View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by University of Worcester Research and Publications

Understanding Engagement With The Privacy Domain Through Design Research

Asimina Vasalou (Corresponding Author)
London Knowledge Lab
Institute of Education
23-29 Emerald Street
London WC1N 3QS
Phone: +44 (0)20 7763 2137
Fax: +44 (0)20 7763 2138
minav@luminainteractive.com

Anne-Marie Oostveen
Oxford Internet Institute
University of Oxford
1 St Giles, Oxford OX1 3JS
Tel. 01865 287210
anne-marie.oostveen@oii.ox.ac.uk

Chris Bowers
Department of Computer Science
University of Birmingham
Birmingham B15 2TT
Tel. 121 4143744, Fax. 121 4144281
C.P.Bowers@cs.bham.ac.uk

Russell Beale
Department of Computer Science
University of Birmingham
Birmingham B15 2TT
Tel. 121 4143744, Fax. 121 4144281
R.Beale@cs.bham.ac.uk

ABSTRACT
This paper reports findings from participatory design research aimed at uncovering how technological interventions can engage users in the domain of privacy. Our work was undertaken in the context of a new design concept "Privacy Trends" whose aspiration is to foster technology users' digital literacy regarding ongoing privacy risks and elucidate how such risks fit within existing social, organizational and political systems, leading to a longer term privacy concern. Our study reveals two challenges for privacy intervention design: the need to develop technology users' intrinsic motivations with the privacy domain and the importance of framing the concept of privacy within users' interests. Setting our study within a design context enables us to identify four design opportunities for fostering engagement with the privacy domain through technology design.

Keywords
Privacy interventions, privacy, engagement, design research, digital literacy, learning, reflection

INTRODUCTION

With technologies becoming more complex and sophisticated, privacy threats and violations are inevitable. For example, only recently it was revealed that the National Security Agency in the US was capable of collecting and interpreting Internet users' online activity[1]. Legal regulation can vary by country (Baumer et al., 2004) but even when technology organizations are legally obliged to be transparent about their data collection practices, their communication with users is often poorly managed through lengthy and ill-structured privacy policies (Jensen and Potts, 2004). As a consequence, there is an ongoing need for additional tools that will help users gain insight into how technologies operate in order to sufficiently understand the risks they are exposed to and formulate definitions of risk. These concerns have created a new design space for privacy interventions that render the system's operations visible to the user, for instance through visualizations or informative alerts (e.g. de Paula et al., 2005; Mazzia et al., 2012; Wills and Zeljkovic, 2011), aimed at raising awareness and/or supporting privacy management.

Despite the growing interest in this field of research, privacy interventions have not gained traction and commercial adoption has been lagging (Brunk, 2002). One of the reasons often cited is technology users' lack of engagement with the domain of privacy. This can lead to low motivation when it comes to managing privacy or security risks with such concerns seen as secondary, and an impediment to their main task (Kirlappos and Sasse, 2012; Whitten and Tygar, 1999; Dourish et al., 2004). Although this might suggest the investigation of the means of effective engagement as an overarching design concern for privacy interventions, researchers have predominantly focused their attention on communicating accurate and comprehensive models of risk without explicitly addressing engagement as a design concern.

The present work addressed this question through participatory design research. Twelve technology users interacted with and reflected on a privacy intervention in the early stages of its design. We found that technology users, at present, are motivated to use technological interventions only when a threat is perceived. Engaging with privacy risks is seen as an undesirable responsibility that can be delegated to technologies. Our findings suggest four guidelines for overturning these expectations with a view to fostering engagement with the domain of privacy through technology. First, we propose that presenting a rich and multi-layered perspective on privacy can be more accommodating to technology users' experiences and expertise as it encourages them to locate their concern with privacy against a larger and more personally relevant narrative. Second, interventions that support technology users to resolve their short-term concern with a given risk, and at the same time deepen their understanding of the social and political dimensions of the risk under scrutiny, offer a way of prolonging engagement beyond the scope of an individual's appraisal of a particular privacy risk. Third, we demonstrate the importance of directed interaction in facilitating reflection into the privacy domain. Finally, we discover a necessity for usable privacy interventions designed to be understood by laypeople and based on credible sources of information.

We begin by discussing the theoretical approaches that designers have taken when crafting their privacy interventions, using these as a background for motivating the need to additionally consider users' engagement with the domain of privacy. We go on to detail our research questions and the design context within which we explored them. Following an overview of our participatory design study, the remainder of the paper presents our key findings concluding with a set of design opportunities for future privacy interventions.

MOTIVATION

A shared aim in privacy research has been to understand how people make information-sharing decisions online, and to influence them with targeted technological interventions. Economists propose that a cost-benefit ratio, subject to cognitive and behavioral biases, underpins privacy decision-making (Acquisti and Grossklags, 2005; Acquisti, 2009). They argue that it is possible to influence the ratio by showing users the costs they incur when sharing information. Acquisti (2009) illustrates how this theory might be expressed when a user shares their date of birth on a social network site, with the added assumption of a "soft paternalistic" obligation to notify users of their risks: "A soft paternalistic approach might provide context to aid the user's decision—such as visually representing how many other users (or types of users) might be able to access that information or what they can do with it..." Inspired by soft paternalism, Maurer et al. (2011)

[1] http://www.theguardian.com/world/2013/aug/16/nsa-revelations-privacy-breaches-udall-wyden

created a rule-based system that calculated levels of risk based on the information users disclosed, issuing privacy and security warnings whenever users shared sensitive data. Context awareness ensured users' attention. In a similar vein, Kirlappos and Sasse (2012) analyzed the likelihood of a phishing attack occurring and displayed a risk assessment to users while they made online purchases.

Taking a different perspective motivated by the situated and socially embedded nature of privacy, Dourish and colleagues argue that many technological systems do not support reflexive interpretation of action so that users can anticipate how their actions appear to others (Palen and Dourish, 2003; de Paula et al., 2005; Dourish et al., 2004). The proposed solution is to design technological systems that can readily communicate the relationship between users' actions and their potential consequences (Dourish and Anderson, 2006). This is accomplished by increasing system transparency while at the same time supporting situated action with usable privacy settings. Egelman et al. (2011), for example, employed Venn diagrams to demonstrate the overlap of social groups on Facebook, with privacy controls placed on the points of overlap. In doing so, they addressed a mismatch between Facebook's controls for group privacy management and users' mental model of their operation. Designers of Impromptu visualized users' file sharing permissions and overlaid privacy controls for regulating the level of sharing (de Paula et al., 2005).

