problem.

To create CreepyLeaks we combined an existing PET software, called ANTMonitor [56], that utilizes screen-based notifications about data leakages with a piece of hardware that we designed, interpreting leakage data from ANTMonitor and turning them into Electric Muscle Stimulation (EMS) sent into the user's body. We hoped that moving from screen-based to embodied forms of interaction with technology would create a stronger connection with the identified instances of data leakage presented by the PET software, potentially motivating people to really pay attention and to act, thus leading to stronger forms of behaviour change.

Below we provide a detailed technical description of the CreepyLeaks system. In the next section we describe how we tested CreepyLeaks in individual one-to-one encounters and in demonstration events and what we have learned from these encounters.

3.1 Technical description

The main purpose of the CreepyLeaks system is to detect privacy leaks on a person's smartphone or tablet and to make the user aware of these leaks in real-time via EMS. In its current form CreepyLeaks only works with Android mobile phones and tablets. CreepyLeaks is composed of three main parts: 1) The AntMonitor app [56], 2) a custom-built app that decides the severity of a leakage instance and 3) a purpose-made bluetooth-enabled hardware that notifies the user of a leakage using Electrical Muscle Stimulation (EMS). The apps (1 & 2) must be installed and run on the user's phone or tablet for CreepyLeaks to work as intended and the hardware's (3) Bluetooth must be paired with the mobile device.

ANTMonitor is a VPN-based packet capturing system that allows interception and analysis of data leakage in real-time (regardless if the mobile device is used or not) [56]. The app is developed by Athina Markopoulou and her team at University of California, Irvine and is available for the Android platform. We developed a severity decision app, in collaboration with the AntMonitor team, to allow ANTMonitor to talk with our CreepyLeaks hardware and to classify the severity level configured for a specific leakage type. When data leakage occurs, for example if the so-called AdvertiserID or the mobile device's current GPS location is sent to an ad-server, this information is forwarded to the severity-decision app. This app checks the severity of the leakage, which

can be template-based or configured by the researchers for each test person and device. For example, we might decide that AdvertiserID is not a severe breach, but GPS location leakage is much worse. The app notifies the purpose-made CreepyLeaks hardware over Bluetooth about the leakage and its set severity, eliciting EMS activation of different strength. Figure 2 shows the technical diagram of the full setup.

The CreepyLeaks hardware is composed of a Bluetooth receiver, a microcontroller (ATMega16) controlling the system and an Electronic Muscle Stimulation generator. The generator is connected to two EMS electrodes, which are attached to the user's body. The electrodes allow the hardware to send small amounts of electrical current (i.e. EMS) into the user's body creating a small muscle contraction for each detected data leakage. The more severe the leakage, the stronger is the signal sent into the body. In other words, the user can feel a faint tickling sensation on his or her body for a non-critical leak, up to a stronger and more unpleasant electric stimulation of a muscle creating discomfort when a critical leak occurs.

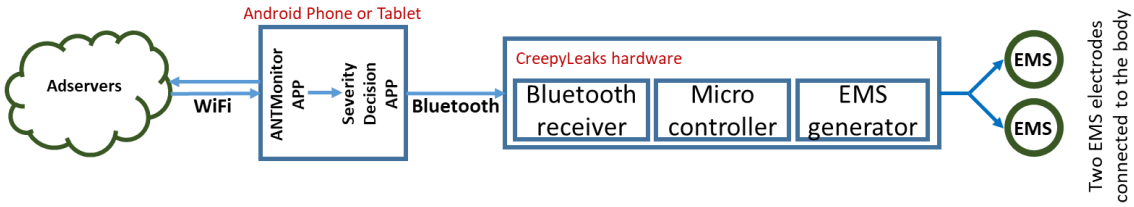

Figure 2: CeepyLeaks - Overall system architecture

4 TESTING CREEPYLEAKS

Initially we sought to test our device in an exploratory fashion, looking to answer questions such as what happens if users can sense and feel their personal data leaking from their mobile phones? How might people react and what sort of actions might they be willing to take? How might physical notifications be utilized to encourage the use of privacy enhancing technologies? As our initial findings largely replicated prior studies, we shifted strategy and adopted the demonstration approach. The patterns of engagement that emerged through the demo format lead us to explore the demo event itself as a participatory inquiry and dialogue tool. Below we present outcomes from both individual testing and the demos.

4.1 Individual testing

Our initial tests involved two small qualitative studies.

Study 1: we recruited four student-participants who were frequent mobile phone users (they used their mobile phone for more than one hour per day). We conducted a pre-interview exploring their perceptions of data, privacy and data leakage on mobile devices. They then installed ANTMonitor on their smart phone. We debriefed them after they used the app for three days. We then asked participants to browse different apps on their smartphone, including games, weather and shopping apps and TV-guides, for about 15-20 minutes while attached to the CreepyLeaks system. Participants found the ANTMonitor system by itself frustrating and too uninformative. They were curious about the CreepyLeaks addition and found it creepy but not actionable.

Study 2: three university students were first interviewed about their privacy attitudes and understanding of data leakage. They were then equipped with CreepyLeaks for two hours and asked to use their mobile phone as they would normally while at the university. We conducted a follow-up interview with each participant. While all participants found the experience entertaining, they stopped paying attention to the EMS signal relatively quickly and two

eventually turned it off after an hour because they found it annoying. One participant commented that he realized he did not actually want to be reminded just how frequently data leaks off his mobile phone even though he was interested in the topic of privacy and was intending to study information security.

These studies focused on user's understanding of data leakage from mobile phone use. Participants experienced data leakage individually as they used different apps on their devices through the on-body notification provided by EMS via the CreepyLeaks system. Predictably, the people that tried CreepyLeaks found the experience uncomfortable but not strongly motivating towards changing their mobile phone usage patterns or their phone privacy settings. Although our study participants expected some apps to leak, they were surprised by which apps actually activated the system and by the amount of leakage. What started out as a curiosity for the study participants using CreepyLeaks often turned into an annoyance or at times even faded into the background. The structured experimental conditions of individual experiences with CreepyLeaks resembled many other efforts to build and deploy privacy enhancing technologies. We managed to create some 'aha'-moments, but did not provide any viable or realistic tools for changing the status quo. CreepyLeaks, in short was going to be consigned to the graveyard of nice ideas that fail to help people cope with data leakage. While the two studies helped us better understand people's perspectives on data leakage, we did not manage to reach a state of deeper reflection or behavioural change. We noticed a completely different pattern when the device was demoed to groups of people who could try it out in turn while discussing the process and the physical sensations with us and with each other. The staging and drama of the demo, the public and communal nature of the strange experience of feeling data through electricity, created curious conditions for discussion and debate. The demo format transformed CreepyLeaks into a kind of critical design engagement.

4.2 The CreepyLeaks demo

In early 2018 we were asked to develop CreepyLeaks as a demo for an event at our university. We installed ANTMonitor and our severity detection system on a basic 7-inch Android tablet and downloaded a range of apps to test for data leakage. We reduced ANTMonitor output to a small notification at the bottom of the screen, only stating what type of information had been leaked. Our goal was to mimic a typical tablet use scenario but with apps that tended leak data predictably and reliably. Although the vast majority of Android apps leak data [52,67], not all of them do so predictably. For example, we found that some game apps such as Angry Birds, do not leak while in use, but release a raft of data some minutes after the app is closed. A predictable leak can for example be every time the user performs a specific action like opening up a menu or swiping the screen. We selected four apps for our purposes: a weather app, the Danish National broadcasting network (DR) app, a local grocery coupon and shopping app and, finally, the children's game Talking Tom app notorious for fairly egregious data leakage [15]. We developed a usage scenario where the user might want to check the weather and local news then perhaps check out relevant grocery coupons. Only then they might hand the tablet to their child to play with. The reason for this progression was that the Talking Tom app leaked so frequently that it would quickly overload our severity detection system, resulting in either system shut down or getting stuck with EMS signal on, and a constantly twitching muscle.

The physical demo setup included two researchers positioned at a table with a CreepyLeaks device paired with an Android tablet running ANTMonitor. We also produced postcard-sized information handouts, kept available on the table for people to pick up and a roll-up placed next to us with information and images. On most occasions we were invited to do our demonstration at an external event

organized by someone else. Some events targeted the general public while others oriented towards a selected group (see Table 1). Often, people approached our table in smaller groups, 2-4 people, where one volunteered to test CreepyLeaks after either a brief presentation from one of the researchers or by observing prior visitors. Before allowing people to test the system, we made sure to ask health-related questions, as the use of EMS is dangerous for people with epilepsy or medical implants. If the use of EMS was not medically counter indicated, we placed electrodes on the visitor's arm and activated the system. Participants were then asked to use the tablet and try out the four apps on the screen. In total, we conducted four demonstrations over the course of a year. Each event had a very different audience in terms of background, education, and age. Table 1 presents a summary of our demos in order of occurrence.

Table 1: The four CreepyLeaks demonstrations.

EVENT	TYPE	# OF PEOPLE	PARTICIPANT CHARACTERISTICS
National Science festival	Public	400+	VIPs, university students and faculty, press, general public
Suburban community library	Public	30-40	General public
Military intelligence agency	Private	80-100	Government employees
UN City Event	Semi-public	200-300	Employees and guests

4.2.1 Demo 1: National Science Festival.

The National Science Festival is an annual weeklong series of events organized by the Danish Ministry of Higher Education and Science. The goal of the event is to inspire interest and curiosity about science and technology in the general population and typically comprises over 700 different events across the country. In April of 2018, the IT University of Copenhagen was selected to host the grand opening of the Festival, attended by Her Royal Highness Crown Princess Mary, who is the Festival's patron, along with the Danish Minister for Higher Education and Science. CreepyLeaks was pre-selected as one of several 'example demonstrations' to be presented for the VIP guests and the media at the event. At our stand, the VIP guests and the press first got a short introduction to CreepyLeaks and the concept of mobile data leakage, and were then allowed to try out the system. Questions and discussions followed after they tried the system. Afterwards, the floor opened to other members of the audience, including high school and university students, researchers and members of the general public. For several hours, we talked with the curious audience and demonstrated the CreepyLeaks device, answered questions and explained the basic concepts behind data leakage. We soon noticed that people around us often started their own debates and discussions prompted by our demo. As researchers, we did not lead these discussions or even participate in many of them after the initial contextualization and system functionality presentation. The demo received a significant amount of publicity and media coverage, something that became important for the continuation of our work.

4.2.2 Demo 2: Ballerup library.

The media coverage of our initial demo at the national Science Festival grand opening, lead to a host of invitations to bring CreepyLeaks to other locations. In the fall of 2018 we were invited to demo CreepyLeaks at the Ballerup public library. The small library, in a relatively well-to-do suburb on the outskirts of Copenhagen, was putting on an event about data security with an activist speaker and wanted us to join. We agreed to briefly present our demo at the

start of the event and then let the audience experience CreepyLeaks during the breaks. There were about 30-40 people in the audience, trending towards middle age and older, from all walks of life including engineers, teachers, hairdressers and senior citizens. During the break a few people cautiously approached our demo and at first only one agreed to try it out. The spectacle of the device produced excited commentary from the onlookers and quickly attracted a small crowd. Although only a few people dared to try the device, the discussion of the topics of data, security and digital infrastructures quickly grew animated among the audience, with people occasionally turning to us as researchers, asking to arbiter this or that disagreement, or provide information about "how this stuff actually works". In many of the discussions we as researchers became spectators, or participated in the discussions on equal terms with the audience members rather than being moderators. The demo, providing a personal and embodied experience for the test-person as well as a spectacular and visceral experience for the audience, allowed people without deep technical knowledge to express and debate opinions (Figure 3).