A third approach has been rooted in cognitive psychology, and focuses on the need for raising awareness of practices that impinge on privacy. Based on a hypothesis that an information gap is the limiting factor, designers present data collection practices that normally remain hidden, in order to heighten users' typically low levels of awareness. For instance, Wills and Zeljkovic (2011) exemplified the risks involved during third-party website tracking through an application that recorded and visualized how many websites logged a user's activities. Kani-Zabihi and Helmhout (2012) developed an interactive map depicting the information sharing flow of an e-government service.

The majority of the work described has drawn inspiration from the decision-making and economics literature. This focus has meant that researchers have been occupied with designing a model—whether of levels of risk, consequences, and so on—and a representation that can convey the relevant consideration to users (e.g. visualization). Their main concern has been whether this kind of representation is well understood and/or if it has resulted in change. Beyond the production of intelligible representations and controls, however, there is a separate question to be addressed concerning why users would be motivated to actively engage with such privacy interventions in light of their inertia with the concept. To take this point seriously would be to acknowledge that the question of *engagement* should be posed as a design consideration during the development of privacy interventions, and moreover that privacy in the context of socio-technical systems should be considered more broadly as a *domain* that must be engaged with before it can be understood and acted upon.

The recognition that engagement sustains people's motivation, participation and commitment to an activity (Chapman, 2003; Zepke and Leach, 2010) has fuelled research in numerous fields, including human-robot interaction (Sanghvi et al., 2011), computer games (Dickey, 2005), and educational technologies (Kearsley and Shneiderman, 1998). The importance of engaging people in the domain of privacy is not unfamiliar to privacy researchers who have looked to engender engagement through participatory methodologies, such as filmmaking or performance art (Coles-Kemp and Ashenden, 2012). In this context, researchers have observed that participatory and creative methods allow users to express themselves, create their own meaning, and as a consequence become opportunities for learning (Kani-Zabihi and Wattam, 2009). Indeed, engagement is considered to be fundamental to learning, and has been linked to deep learning (Zepke and Leach, 2010). Even though participatory research can have a profound impact on a small group of recruited participants, technological interventions offer the possibility of involving a broader community of people. Yet the potential of privacy interventions in creating engaging experiences with the domain of privacy has not received sufficient attention to date. In adopting an engagement perspective, we argue that it may be possible to overcome technology users' typically low levels of motivation with the concept of privacy, stimulate deep learning around privacy risks and responses, and promote understanding of the socio-political decisions that shape their futures (see Zepke and Leach, 2010 for a broader discussion on the significance of engagement).

RESEARCH AIMS AND APPROACH

Our central objective in this work has been to understand how technology users themselves engage, and desire to engage with the privacy domain through a privacy intervention under development, using this as a basis for identifying new design opportunities for technological interventions at large. Engagement has been previously defined as a dynamic process characterized by three key stages through which a user may loop: the starting point of engagement when the user is drawn into the technology, a prolonged period of engagement with the technology, ending with a period of disengagement (O'Brien and Toms, 2008).

O'Brien and Toms (2008) propose an inclusive set of attributes that provoke or characterize engagement within each of these stages on the basis of which they define engagement 'as a quality of user experiences with technology that is characterized by challenge, aesthetic and sensory appeal, feedback, novelty, interactivity, perceived control and time, awareness, motivation, interest, and affect'. Although this definition could be viewed as being restricted to the design of technology, it is important to emphasize that it was developed based on an exploration of the mechanisms that foster the experience of engagement. Indeed, many of the technology attributes (e.g. challenge, control) it encapsulates have been long recognized in their faculty to foster engagement (Zepke and Leach, 2010). Furthermore, even though O'Brien and Toms (2008) argue that the engagement model generalizes to any technology, attributes must be designed to be meaningful for the context within which they will operate, thus suggesting that technology and domain are inseparable. In wanting to explore how privacy interventions can foster technology users' engagement with the privacy domain, we use these attributes as a broad framework for investigation.

In order to design engaging activities or technologies, it is important to understand the people who will be involved in them. However, as Deci (1992) points out, people's engagement and interest must be inevitably assessed through activities, "however broadly these activities are defined". In this work we sought to understand engagement with the privacy domain through a set of activities generated in a design context centered on a privacy intervention called Privacy Trends. In the early stages of design, our participants were asked to take on two different roles. As *co-designers* of Privacy Trends, we presented them with our concept and its design constraints. This allowed us to elicit their ideas on how our application might be designed to foster their engagement with the privacy domain. As *users* of Privacy Trends, our participants interacted with a range of informational materials about a particular privacy risk. During this exploratory task, we asked them to customize these materials, as they would want them to appear in Privacy Trends. This enabled us to observe the unfolding process of engagement and to locate each participant's interest in the privacy domain.

The process of developing Privacy Trends was "a means than an end" (Fallman, 2003; 2005), in the sense that our aim was not to develop a tool. Rather, our aim was to understand how engagement with the privacy domain could be fostered by technology through the collaborative process of designing and interacting with this tool. This allowed our team to reflect *in action* (Schön, 1983) on surprises and paradoxes regarding the ability of Privacy Trends to encourage engagement with the domain of privacy, leading to a set of new design guidelines for privacy interventions more generally. The following section explains how Privacy Trends was conceived.

Privacy Trends

Privacy is a concern that confronts us individually as we seek to manage our social interactions (Dourish and Anderson, 2006; Palen and Dourish, 2003). It is also an issue of larger social and political significance. In its latter capacity it serves to protect political freedom, provides choice and safeguards intimacy (Margulis, 2003). Motivated both by its individual and wider social importance, we sought to design a tool that would enable users to understand risks arising in the context of particular socio-technical systems and additionally support them in conceptualizing how these risks form longer-term privacy concerns. Therefore, the current research defined the boundaries of the privacy domain broadly as (a) entailing risks with potential personal relevance that may necessitate an action; (b) the risks originate, influence and are shaped by social, organizational and political actors, and; (c) the risks form the basis for longer term social issues and concerns.