Figure 3: Demo audience and participants discuss data leakage. The two researchers listen in and answer questions rather than moderating the discussion (Photo provided by the Ballerup Library)

4.2.3 Demo 3: National military intelligence agency.

Although we were not aware at the time, one of the attendees at the Ballerup library event was a security associate at a large transnational NGO. A month later he contacted us about joining a data security event at the national military intelligence agency that he organized. The event involved several speakers addressing different aspects of computer and data security oriented towards a non-technical audience. It is our impression that most of the approximately 80-100 participants were employed by the national defence forces but in a range of positions from active duty (some attendees wore military fatigues and side arms) to management, research, administrative, and clerical duties. We briefly presented CreepyLeaks as speakers on stage and invited the audience to try out our system during the break. As people tried out the device, we paid attention to the animated discussions that ensued. People began by debating whether it was possible (or even necessary) for individuals to

protect themselves from data leakage but then pivoted towards what might be achieved with a more organized regulatory response.

4.2.4 Demo 4: UN City Denmark.

For our final demo, we were invited to UN City - the Danish UN headquarters in Copenhagen for another data security event oriented towards a broader audience. As part of the event we first presented our work on the event main stage and then invited people to try out CreepyLeaks after the talks, via a booth located in the main lobby area of the UN City building. What stood out at this event is that people often came in small groups that knew each other very well. Groups of colleagues passed by our booth to learn more about CreepyLeaks and to try out the system first-hand. Often one person in the group was more eager to try the system with their co-workers looking on. The dynamics were slightly different as it was a bit of fun to see colleagues experience EMS and temporarily loose control of the arm as the muscles responded to the detected data leakage. Nevertheless, we observed many discussions and debates about data leakage, the infrastructures of digital data flows and the options available to regular people using these technologies.

4.3 Reflections on the four demos

Looking back, we found that the demos tended to unfold in a similar, two-stage fashion. This first part was comprised of a researcher-led activity with a scripted introduction where we explained CreepyLeaks and the data flows it was making visible and felt. We then invited the audience to try the device and fitted volunteers with the electrodes. The second part was non-scripted, where the people trying out CreepyLeaks and the immediate onlookers turned to each other to discuss and make sense of their experience, debating what data-leakage is and how to think about it. The researchers had a prominent role in the first part, but became incidental in the second part. We were there, consulted when a technical question came up, sometimes joining the discussion, but mainly remained onlookers to our audiences' debates.

In group situations CreepyLeaks performed a significantly different function than in the isolation of an individual experience. Here, the device, with its relatively inscrutable physical and screen-based notifications, motivated generative discussions about the meanings of leakage and what constituted right and wrong actions in response. People debated whether leaking an AdvertisingID mattered, why for example the Danish Radio app would leak such data when it has no use for advertising revenue, the logical conclusions of bad programming and current structures of existing SDK libraries, the privacy innovations introduced by Apple and many other topics. Discussions always started with expressions of discomfort - "this is scary" was one of the most common initial responses. Over time, the discussions became more exploratory and curious, trying to better understand the infrastructures of data that underlie the mundane functions of their mobile devices. People asked what they could do in response, but then ended up debating what mattered and what could be overlooked. The CreepyLeaks demo made data leakage a physical and more concrete experience, thus creating a space for discussions where people debated norms and the sense of right and wrong with respect to mobile technologies.

In this way the Demo, when properly configured and performed, thread the needle between the spectacular and the individual, offering a space for participatory speculation. In this context participatory speculation was made possible by the demo format, the particular interactive modalities of the CreepyLeaks prototype including its use of the spectacular and of public discomfort through EMS, and the sensitive yet difficult to understand topic of data privacy. While the CreepyLeaks demo in many ways aligns with Mollons and Gentes in how critical design may triggering questions, discussions and debates [46], the CreepyLeaks demonstration downplays the role of the designer and even

shifts the artefact in the background. Instead, we found ourselves creating conditions for audience-members to discuss and debate among themselves, engaging in participatory speculation about technology, privacy, and data leakage. Interestingly, while we as researchers could observe the speculations, to a large degree the discussions were by, and consequently for, the participants themselves.

5 DISCUSSION

CreepyLeaks was developed as a provocative technology intended to challenge accepted ideas about privacy and data by making the invisible data flows not only visible but also felt through the body. While our initial user testing demonstrated all the same failings of similar prior projects, we found that the demo format for this kind of technology offered interesting opportunities not only for rethinking the design of privacy enhancing technologies but also for engaging people in reasoned discussions about this topic. In the discussion below we challenge the overarching focus on the object of design in HCI that tends to overlook the importance of engagement and debate about technology that the demo makes possible and consider what opportunities this might offer for convening participatory speculation about technological futures with non-technical audiences.

5.1 Communal sense-making of data leakage

PETs tend to be oriented towards individual and private experiences. After all, the goal is to empower individual decision-making about personal data disclosure. The technical privacy community tends to be focused on personal secrets as a basic concern, thus any reflection or nudging is done in the intimate space of an individual interacting with technology. The focus on privacy may even preclude storytelling and recounting as decisions about whether to disclose data can be seen as value-laden and highly personal. The focus on empowering the user and providing endless choices in disclosure can also create interactions with the application that are repetitive and boring. As a result, many privacy technologies do not lend themselves well to a demo experience because they tend to preclude a sense of drama and performance by design.

The original idea that drove the design of CreepyLeaks only intended to create a different channel for making people aware of data leakage from their personal mobile devices. Even when creating a demo version we focused on mimicking as closely as possible a prototypical individual experience with a mobile device. Although individual experience remained at the centre of our demo spectacle, the unusual embodied nature of the interaction, when made public, offered itself as a topic of discussion that also included the onlookers. The EMS was a little bit threatening in its promise of discomfort and it required some courage to try out CreepyLeaks.

The abstraction of data flows made visible by CreepyLeaks is by nature difficult to illustrate, and EMS should not be seen as the only possibility. The muscle stimulation became an embodied feeling for the complexity of the software infrastructures that underpin our use of technology. The view ANTMonitor provided on the screen was still very limited. A little bit of text informing the user that an application sent out a particular bit of information was just a peep-hole into the reality of software infrastructures, but that view was still more than is typically available to an average user. The visible fact of leakage is not one that can be controlled or managed by the user because we did not make that aspect of the ANTMonitor interface available. Arguably, it is also not the result of user actions, since they did not make the decision to install the apps they have been asked to launch on the screen. They couldn’t have known better and the CreepyLeaks view of data leakage is

impossible to know without the software and impossible to feel without the device. Disconnected from the pressing demand to make a personal decision about whether to limit or prevent this disclosure, because this was not their own device, our participants instead were left free to puzzle over the fact of the data leakage and to recount the experience to immediate onlookers. Curiously, in the narrative of the data leakage experience, the discomfort caused by the EMS was quickly discarded in favour of making sense of the data leakage itself and debating its purpose and possibilities.

The discussions we observed during the demo made us realize that getting people to think more deeply about privacy and data can be more involved in communal rather than individual contexts – group discussions about personal data and privacy may just be more effective than individual reflections or at least just as important. There is value to communal sense making precisely because privacy, data and leakage are abstract and rely on invisible infrastructures.

5.2 Demo as a site of debate

The demo is not only a performance of a new technology although it often starts with that. We argue that the demo also offers an opportunity to the audience to question and engage with each other not just about the object being presented but also about the broader ideas underlying the presented technology. Rather than merely a presentation stage, the demo can become a site of politics, a potential site for discussion, reflection, mutual learning and communal experience especially for topics that are often difficult to grasp, setting it apart from the "demo or die" kinds of expectations.

In our case, while there is a lot of public anxiety about information privacy and security, what these terms actually mean in practice is often difficult to understand. This is in part due to the very abstract nature of concepts such as data and data flows. What does "data leakage" actually mean in practical terms? How might we create conditions for developing a shared understanding and for negotiating opinions on what is actually happening? Our demo was not intended to be about inspiring the audience to think positively about this or that design or functionality. Neither was it focused on imagining other futures or realities. Grounded in deeply mundane technology interactions and very everyday realities, we found our demo to offer an opportunity to develop a shared idea of concepts and problems that are difficult to grasp individually. The demo of CreepyLeaks was effective because it happened to connect to current debates in society, the general sense of unease with data and its invisible flows within everyday digital systems. Where there is a desire to discuss and debate these issues, there is also a lack of knowledge, understanding and tools for gaining some insight into the workings of what generally appears to be ethereal and unreal. Our demo provided some language and insight into the kinds of problems that could be attended to.

Of course we designed the demo, ascribed a lot of meanings and structured the kinds of speculation or at least the topics and reaction of the discussions that can happen in this context. Yet, we were never in full control of the context – always invited to other people's events and engaging their audiences. CreepyLeaks had to fit in with someone else's structure and narrative that, in our case and somewhat predictably, always focused on data and security for a lay audience. In two of the demos one of the speakers was a magician/illusionist that demonstrated how human attention can be manipulated and read for nefarious purposes such as plain thievery where wallets were artfully removed from pockets and credit cards out of wallets that remained in pockets.

While our audiences were already primed to think about security in different ways, few of the discussions centred on anything beyond maintaining personal vigilance or espousing abstract ideas about the importance of privacy and

government over-reach through surveillance programs. Our demo offered an opportunity for collective sense making in an area where there is typically an emphasis on personal responsibility. Our setup ensured that the data leakage was not the fault of the user, but a glimpse into the hidden data infrastructures. This gave people something concrete to debate and a potential focus for seeking how to address the problems they discovered without the attendant guilt of not reading end-user license agreements. In this process we as the researchers, while remaining important for providing explanations about how our device worked and suggestions for how to interpret the output on the screen, faded into the background as debates left the particulars of the device and turned towards the collective speculation about what could be done.

We realize that the demo is not something that can be done at scale, but perhaps scale is not what is important sometimes. What is the value of inspiring debate in a few dozen people at a time? As researchers we do not have time to do such demos frequently and we are not rewarded for it. Why should we worry about the demo if it is mostly a box-checking exercise and shouldn't we just let it be that? Our point is not that every demo must focus on creating conditions for participatory speculation in lieu of traditional goals of demonstrating, inspiring and informing. Rather, we argue that many demos already have the potential to enable such audience participation. This requires openness and attention from the researchers rather than specific effort. As a side benefit, such a demo can be conceptualized as a research inquiry where the audience reactions can provide useful and potentially productive data for improving technologies. There is an opportunity in demos to collect data as the event can act as a kind of research probe. Clearly, this sort of reframing of the demo may work for some types of technology and research orientations and not for others. While our paper has identified the link between demos and participatory speculation, more work is needed to further generalize our experiences of demos as a place for debate and participatory speculation.

5.3 Creating conditions for participatory speculation

Perhaps in this time of COVID-19 an argument for in-person group demo experiences seems strange. Yet even in the time social isolation, or perhaps especially in the time of social isolation we must not lose sight of the importance of collective sense making and group debate as core ingredients for collective action. The addition of spectacle to even the most personal and private technology use puts such experiences into a public space, generative of conversation and creating opportunities for intervention. We do not speculate on what does or could potentially happen after the demo is completed. Our purpose here is to point to the role demos can and often do play as enactments of politics. We see demos as an interesting platform to further investigate for collaborative design and participatory speculations.