Our conceptualization of this tool was rooted in, and drew on, recent developments in online media that have opened new possibilities for engaging with the domain of privacy, which have not been hitherto sufficiently harnessed. The advent of online media has played a critical role in raising transparency into the operations of organizations and governments during events of social or political importance — including, notably for our

context, privacy infringements (e.g. Vasalou et al., 2011) — by providing timely access to aggregated opinions. For example, a recent study reported over 85% of trending topics within Twitter to express a news headline (Kwak et al., 2010). Transparency has therefore become the outcome of collective action and civic participation (Diamond, 2010)[2]. Previous design work has looked to support transparency during events of importance by prioritizing information cues seen as necessary to address a range of problems. Practical tools have been developed based on temporal visualizations of aggregated language from online media, such as micro-blogs (e.g. Diakopoulos et al., 2012; Social Mention, 2012; Chakrabarti and Punera, 2011). For instance, Twitinfo is a tool for making sense of large-scale events. Users can scope an event by entering keyword combinations. The application accesses the Twitter Stream to then display a timeline of language peaks that can be further explored by looking at individual tweets, their geo-location, overall sentiment and the most popular links shared (Marcus et al., 2011). Another example is the SRSR (Seriously Rapid Source Review) tool, which was designed to enable journalists to find and access interesting and trustworthy sources in Twitter around breaking news events. SRSR organizes Tweets by user type, location, and network composition (Diakopoulos et al., 2012).

This previous work shows that it is computationally possible to capture timely information when an event of importance, in this case a privacy risk or violation, occurs. It is also reasonable to assume that online media contributors will write about risks associated with a range of different technologies, thus stretching the public's awareness beyond a particular technological domain. Basing ourselves on these possibilities, we envisioned Privacy Trends to function in the following manner: (a) access and store Tweets from the Twitter stream; (b) apply event detection algorithms that will cluster the Tweets into discrete categories each of which encapsulate a privacy risk or violation; (c) analyze the content of the Tweets and their outlinks to online media in order to construct an interactive visualization that will allow users to move from summarized to in-depth views of the stories written about a given privacy event. Given that online media stories formed the content of our intervention, the privacy domain covered in this research was represented by the multiple perspectives and knowledge expressed by online authors.

METHODS

Participants

An advert was placed in a local newspaper in the city of Oxford seeking Internet users who were willing to provide feedback on the design of a new privacy risk awareness application. Interviews with twelve participants (6 females, 6 males) were carried out over the month of June 2012. We ceased to recruit interviewees when our analysis was no longer yielding new themes. Participants' mean age was 40.5 (SD=19.4). The youngest participant was 21 and the oldest 79. At the end of the session, we compensated the interviewees with £15.

Table 1 – Participants' technology use

Technology use	%
Social networks	81%
Searching for information	100%
Browsing news	100%
Buying a consumer product	72%
Doing Internet banking	90%
Ordering groceries	27%
Playing games	27%
File sharing	45%
Watching videos	54%
Listening to the radio or watching TV	81%

[2] Transparency does not necessarily indicate accurate and complete coverage of an event. It is unlikely that depth, breadth or accuracy are measurable given that consequences to privacy risks are *anticipated*, while the public (and sometimes even the offender) may not be aware of the exact nature of the risk.

Procedure

The study was organized into two parts. The first part aimed at broadly understanding participants' day-to-day engagement with the privacy domain. Once they arrived, participants filled out a demographics questionnaire that determined their technology use (see Table 1). After completion of the questionnaire, a semi-structured interview was carried out to probe their existing level of engagement with the privacy domain. This background information was necessary in understanding how Privacy Trends can fit with and influence present levels of engagement.

The second part of the interview focused on Privacy Trends. Our participants were invited to serve as *co-designers* for the tool. We elicited relevant feedback from them about their possible use of Privacy Trends, with a particular focus on how such a privacy intervention may engage them with the privacy domain. The aim and expected function of Privacy Trends, as outlined above, was first explained. Next, we provided participants with an example risk and online media stories written about it in order to ground the tool in a concrete example (see Table 2). Participants' desire to engage with the privacy domain through technology was examined by asking them to design aspects of Privacy Trends that we had not yet developed: in particular, we asked them to detail whether the risks presented within the tool should be tailored to their own technology use, under what circumstances they envisioned using it and how reactive or proactive our privacy intervention should be.

As noted above, to ground Privacy Trends in an example, and to stimulate and observe our participants' engagement with the privacy domain, we asked them to take the role of the *user*, during which period they interacted with a sample case. Given the ubiquitous use of the Google search engine, and thus its personal relevance to our participants, we chose to present participants with Google's privacy policy change. Having come into effect several months before the interview, Google had consolidated its privacy policies, enabling information collected in one application to be shared in the context of another. Participants were shown printouts of eight online sources written by reporters of news media, Google, technology bloggers, micro-bloggers (extracted from Twitter), and privacy advocates (see Table 2). These stories were originally linked from Twitter and were chosen after appearing in a keyword search for "Google Privacy Policy". This task consisted of showing participants the in-depth view of each story and was thus in part aligned with how our proof-of-concept was expected to operate. Upon reading each story, participants were asked to highlight with a marker the areas of the text deemed to be most important to them personally, to explain why and to reflect on how this information could be embedded or represented within Privacy Trends. The involvement this task introduced allowed us to observe and understand engagement with the domain of privacy as a process.

Table 2 – Online Media Stories

Original Source	Page Title	URL
CBC News	Google Data Merge Called Privacy Threat	http://tinyurl.com/83sohfl
CNN	Google to Merge User Data Across its Services	http://tinyurl.com/7k6vhr8
Google	Policies and Principles	http://tinyurl.com/84cr3ux
Technical News Cast	Google's New Privacy Policy Goes into Effect Today	http://preview.tinyurl.com/po5dcx5
Anglia CV Solutions	How to Delete Your Personal Information from Google's Browsing History	http://tinyurl.com/orwhbx5
Tips4PC	Google's New Privacy Policy – Understanding the Possible Impact	http://tinyurl.com/lt64xzq
Electronic Frontier Foundation	How to Remove Your Google Search History Before Google's New Privacy Policy Takes Effect	http://tinyurl.com/6v9mddu

Qualitative Analysis

Our methods combined semi-structured interviewing and observations of participants' exploration of the information exploration task. We conducted thematic analysis on our findings. The interviews were first transcribed. We then analyzed them thematically to identify emerging concepts with relevance to how technology users' engaged with the privacy domain, both in their daily life and through Privacy Trends. We

read each interview multiple times taking notes on recurrent codes. These codes were thematically categorized and our analysis ended when we felt confident that our data was fully described by our scheme. Our qualitative analysis yielded four key themes with attributes (appearing in small caps) centered on two key phases: the initial point of engagement and the period of engagement.

RESULTS

Point of Engagement – A Lack of Motivation

The engagement model features MOTIVATION as a necessary attribute for users' initial engagement with a technology. Privacy researchers have previously noted that users lack the motivation to engage in understanding and appropriately responding to privacy risks (Whitten and Tygar, 1999; Kirlappos and Sasse, 2012). In line with this view, with the exception of a retired participant who kept up with national news on a daily basis, our remaining participants, even those who expressed serious concerns about their online privacy, showed inertia in keeping up with new privacy risks. As one of our participants explained: "*I am naïve when it comes to privacy, which is an odd thing because it is quite important. If I am honest, the reason I would not spend that much time is because I am not that interested. That is the crux of it."* When we asked our participants how they learned about privacy matters, many of them struggled to reply. In support of previous research (e.g. Adams and Sasse, 1999; Rader et al., 2012; Dourish et al., 2004; Rode, 2009), we found that new threats to privacy were learned, either by chance (e.g. through the news, word of mouth) or through institutional enforcement (e.g. company regulations). Participants' disengagement with privacy risks was further evidenced during the information exploration task: even though Google had featured prevalent notifications on its search page at the time of its privacy policy change, the majority of participants were surprised to hear about this change.

Participants offered a number of justifications for their complacency. Some believed that privacy risks were not applicable to them and were typically relevant to people in the public eye. Others had transferred the responsibility of privacy management to third parties and dealt with uncertainty through trust. In the words of one participant: "*I think I've become a bit blasé about Amazon now and eBay. And in eBay I'm reasonably confident it will work.*" Another way to avoid the personal responsibility that arises from a violation was to hold others liable. One participant for instance had come to accept the risks involved in online banking: "*It's going to happen to you at some point if you buy things on the Internet and you sort of go to ATM machines and things like that. It could happen to anyone, so… There are always safeguards and protections that if it does happen you will get it [your money] all back. It's not the biggest deal in the world.*" Indeed, when presented with Google's privacy policy change, many participants' worries were appeased after finding out that Google was being audited on a regular basis and thus some regulation was in place to protect their interests.

Point of Engagement – Goals of Privacy Interventions

With the exception of one participant who admitted to being negligent about her privacy, all others had installed third party applications to protect themselves against spam and viruses. When discussing Privacy Trends, it became evident that previous experiences with these types of technological interventions created constraints around the domain of privacy that participants considered to be relevant to themselves and the types of outcomes they expected from technologies. Even though our explanation of Privacy Trends was clear, when discussing the functionality of our application with them, time and time again, participants focused on the provision of automatic assistance that would flag and work out a risk on their behalf, suggesting a concern to minimize their own continued engagement. This supports findings by Dourish et al. (2004) who found that in dealing with security risks, technology users often sought to delegate their technical responsibility to others. To give an illustrative example of this trend within our study, one of our participants proposed: "*depending on the website that you are surfing it should popup messages that this is a new website. Do you want me to do privacy settings for you on this website?*" Therefore, when acting in the capacity of a designer, many of our participants believed that the GOAL of privacy interventions was to protect them from risks, and concurrently maintain their levels of disengagement with the domain of privacy.

Nonetheless, a few participants were able to step away from this dominant frame to conceive more broadly how Privacy Trends could fulfill uncharted GOALS that benefit them and others. One of our participants acknowledged that Privacy Trends would not only raise awareness about ongoing privacy risks, but could also

empower users by providing appropriate responses that led to resolution: "*It's not just ah look what's happening but positive resolution is…and prevention… explaining to people that it is prudent to delete your cookies and backup your hard drives and whatever else and keep software up to date and things*". Another participant reflected on how an all-encompassing tool of privacy could transform her own use of technology: "*Because what I'm doing at the moment is I'm telling myself I have no idea of this at all, I don't know who might be spying on me so to speak, might be using my data, so I don't give anything out to them that I wouldn't be happy for them to have. And if I had such a thing I think it would be very helpful and it might help me be more secure in my ways of dealing with the Internet.*" Yet a few others were able to look beyond their own use to how such a tool could influence the politics of privacy. They proposed that the publicity and visibility of online media stories was extremely important in holding organizations accountable for their actions, suggesting that designers build on this affordance by visually representing the magnitude of an issue or the exposure it had received.

Engagement – Time, Attention And Awareness

Given participants' general levels of disengagement with the domain of privacy, it is not surprising that they wanted to carefully define the TIME they spent on addressing privacy matters, with a view to reducing the period of engagement. They proposed that Privacy Trends 'push' the information to them as a way to diminish any initial effort involved in seeking out information thereby relieving them from the task of seeking it out themselves. Some participants wanted a tool that would be embedded in the browser, enabling it to identify ongoing risks resulting from the user's activities and to flag appropriate moments of intervention. Others proposed news bulletins and emails that would contain summaries of privacy risks currently under review. Our participants regarded the Google Privacy Policy, and privacy risks more generally, as not particularly urgent, thus requiring only their intermittent ATTENTION. As one participant noted: "*I think it would maybe annoy me if it popped up everyday*." In the words of another: "*Daily basis, no but perhaps once a week yes. And maybe if it is kind of an update you know, that comes to you in an email*." Moreover, when prompted on the kind of risks they wanted to be AWARE of, all of our participants requested information that was relevant to their own use of technologies. To this end, one of our participants highlighted how important it was to have a tool that would span all of his technology use: "*…I really wonder what kind of a tool that would be because, you know, these days we have personal data spread across many different websites and many different forums I would say. So the tool should be something that could encompass all these different websites and different forums and maybe you know it could do your banking websites, your social networking websites or email websites and any other websites*." A minority of our participants also expressed the need to be informed about privacy problems that were deemed important for them to know more generally in their capacity as digital citizens. One participant drew a distinction between "local" risks, i.e. customized to a user's technology use, and "global" risks, i.e. those important to know as a digital citizen.