The pace of technological change and the mounting evidence make it increasingly more difficult to dismiss the idea that engaging in technology development is essentially equivalent to shaping humanity [1,29]. The power inherent in the act of developing and deploying technologies must be acknowledged, tempered and carefully deployed rather than ignored as it has often been until now. Much research and debate in design acknowledges the normativity of design practices and explores the political intentions and possibilities of design in changing minds and triggering conversation [19,21,23,51]. Yet in this space too, the designer and the design often become separated where the design operates on its own. In bringing the demo into the process of engagement, CreepyLeaks begins as a traditional mode of witnessing but then is allowed to turn into a space for debate and discussion deliberately, making the roles of the designers or the researcher inalienable from the design, the demo and the purposefulness of such intervention.

Even as questions of accountability and responsibility become more prominent they remain with no easy answers. In thinking of technology as experience the idea of recounting must move from being yet another stage, perhaps with an interpersonal component and take centre stage. Recounting after all is key to thinking through experience and sense making in technology and its dialogic aspect is central to understanding how and why to react especially in contexts where the right and wrong are not clear. In creating demonstrations for new technologies, "we are not designing computers, nor can we design interactions. What we seem to be doing is creating configurations that enact certain phenomena." [29:12].

McCarthy and Wright point to the fact that even "fairly straightforward artifacts" [45:195] can be demonstrated and presented for interaction in such a way that they leave room for interpretation and create possibilities for communal and thus dialogic experience or, in Fraueberger's terms, "participatory speculation". Not every demo must turn to politics, but every demo ought to be ready for the possibility of creating conditions for the audiences to reason about technology and its futures generatively, critically and communally.

6 CONCLUSION

The CreepyLeaks demo made the moment of data leakage in the course of technology use an uncomfortable, punitive experience, in an attempt to make data and its leakage material experiences rather than abstract notions. Our work points to a broader potential of the demo format more generally as an opportunity to convene critical debates about technology and its various futures. By offering a glimpse into the material realities of digital infrastructures to a lay, non-technical audience, the demo opened a space for discussion and communal sense-making shifting towards participatory speculation. In this approach to the use of demos for participatory speculation we as researchers, and even the demonstrated technology moves in the background while the intra-participant conversations are foregrounded. People need a glimpse into these infrastructures but they also need others to help them make sense of this new information. Perhaps such communal and group debates can be an antidote to the problems of learned helplessness and digital resignation.

The paper is based on our subjective understanding of the depict demo events and we recognize that more work is needed to unfold the demo as a method of inquiry and as a space for participatory speculation. The demo is an opportunity to not only shape immediate experience with a new or imagined technology, but it can also be a site of participatory speculation about technological futures that will shape the society to come. The question remains whether a less political and less value-laden design can spark interesting debates and discussions with speculations for visions of the future. Can this be done and should it be done?

ACKNOWLEDGMENTS

We thank all the students involved in the first two pre-studies and all later demonstration participants that have tried out CreepyLeaks and participated in engaged discussions. We also extend our gratitude to the people and organizations that invited us to do our demonstrations at their different events. We are indebted to Professor Athina Markopoulou and her team at UC Irvine for their work on ANTMonitor and for supporting us in interfacing their software. Janus Varmarken and Simon Langhoff developed the Android app for interfacing the CreepyLeaks hardware with ANTMonitor.