Engagement – Interests, Challenge and Information Consumption Strategies

Our study explored people's INTERESTS within the privacy domain. To achieve this understanding, we asked participants to highlight passages within each online media story that were most important to know about. This interactive activity revealed a clear trend: our participants marked *when* the privacy risk was first identified, *why* it was happening, what the *nature* of the problem was, what its *consequences* were, whether *regulation* existed and what *actions* were available. Therefore, participants agreed that certain dimensions of interest existed in the range of online media coverage. At a rudimentary level, the outcome of this activity was to help raise participants' awareness about Google's new privacy policy given that most of them were unfamiliar with this change. It also developed their understanding in Internet economics and the advertising model often underlying technology companies, which many of them were unfamiliar with. For those who were already digitally literate, the information they read provided evidence to confirm their current understanding. Participants' involvement in the information exploration activity additionally strengthened their existing attitudes against the collection and storage of information by companies. The most powerful outcomes, however, did not come from the acquisition of facts, or the affirmation of knowledge previously acquired, but from a more active involvement that facilitated learning.

In particular, the CONTROL afforded by the information seeking activity, with the INTERACTIVE annotations serving as an additional scaffold, helped participants to focus on personally meaningful CHALLENGES. This resulted in many of our participants engaging in critical thinking. For example, even though a few stories

proposed that one way to opt out would be to stop using Google, a few of them questioned whether this was true given that Google had become an indispensable service. Others expanded the implications of Google's privacy policy change by considering it within a larger system of actors. This led them to propose new sources of risk such as hackers who might obtain one's data, or Google employees who might act out of negligence. Several participants evaluated the solutions that online media authors proposed to combat Google's privacy policy change through targeted questions: one of them asked whether the act of deleting information from Google was permanent; another one wanted to know whether the police had unlimited access to the data collected; and yet another participant questioned if Google's conviction not to sell information also prohibited them from sharing data with third parties. The questions posed often guided and structured participants' exploration of the informational materials. In addition to exercising critical thinking, our participants engaged in meaning making. They reflected on their own use of Google's tools, and the use of close others (e.g. children, grandchildren), to identify whether they were at risk. This process led some participants to imagine new consequences spanning from tailored adverts that impinge on their freedom of choice, to a 'private' cancer condition becoming visible to their relatives. Although most of our participants reached the conclusion that they were not personally at risk, they had become invested in the activity and continued interacting with the stories aiming to better understand the social implications of the risk.

The most illustrative example of this learning journey came from an elderly retired male participant who entered the task with the understanding that "personal information" was of financial nature. He falsely assumed that Google accesses users' banking information. However, after reading the various stories, he came to realize that personal information included patterns of online browsing. He went on to reflect on how he uses the various Google products to conclude that he was not at risk. Furthermore, he proposed new sources of risk stemming from Google's intention to exploit the data and possible employee misconduct. Initially questioning whether the police had unfettered access to Google's database, his concerns were later put to rest after reading that Google gave access to users' data only when a legal case was raised.

Participants employed a number of strategies targeted at building up an accurate mental model of the risk under investigation. Many of our participants wanted to read stories from different sources in order to balance the opinions they came across. As one of them noted: "*I think by looking at a range of them you may get an unbiased opinion. Some of them are quite balanced. By reading 3 or 4 then you will get a whole balanced idea*." This strategy also allowed them to answer the entire range of questions they had, given that often a single story tended to cover a limited set of issues. For example, the article written by Google focused on the benefits brought upon by its change, whereas the Electronic Frontier Foundation discussed the consequences. In wanting to obtain a rounded and unbiased portrayal of the risk, several of our participants resisted reading stories whose authors appeared to express strong opinions. One of our participants explained: "*At the end of the day the articles are quite biased especially if you read quite a few of them. I don't think I need to read other people's opinions."* Identifying whether an author was biased was often challenging and therefore led our participants to use a variable set of heuristics in order to assess each story's credibility, namely the story source, author and online medium. Conversely, a minority of our participants embraced this bias. They explicitly searched for polar opinions, which allowed them to understand the different perspectives with the aim of "*finding the truth*".

Engagement with the privacy domain was influenced by characteristics of online media, such as the presentation of each story. Participants searched for stories that were simply laid out and featured clear sections or headers. Furthermore, a few of them identified imprecise or unsupported arguments that decreased the perceived credibility of the story. To give one example, in reading about the politics of privacy, one participant disagreed with an inaccurate statement that had been made regarding US data regulation: "*The USA is one of the only countries that do not protect the privacy of information that is stored on any database. I didn't know that. I think, a statement like that…I mean it's almost certainly incorrect. By saying "one of the only countries" because I suspect there are dozens of countries, which don't, but it will almost certainly be the most important country that doesn't. Throughout Africa, throughout Asia, hundreds of countries won't protect data stored on a database.*" Finally, most of our participants repeatedly highlighted the importance for online media authors to use laypeople's language when writing about pertinent privacy issues. Many of them argued that legal terminology would disengage them with the privacy risk being covered.

DISCUSSION

This paper reported findings from participatory design research aimed at uncovering how technological interventions foster technology users' engagement with the domain of privacy. Our research was undertaken in the context of developing a new design concept "Privacy Trends" whose aspiration is to raise technology users' privacy awareness and more specifically, to foster their digital literacy regarding ongoing privacy risks while demonstrating how such risks are becoming longer term social concerns. Technically, Privacy Trends was envisaged to collect, aggregate and visualize clusters of online media stories written about ongoing privacy problems, allowing users to gain insight into a current privacy risk. We invited participants to act in the capacity of *co-designers* during which they provided input into the design of this new privacy intervention, and *users* during which they interacted with content similar to that expected to form the basis of Privacy Trends.

Engagement theory proposes that people's motivation is necessary for their initial engagement with a technology (O'Brien and Toms, 2008). As argued earlier, technology and domain are closely coupled, i.e., those motivated to engage with the privacy domain are more likely to engage with the technological intervention. In this study, we found that participants were generally not motivated to engage with the domain of privacy. Even those who declared to be the most concerned became aware of new privacy risks either by chance or through mandatory procedures enforced by their employer. Moreover, when participants used technical tools it was because they were directed by extrinsic motivations, i.e., an imminent privacy threat being perceived. The majority of our participants used virus checkers and spam filters. Influenced by their previous experience with these technologies, many of them had formed specific expectations about the role and function of privacy interventions. As a consequence, they wanted Privacy Trends to act as a delegation tool that would combat specific risks they faced, thus requiring very little involvement on their part.

Friedman and Kahn (1992) have previously warned that assistive and proactive tools can limit user agency, and argue that designers of such tools may be encouraging users to delegate moral decisions and responsibilities to the technology. Similarly, Sengers et al. (2005) propose that technology must not become the authority to what a user is doing but stimulate the user to reflect on his/her behavior. Even though authoritative tools may be the appropriate response to combat a subset of privacy risks (e.g. spam), many contemporary privacy risks (e.g. sharing on a social network site) spawn from individual users' use of technology, and are malleable to personal norms and preferences. In such cases, technology users must make sense of the risk toward forming their own opinions and responses. Our study underscores a first caveat for those wanting to develop technology users' literacy and competence with privacy: *by designing interventions that extrinsically motivate them, while teaching them that privacy decisions can be delegated, it is unlikely that technology users will develop the motivation to engage in understanding the domain of privacy*.

In their model of engagement, O'Brien and Toms (2008) additionally show that engagement with a technology is provoked and sustained when technology users' interests are reflected in technology design. Our findings show that while engaging with a privacy risk, technology users are drawn to answer the following inclusive set of questions: when a risk is being encountered, why it has happened, the nature of the problem, what actions are available and whether legal regulation exists. This suggests that the breadth of information currently included in many privacy interventions might be too narrow to reflect the rounded perspective that users seek. For example, in choosing to focus on displaying system operations to the user, Wills and Zeljkovic (2011) offered little guidance on what can be done to combat the risk. Likewise, when aiming to nudge users to change their behaviors, Maurer et al. (2011) did not present an explanation of the risk under consideration. Our study, therefore, highlights a second consideration: *privacy interventions that address a limited set of questions, for example by basing themselves within the tight remit of domain expert definitions, are less likely to stimulate users' initial engagement with the domain of privacy or to sustain it*.

In the present study, technology users' engagement with the domain of privacy was investigated within a design activity. There is no doubt that engagement was fostered or hindered due to the particular characteristics and constraints of this design context. The remainder of this paper unpacks four key areas of possible development for privacy intervention design suggested by this contextual investigation.

Allow The Space For Interpretation

Engagement theory features control as an imperative feature of engagement (O'Brien and Toms, 2008). Sengers et al. (2005) elaborate on this to suggest leaving the design space open in order for users to "maintain control of and responsibility for the meaning-making process". In applying this principle to the context of learning, previous research has found that engagement follows from people's freedom to construct their own knowledge. At the centre of this process is the ability to exercise agency and control in defining one's learning goals (Zepke and Leach, 2010). Lord (1997) compared a teacher-led environment with one that supported students to construct their knowledge and found that students in the latter setting performed better and also became engaged with the subject matter more generally. Schuetz (2008) showed that autonomous learning, characterized by the student's ability to integrate knowledge in ways that resonates with their experiences, was a driving force in students' continued participation in education. In inviting participants to define what components of privacy were personally important to them, two core characteristics of our methodology were its *agency* and *openness*. This enabled our participants to negotiate and integrate the multiple perspectives that different authors brought to privacy into one cohesive story. In addition to this, by choosing what issues within each story were important to further pursue and analyze, our participants were able to set their own learning goals and to explore them against their experiences and knowledge (Kolb, 1984). As a consequence, each of them experienced a different learning trajectory. Basing ourselves on the learning prospects fostered by our methodology, we highlight the importance of creating experiences that will allow the space for multiple interpretations and that are malleable to fit with users' diverse mental models, priorities and interests. Designers can achieve this, for instance, by exposing technology users to ambiguous representations of privacy, or to different and contrasting opinions and/or perspectives on privacy, which can allow them to imbue the content or representation presented with their own meaning.

Scale Privacy From A Personally Relevant Risk To A Social Issue

Our participants initially approached the information exploration activity by taking a goal-oriented viewpoint, i.e., centered on the immediate resolution of the risk. They sought to make sense of Google's privacy policy change, its assumptions and boundaries, as well as its application to themselves and close others. As they went along, however, they gradually began to explore privacy as a social issue. Although many participants concluded that they were not at risk, they were motivated to continue interacting with the activity in order to explore and stretch how Google's privacy policy fits within current social, organizational and political systems. This dual engagement with the privacy domain, i.e., goal-oriented and civic, was also evident when participants adopted the role of the designer. While some were quick to propose Privacy Trends as a tool for personal safety, others suggested the inclusion of metrics that might express the magnitude of the offence and consequently hold the offender accountable. Moreover, while all of our participants requested to learn about risks relevant to their own technology use, others wanted to engage with risks that were important to know as digital citizens. Our findings demonstrate that designing to support this multi-layered nature of privacy can lead to different but complementary outcomes. Developing the privacy intervention as a goal-oriented activity can provide users with the initial motivation to engage in privacy, and advance their understanding of the risk under scrutiny. Presenting the risk against its complex socio-political context can create a prolonged dialogue and engagement, and encourage them to generalize a particular case to existing social structures. In embodying this principle, designers can extend existing, context-aware privacy interventions by linking them to resources that express the risk's social and political implications.