REFERENCES

<bib id="bib1"><number>1. </number>Philip Agre. 1994. Surveillance and capture: Two models of privacy. *The Information Society* 10, 2: 101–127. https://doi.org/10.1080/01972243.1994.9960162</bib>
<bib id="bib2"><number>2. </number>Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 2015. Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (CHI '15), 787–796. https://doi.org/10.1145/2702123.2702210</bib>
<bib id="bib3"><number>3. </number>Mark Andrejevic. 2015. Personal Data: Blind Spot of the "Affective Law of Value"? *The Information Society* 31, 1: 5–12. https://doi.org/10.1080/01972243.2015.977625</bib>
<bib id="bib4"><number>4. </number>Hala Assal, Stephanie Hurtado, Ahsan Imran, and Sonia Chiasson. 2015. What's the Deal with Privacy Apps?: A Comprehensive Exploration of User Perception and Usability. In *Proceedings of the 14th International Conference on Mobile and Ubiquitous Multimedia* (MUM '15), 25–36. https://doi.org/10.1145/2836041.2836044</bib>
<bib id="bib5"><number>5. </number>Madeline Balaam and Lone Koefoed Hansen. 2019. *Wilful Technologies - Rage & Resilience*. Århus, Denmark & Stockholm, Sweden. Retrieved February 5, 2020 from https://datasociety.net/blog/2018/02/12/wilful-technologies-feminismtechnologiesdesign-google-docs-deadline-february-20/</bib>
<bib id="bib6"><number>6. </number>Jeffrey Bardzell and Shaowen Bardzell. 2013. What is "Critical" About Critical Design? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '13), 3297–3306. https://doi.org/10.1145/2470654.2466451</bib>
<bib id="bib7"><number>7. </number>Jeffrey Bardzell, Shaowen Bardzell, and Erik Stolterman. 2014. Reading critical designs: supporting reasoned interpretations of critical design. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '14), 1951–1960. https://doi.org/10.1145/2556288.2557137</bib>
<bib id="bib8"><number>8. </number>Oliver Bates, Kathy New, Samantha Mitchell-Finnigan, Matthew Louis Mauriello, Christian Remy, Roy Bendor, Samuel Mann, Simran Chopra, Adrian K. Clear, and Chris Preist. 2019. Towards a Responsible Innovation Agenda for HCI. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems* (CHI EA '19), 1–8. https://doi.org/10.1145/3290607.3299017</bib>
<bib id="bib9"><number>9. </number>Jonathan Bean and Daniela Rosner. 2013. Demo or Die?: The Role of Video Demonstrations in the Public Domain. *interactions* 20, 5: 80–81. https://doi.org/10.1145/2500502</bib>
<bib id="bib10"><number>10. </number>Steve Benford, Chris Greenhalgh, Gabriella Giannachi, Brendan Walker, Joe Marshall, and Tom Rodden. 2012. Uncomfortable Interactions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '12), 2005–2014. https://doi.org/10.1145/2207676.2208347</bib>
<bib id="bib11"><number>11. </number>Erling Björgvinsson, Pelle Ehn, and Per-Anders Hillgren. 2010. Participatory design and "democratizing innovation." In *Proceedings of the 11th Biennial Participatory Design Conference on - PDC '10*, 41. https://doi.org/10.1145/1900441.1900448</bib>
<bib id="bib12"><number>12. </number>Susanne Bødker, Pelle Ehn, Dan Sjögren, and Yngve Sundblad. 2000. Co-operative Design — perspectives on 20 years with 'the Scandinavian IT Design Model.' In *Proceedings of NordiCHI 2000*.</bib>
<bib id="bib13"><number>13. </number>Susanne Bødker, Henrik Korsgaard, and Joanna Saad-Sulonen. 2016. "A Farmer, a Place and at least 20 Members": The Development of Artifact Ecologies in Volunteer-based Communities. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (CSCW '16), 1142–1156. https://doi.org/10.1145/2818048.2820029</bib>
<bib id="bib14"><number>14. </number>Eva Brandt and Camilla Grunnet. 2000. Evoking the future: Drama and props in user centered design. In *Participatory Design Conference 2000*.</bib>
<bib id="bib15"><number>15. </number>CNN. Apps aimed at children collect a shocking amount of data. Retrieved from https://money.cnn.com/2014/11/06/technology/security/app-privacy-kids/index.html</bib>
<bib id="bib16"><number>16. </number>Randall Collins. 2009. *The Sociology Of Philosophies*. Harvard University Press.</bib>
<bib id="bib17"><number>17. </number>Andy Crabtree, Peter Tolmie, and Will Knight. 2017. Repacking 'Privacy' for a Networked World. *Computer Supported Cooperative Work (CSCW)*26, 4: 453–488. https://doi.org/10.1007/s10606-017-9276-y</bib>
<bib id="bib18"><number>18. </number>George Danezis and Seda Gürses. 2010. A critical review of 10 years of Privacy Technology. *The Proceedings of Surveillance Cultures: A Global Surveillance Society?</bib>*
<bib id="bib19"><number>19. </number>Christopher A Le Dantec and Carl DiSalvo. 2013. Infrastructuring and the formation of publics in participatory design. *Social Studies of Science* 43, 2: 241–264. https://doi.org/10.1177/0306312712471581</bib>
<bib id="bib20"><number>20. </number>Audrey Desjardins, Cayla Key, Heidi R. Biggs, and Kelsey Aschenbeck. 2019. Bespoke Booklets: A Method for Situated Co-Speculation. In *Proceedings of the 2019 on Designing Interactive Systems Conference* (DIS '19), 697–709. https://doi.org/10.1145/3322276.3322311</bib>
<bib id="bib21"><number>21. </number>Carl DiSalvo. 2012. *Adversarial Design*. The MIT Press.</bib>
<bib id="bib22"><number>22. </number>Paul Dourish, Janet Finlay, Phoebe Sengers, and Peter Wright. 2004. Reflective HCI: towards a critical technical practice. In *Extended abstracts of the 2004 conference on Human factors and computing systems - CHI '04*, 1727. https://doi.org/10.1145/985921.986203</bib>
<bib id="bib23"><number>23. </number>Anthony Dunne and Fiona Raby. 2014. *Speculative Everything: Design, Fiction, and Social Dreaming*. MIT Press, Cambridge, Massachusetts ; London.</bib>
<bib id="bib24"><number>24. </number>Pelle Ehn. 2008. Participation in design things. In *Proceedings of the Tenth Anniversary Conference on Participatory Design 2008* (PDC '08), 92–101.</bib>
<bib id="bib25"><number>25. </number>Madeleine Clare Elish. 2011. Responsible Storytelling: Communicating Research in Video Demos. In *Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction* (TEI '11), 25–28. https://doi.org/10.1145/1935701.1935707</bib>
<bib id="bib26"><number>26. </number>Chris Elsden, David Chatting, Abigail C. Durrant, Andrew Garbett, Bettina Nissen, John Vines, and David S. Kirk. 2017. On Speculative Enactments. In *Proceedings of the*