Scaffold And Guide Reflection

While reading each online media story, we asked participants to highlight areas of the text that were important to them personally. This revealed that technology users want to answer a finite set of questions about a new privacy risk: e.g. what is the nature of the risk? These questions were posed and answered as participants prioritized and annotated a series of online media stories. This type of directed interaction created a scaffold that proved to be critical: by asking our participants to highlight important areas of text we encouraged a form of annotation that has been previously featured in technological systems wanting to incite reflective thinking (e.g. Pike et al., 2009; Rich and Hannafin, 2009). Therefore, even though our study underscores the importance of allowing the space for interpretation, it also reveals the necessity of including mechanisms that will support technology users to answer personally relevant questions about privacy. Such mechanisms can provide a scaffold for reflection as long as they are designed to strengthen technology users' interests.

Examples of guiding reflection through design may include directed annotations, prompts, or storytelling applications that allow technology users to construct their own narratives of privacy risks.

Present Privacy As A Comprehensive Concept

Our participants' engagement with the domain of privacy was moderated by the perceived comprehension of a given online media story. Stories that covered one facet of privacy (e.g. its consequences), neglecting others, were perceived to be incomplete. This motivated participants to continue looking for answers within other sources. In addition to seeking breadth of information, comprehension was increased when a story was well organized into manageable and easy to read sections. It was influenced by the author's reflexivity and whether it was grounded in accurate examples and arguments. Additionally, it was increased when the author's story was written for laypeople. Comprehension, therefore, emerged as a foundational design principle for engagement with the privacy domain and a possible cause for disengagement. In applying this principle, online media authors may construct their texts to cover the questions that technology users want to answer while at the same time provide structure to the way the text is organized.

CONCLUSION

The aim of this paper was to establish how privacy interventions could be designed to foster users' engagement with the privacy domain. Our investigation took place during the design process of a new privacy intervention, Privacy Trends. Our first contribution is to reveal a set of challenges in relation to how privacy interventions are currently being designed. Many interventions have relied on extrinsically motivating technology users to attend to privacy matters through the threat of potential consequences, while at the same time offering authoritative solutions that diminish users' agency. As a consequence of this, we found that technology users had formed expectations that privacy risks can be handed over to technologies. Such expectations were also fuelled by their sense of inertia about privacy, present even amongst those reporting to be most privacy concerned. Moreover, we found that technology users made sense of a privacy risk through a broad but yet consistent inquiry – ranging from attaining an understanding of the nature of the risk, to the responses that were available to them. In reviewing existing privacy interventions, we observed that they only met in part the breadth of information that technology users seek.

The second contribution of our research stems from its aim to offer solutions to the shortcomings it identified. By observing how technology users engaged with the domain of privacy in the context of an intervention under development, we were able to uncover new design principles for privacy interventions at large. Our findings emphasize the importance of leaving the space open so that technology users can situate privacy against their knowledge and experience. Moreover, we found that engagement with the domain of privacy can be prolonged and deepened by presenting privacy as a personal as well as a socio-political concern. We also identified the role of reflection in deepening participants' understanding and encouraging inquiry. Finally, we discovered that our participants engaged with the privacy domain as long as the information they consumed was credible and accessible.

Our research reframes the 'privacy problem' by arguing in favor of a shift from approaches that seek to influence technology users' information-sharing behavior, to approaches that will additionally foster learning by creating engagement with the domain of privacy. Our design principles emphasize technology users' capacity to be autonomous learners whose experiences are central to their understanding of the domain. While our hope is that this research may open up new directions for the design of privacy interventions, we believe that the implications of our findings go beyond the realm of design. Privacy researchers who want to create more engaging methodologies can use our design principles to inform their methodological decisions. Our findings also offer guidance to designers of text analytics applications (e.g. SRSR) by highlighting the potential value of developing cues that will support technology users' interpretation of divergent or convergent perspectives with regards to social issues. Finally, by revealing a rounded portrayal of what technology users want to know about privacy and how they want information to be presented, our study provides guidance to online media authors and public communicators for crafting their stories.

ACKNOWLEDGEMENT

This research was funded by a Google Research Award granted to the first author. We gratefully acknowledge Jens Riegelsberger, Martin Ortlieb, Charlie Pinder, Tim Ryles and Rilla Khaled for numerous inspiring discussions about this work.

REFERENCE

Acquisti, A. and Grossklags, J. Privacy and Rationality in Individual Decision Making. *IEEE Security and Privacy* 3, 1 (2005), 26-33.

Acquisti, A. Nudging Privacy: The Behavioral Economics of Personal Information. *IEEE Security and Privacy* 7, 6 (2009) 82-85.

Adams, A. and Sasse, A. Users Are Not The Enemy. *Commun. ACM* 42, 12 (1999), 40-46.

Baumer, D. L., J. B. Earp, et al. (2004). Internet privacy law: a comparison between the United States and the European Union. Computers & Security 23(5): 400–412.

Brunk, B. D. (2002). Understanding the Privacy Space. First Monday 7(10).

Chakrabarti, D., and Punera, K. (2011). Event summarization using tweets. In Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media (pp. 66-73).

Chapman, E. (2003). Alternative approaches to assessing student engagement rates. Practical Assessment, Research & Evaluation 8(13).

Coles-Kemp, L. and D. M. A. Ashenden (2012). Community-centric engagement: lessons learned from privacy awareness intervention design. Proceedings of HCI 2012. The 26th BCS Conference on Human Computer Interaction.

de Paula, R., Ding, X., Dourish, P., Nies, K., Pillet, B., Redmiles, D.F., Ren, J., Rode, J.A., and Silva Filho, R. In the eye of the beholder: a visualization-based approach to information system security. *Int. J. Hum.-Comput. Stud*. 63, 1-2 (2005), 5-24.

Deci, E.L. 1992. The relation of interest to the motivation of behavior: A self-determination perspective. In Renniger, K.A. Hidi, S. Krapp, A. (eds) *The role of interest in learning and development*.

Diakopoulos, N., De Choudhury, M., and Naaman, M. 2012. Finding and assessing social media information sources in the context of journalism. In Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems (CHI '12). ACM, New York, NY, USA, 2451-2460.

Diamond, L. Liberation Technology. Journal of Democracy 21, 3 (2010), 69-83.

Dickey, M. (2005). Engaging By Design: How Engagement Strategies in Popular Computer and Video Games Can Inform Instructional Design. ETR&D 53(2): 67–83.

Dourish, P. and Anderson, D. Collective Information Practice: Exploring Security and Privacy as Social and Cultural Phenomena. *Human Computer Interaction* 21, 3 (2006), 319-342.

Dourish, P., Grinter, R. E., de la Flor, J.D. and Joseph, M. (2004). Security in the wild: user strategies for managing security as an everyday, practical problem. Personal Ubiquitous Computing 8: 391–401.

Egelman, S., Oates, A. and Krishnamurthi, S. 2011. Oops, I Did It Again: Mitigating Repeated Access Control Errors on Facebook. *In Proceedings of the SIGCHI conference on Human Factors in Computing Systems* (CHI '11). ACM, New York, NY, USA, 2295-2304.

Fallman, D. 2003. Design-oriented human-computer interaction. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '03). ACM, New York, NY, USA, 225-232.

Fallman, D. 2005. Why Research-Oriented Design Isn't Design-Oriented Research. Proc. NordiCHI 2005, Umea Institute of Design Press.

Friedman, B. and Kahn, P.H. Human agency and responsible computing: Implications for computer system design. *Journal of Systems and Software* 17,1 (1992) 7-14.

Jensen, C., and C. Potts, (2004). Privacy policies as decision-making tools. Conference on Human Factors in Computing Systems (CHI), Vienna, Austria, ACM Press.

Kani-Zabihi, E. and Helmhout, A., 2012. Increasing Service Users' Privacy Awareness by Introducing On-Line Interactive Privacy Features. *In proceedings of NordSec*, 131-148

Kani-Zabihi, E. and E. Wattam. (2010). Understanding users' requirements with respect to privacy: A mixed-method research methodology. Retrieved 1/07/2013, from http://scone.cs.st-andrews.ac.uk/pump2010/slides/kani-zabihi.pdf.

Kearsley, G. and B. Shneiderman (1998). Engagement Theory: A Framework for Technology-Based Teaching and Learning. Educational technology 38(5): 20-23.

Kirlappos, I., Sasse, M. A. Security Education against Phishing: A Modest Proposal for a Major Rethink. *IEEE Security and Privacy Magazine* 10, 2 (2012), 24-32.

Kolb, D.A. 1984. *Experiential learning: experience as the source of learning and development*, Englewood Cliffs, NJ: Prentice Hall.

Kwak, H., Lee, C., Park, H., and Moon, S., 2010. What is Twitter, a social network or a news media?. In Proceedings of the 19th international conference on World wide web (WWW '10). ACM, New York, NY, USA, 591-600.

Lord, T. R. (1997). A comparison between traditional and constructivist teaching in college biology. Innovative Higher Education 21(3): 197-216.

Marcus, A. Bernstein, M.S, Badar, O., Karger, D.R., Madden, S. and Miller, R.C. 2011. Twitinfo: aggregating and visualizing microblogs for event exploration. In *Proceedings of the 2011 annual conference on Human factors in computing systems* (CHI '11). ACM, New York, NY, USA, 227-236.

Margulis, S. T. On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues*, 59, 2 (2003) 411-429.

Mazzia, A., LeFevre, K., and Adar, E. 2012. The PViz comprehension tool for social network privacy settings. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (SOUPS '12). ACM, New York, NY, USA, Article 13, 12 Pages.

Maurer, M., De Luca, A., and Kempe, S., 2011. Using data type based security alert dialogs to raise online security awareness. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (SOUPS '11). ACM, New York, NY, USA, Article 2 ,13 pages

O'Brian, H., Toms, E., 2008. What is user engagement? A conceptual framework for defining user engagement with technology. JASIST 59(6), pp. 938-955.

Palen, L. and Dourish, P., 2003. Unpacking "privacy" for a networked world. *In Proceedings of the SIGCHI conference on Human factors in computing systems* (CHI '03). ACM, New York, NY, USA, 129-136.

Rader, E., Wash, R., and Brooks, B. 2012. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (SOUPS '12). ACM, New York, NY, USA, Article 6 , 17 pages.

Rich, P. J., and Hannafin, M. Video Annotation Tools Technologies to Scaffold, Structure, and Transform Teacher Reflection. Journal of Teacher Education, 60, 2 (2009) 52-67.

Rode, J. A. 2009. Digital Parenting: Designing for Children's Safety. In Proceedings of HCI 2009.

Pike, W.A., Stasko, J. Chang, R. and. O'Connell, T.A. *The science of interaction. Information Visualization* 8, 4 (2009), 263-274.

Sanghvi, J., C. Castellano, et al. (2011). Automatic analysis of affective postures and body motion to detect engagement with a game companion. Human-Robot Interaction (HRI).

Schuetz, P. (2008). Developing a Theory-Driven Model of Community College Student Engagement. New Directions for Community Colleges. Wiley Periodicals, Inc. 144.

Sengers, P., Boehner, K., David, S., and Kaye, J.J., 2005. Reflective design. In *Proceedings of the 4th decennial conference on Critical computing: between sense and sensibility* (CC '05), Olav W. Bertelsen, Niels Olof Bouvin, Peter G. Krogh, and Morten Kyng (Eds.). ACM, New York, NY, USA, 49-58

Schön, D.,1983. The Reflective Practitioner: How professionals think in action. London: Temple Smith.

Social Mention. Retrieved on September 1, 2012. http://www.socialmention.com/about/

Whitten, A. and Tygar, J. D., 1999. Why johnny can't encrypt: A usability evaluation of PGP 5.0. In *Proceedings of the 8th USENIX Security Symposium*,169–184.

Wills, C.E. and Zeljkovic, M. A personalized approach to web privacy--awareness, attitudes and actions. *Information Management and Computer Security* 19, 1 (2011) 53-73.

Vasalou, A., A. Gill, et al. (2011). Privacy dictionary: A new resource for the automated content analysis of privacy. JASIST 62(11): 2095-2105.

Zepke, N. and L. Leach (2010). Improving student engagement: Ten proposals for action. Active Learning in Higher Education 11(3): 167-177.