2017 CHI Conference on Human Factors in Computing Systems (CHI '17), 5386–5399. https://doi.org/10.1145/3025453.3025503</bib>
<bib id="bib27"><number>27. </number>Luis Hernandex Encinas, Agustin Martin Muñoz, Victor Gayoso Martinez, Jesus Negrillo Espigares, Jose Ignacio Sanchez Garcia, Claude Castelluccia, and Athena Bourka. 2016. *Privacy Enhancing Technologies: Evolution and State of the Art — ENISA*. European Union Agency for Network and Information Security (ENISA). Retrieved February 6, 2019 from https://www.enisa.europa.eu/publications/pets-evolution-and-state-of-the-art</bib>
<bib id="bib28"><number>28. </number>Luciano Floridi. 2005. The Ontological Interpretation of Informational Privacy. *Ethics and Information Technology* 7, 4: 185–200. https://doi.org/10.1007/s10676-006-0001-7</bib>
<bib id="bib29"><number>29. </number>Christopher Frauenberger. 2019. Entanglement HCI The Next Wave? Retrieved May 3, 2020 from https://doi.org/10.1145/3364998</bib>
<bib id="bib30"><number>30. </number>Alix Gerber. 2018. Participatory speculation: futures of public safety. In *Proceedings of the 15th Participatory Design Conference on Short Papers, Situated Actions, Workshops and Tutorial - PDC '18*, 1–4. https://doi.org/10.1145/3210604.3210640</bib>
<bib id="bib31"><number>31. </number>Barbara Grimpe, Mark Hartswood, and Marina Jirotka. 2014. Towards a closer dialogue between policy and practice: responsible design in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '14), 2965–2974. https://doi.org/10.1145/2556288.2557364</bib>
<bib id="bib32"><number>32. </number>Erik Grönvall, Jonas Fritsch, and Anna Vallgårda. 2016. FeltRadio: Sensing and Making Sense of Wireless Traffic. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems - DIS '16*, 829–840. https://doi.org/10.1145/2901790.2901818</bib>
<bib id="bib33"><number>33. </number>Seda Gürses and Joris van Hoboken. 2017. Privacy After the Agile Turn. In *Cambridge Handbook of Consumer Privacy*. Cambridge University Press, 579–601. Retrieved from https://osf.io/preprints/socarxiv/9gy73/</bib>
<bib id="bib34"><number>34. </number>Patrick Gage Kelley, Sunny Consolvo, Lorrie Faith Cranor, Jaeyeon Jung, Norman Sadeh, and David Wetherall. 2012. A Conundrum of Permissions: Installing Applications on an Android Smartphone. In *Financial Cryptography and Data Security* (Lecture Notes in Computer Science), 68–79. https://doi.org/10.1007/978-3-642-34638-5_6</bib>
<bib id="bib35"><number>35. </number>J. Knibbe, A. Alsmith, and K. Hornbæk. 2018. Experiencing Electrical Muscle Stimulation. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*2, 3: 118:1–118:14. https://doi.org/10.1145/3264928</bib>
<bib id="bib36"><number>36. </number>Tuukka Lehtiniemi and Yki Kortesniemi. 2017. Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach. *Big Data & Society* 4, 2: 2053951717721935. https://doi.org/10.1177/2053951717721935</bib>
<bib id="bib37"><number>37. </number>Minxing Liu, Haoyu Wang, Yao Guo, and Jason Hong. 2016. Identifying and Analyzing the Privacy of Apps for Kids. In *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications* (HotMobile '16), 105–110. https://doi.org/10.1145/2873587.2873597</bib>
<bib id="bib38"><number>38. </number>Pedro Lopes and Patrick Baudisch. 2013. Muscle-propelled force feedback: bringing force feedback to mobile devices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '13), 2577–2580. https://doi.org/10.1145/2470654.2481355</bib>
<bib id="bib39"><number>39. </number>Pedro Lopes, Alexandra Ion, Willi Mueller, Daniel Hoffmann, Patrik Jonell, and Patrick Baudisch. 2015. Proprioceptive Interaction. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (CHI '15), 939–948. https://doi.org/10.1145/2702123.2702461</bib>
<bib id="bib40"><number>40. </number>Pedro Lopes, Patrik Jonell, and Patrick Baudisch. 2015. Affordance++: Allowing Objects to Communicate Dynamic Use. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (CHI '15), 2515–2524. https://doi.org/10.1145/2702123.2702128</bib>
<bib id="bib41"><number>41. </number>Nicola A. Maffiuletti, Marco A. Minetto, Dario Farina, and Roberto Bottinelli. 2011. Electrical stimulation for neuromuscular testing and training: state-of-the art and unresolved issues. *European Journal of Applied Physiology* 111, 10: 2391–2397. https://doi.org/10.1007/s00421-011-2133-7</bib>
<bib id="bib42"><number>42. </number>Sanna Marttila, Andrea Botero, and Joanna Saad-Sulonen. 2014. Towards commons design in participatory design. In *Proceedings of the 13th Participatory Design Conference: Short Papers, Industry Cases, Workshop Descriptions, Doctoral Consortium papers, and Keynote abstracts - Volume 2* (PDC '14), 9–12. https://doi.org/10.1145/2662155.2662187</bib>
<bib id="bib43"><number>43. </number>Christian Matt and Philipp Peckelsen. 2016. Sweet Idleness, but Why? How Cognitive Factors and Personality Traits Affect Privacy-Protective Behavior. In*2016 49th Hawaii International Conference on System Sciences (HICSS)*, 4832–4841. https://doi.org/10.1109/HICSS.2016.599</bib>
<bib id="bib44"><number>44. </number>John McCarthy and Peter Wright. 2004. Technology as experience. *Interactions* 11, 5: 42–43. https://doi.org/10.1145/1015530.1015549</bib>
<bib id="bib45"><number>45. </number>John McCarthy and Peter Wright. 2007. *Technology as Experience*. MIT Press, Cambridge, Mass.</bib>
<bib id="bib46"><number>46. </number>Max Mollon and Annie Gentes. 2014. The Rhetoric of Design for Debate: triggering conversation with an ' ' uncanny enough ' ' artefact. In *Design Research Society 2014*, 1049–1061.</bib>
<bib id="bib47"><number>47. </number>Ildar Muslukhov, Yazan Boshmaf, Cynthia Kuo, Jonathan Lester, and Konstantin Beznosov. 2012. Understanding Users' Requirements for Data Protection in Smartphones. In*2012 IEEE 28th International Conference on Data Engineering Workshops*, 228–235. https://doi.org/10.1109/ICDEW.2012.83</bib>
<bib id="bib48"><number>48. </number>Donald A. Norman. 2001. *The design of everyday things*. MIT Press [u.a.], London.</bib>
<bib id="bib49"><number>49. </number>James Pierce, Phoebe Sengers, Tad Hirsch, Tom Jenkins, William Gaver, and Carl DiSalvo. 2015. Expanding and Refining Design and Criticality in HCI. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (CHI '15), 2083–2092. https://doi.org/10.1145/2702123.2702438</bib>

<bib id="bib50"><number>50. </number>Henning Pohl and Kasper Hornbæk. 2018. ElectricItch: Skin Irritation as a Feedback Modality. In *Proceedings of the 31st Annual ACM Symposium on User Interface Software and Technology* (UIST '18), 765–778. https://doi.org/10.1145/3242587.3242647</bib>
<bib id="bib51"><number>51. </number>Daniela K. Rosner. 2018. *Critical Fabulations: Reworking the Methods and Margins of Design*. MIT Press, Cambridge, MA.</bib>
<bib id="bib52"><number>52. </number>Gian Luca Scoccia, Ibrahim Kanj, Ivano Malavolta, and Kaveh Razavi. 2020. Leave my Apps Alone! A Study on how Android Developers Access Installed Apps on User's Device. In *MOBILESoft '20*.</bib>
<bib id="bib53"><number>53. </number>Asaf Shabtai, Yuval Elovici, and Lior Rokach. 2012. *A Survey of Data Leakage Detection and Prevention Solutions*. Springer Science & Business Media.</bib>
<bib id="bib54"><number>54. </number>Irina Shklovski. 2018. Privacy as an ability or a state: An argument for a relational view. *Workshop on Networked Privacy: Exploring individual differences in privacy*.</bib>
<bib id="bib55"><number>55. </number>Irina Shklovski, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '14), 2347–2356. https://doi.org/10.1145/2556288.2557421</bib>
<bib id="bib56"><number>56. </number>Anastasia Shuba, Anh Le, Minas Gjoka, Janus Varmarken, Simon Langhoff, and Athina Markopoulou. 2015. AntMonitor: Network Traffic Monitoring and Real-Time Prevention of Privacy Leaks in Mobile Devices. In *Proceedings of the 2015 Workshop on Wireless of the Students, by the Students, & for the Students* (S3 '15), 25–27. https://doi.org/10.1145/2801694.2801707</bib>
<bib id="bib57"><number>57. </number>Jesper Simonsen and Toni Robertson. 2012. *Routledge International Handbook of Participatory Design*. Routledge.</bib>
<bib id="bib58"><number>58. </number>Felix Stalder. 2002. The Failure of Privacy Enhancing Technologies (PETs) and the Voiding of Privacy. *Sociological Research Online* 7, 2: 1–15. https://doi.org/10.5153/sro.718</bib>
<bib id="bib59"><number>59. </number>Luke Stark. 2016. The emotional context of information privacy. *The Information Society* 32, 1: 14–27. https://doi.org/10.1080/01972243.2015.1107167</bib>
<bib id="bib60"><number>60. </number>Oleksii Starov and Nick Nikiforakis. 2018. PrivacyMeter: Designing and Developing a Privacy-Preserving Browser Extension. In *Engineering Secure Software and Systems* (Lecture Notes in Computer Science), 77–95. https://doi.org/10.1007/978-3-319-94496-8_6</bib>
<bib id="bib61"><number>61. </number>Stelarc. 1999. From zombies to cyborg bodies: exoskeleton, extra ear and avatars. In *Proceedings of the 3rd conference on Creativity & cognition* (C&C '99), 23. https://doi.org/10.1145/317561.317566</bib>
<bib id="bib62"><number>62. </number>P. Strojnik, A. Kralj, and I. Ursic. 1979. Programmed Six-Channel Electrical Stimulator for Complex Stimulation of Leg Muscles During Walking. *IEEE Transactions on Biomedical Engineering* BME-26, 2: 112–116. https://doi.org/10.1109/TBME.1979.326520</bib>
<bib id="bib63"><number>63. </number>Emi Tamaki, Takashi Miyaki, and Jun Rekimoto. 2011. PossessedHand: techniques for controlling human hands using electrical muscles stimuli. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '11), 543–552. https://doi.org/10.1145/1978942.1979018</bib>
<bib id="bib64"><number>64. </number>Joseph Turow, Michael Hennessy, Nora Draper, and Ope Akanbi. 2018. *Divided We Feel: Partisan Politics Drive Americans' Emotions Regarding Surveillance of Low-Income Population*. University of Pennsylvania: Annenberg School of Communication. Retrieved April 2, 2019 from https://www.asc.upenn.edu/sites/default/files/documents/Turow-Divided-Final.pdf</bib>
<bib id="bib65"><number>65. </number>Yang Wang, Pedro Giovanni Leon, Alessandro Acquisti, Lorrie Faith Cranor, Alain Forget, and Norman Sadeh. 2014. A Field Trial of Privacy Nudges for Facebook. In *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems* (CHI '14), 2367–2376. https://doi.org/10.1145/2556288.2557413</bib>
<bib id="bib66"><number>66. </number>P Westenberg. Routes + Routines. Retrieved October 22, 2019 from http://constantvzw.org/verlag/spip.php?article111</bib>
<bib id="bib67"><number>67. </number>Wired. Thousands of android apps are silently accessing your data. Retrieved from https://www.wired.com/story/thousands-of-android-apps-are-silently-accessing-your-data/</bib>
<bib id="bib68"><number>68. </number>Zhemin Yang, Min Yang, Yuan Zhang, Guofei Gu, Peng Ning, and X. Sean Wang. 2013. AppIntent: analyzing sensitive data transmission in android for privacy leakage detection. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security* (CCS '13), 1043–1054. https://doi.org/10.1145/2508859.2516676</bib>
<bib id="bib69"><number>69. </number>Bo Zhang and Heng Xu. 2016. Privacy Nudges for Mobile Applications: Effects on the Creepiness Emotion and Privacy Attitudes. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (CSCW '16), 1676–1690. https://doi.org/10.1145/2818048.2820073</bib>
<bib id="bib70"><number>70. </number>Shoshana Zuboff. 2019. Surveillance Capitalism and the Challenge of Collective Action. *New Labor Forum*: 1095796018819461. https://doi.org/10.1177/1095796018819461</bib>