Understanding the Experience-Centeredness of Privacy and Security Technologies

Paul Dunphy[1], John Vines[1], Lizzie Coles-Kemp[2], Rachel Clarke[1], Vasilis Vlachokyriakos[1], Peter Wright[1], John McCarthy[3], Patrick Olivier[1]

[1]Culture Lab
School of Computing Science
Newcastle University
{forename.surname}@ncl.ac.uk

[2]Information Security Group
Royal Holloway
University of London
lizzie.coles-kemp@rhul.ac.uk

[3]School of Psychology
University College Cork
Republic of Ireland
john.mccarthy@ucc.ie

ABSTRACT
The joint study of computer security, privacy and human-computer interaction (HCI) over the last two decades has shaped a research agenda focused upon *usable privacy & security*. However, in HCI research more generally there has long been an awareness of the need to understand and design for user experience, in recognition of the complex and multi-faceted role that technology now plays in our lives. In this paper we add to the growing discussion by introducing the notion of *experience-centered privacy and security*. We argue that in order to engage users of technology around issues related to experiences of privacy and security, research methods are required that may be outside of the normal repertoire of methods that we typically call upon. We describe three projects that developed non-typical research methods to reveal experiential insights into user interactions with privacy and security-related technologies. We conclude by proposing a research agenda that begins to illustrate how the discourse and methods of experience-centered design might serve to provide valuable alternative perspectives on new and enduring user-facing privacy and security problems.

ACM Classification Keywords
H.1.2 [User/Machine Systems]; K.4.m [Computers and Society]: Miscellaneous

General Terms
Design, Security, Human Factors

Keywords
Experience-centered security; experience-centered privacy; design methods; user experience, usable privacy and security.

1. INTRODUCTION
In their 1996 article 'User-centered security', Zurko and Simon brought about a new paradigm in secure systems research that has in recent years become the predominant way to align information security and privacy with the consideration of human factors. This new paradigm called for the development of "*security models, mechanisms, systems, and software that have usability as a primary motivation or goal* [46]". Today, nearly twenty years later, interactions with digital technologies—and their associated security and privacy features— now pervade almost all of human life. In the wider field of human-computer interaction (HCI), this reality has forced reflection not only regarding how technology is designed to account for the multifaceted lives of users, but also how we can understand design requirements and user needs in increasingly diverse contexts of use. For some time now, much HCI research has orientated towards understanding user experience [22][1] and designing in an *experience-centered* manner [43]. This approach reflects a new sensitivity to the complex role that technology now has in our lives, and that, today, successful technologies are those that respond sensibly to the needs and values of users, and are not necessarily those that are the most usable. Despite this wide acceptance that experience is a fundamental aspect of how we should study technology use and design new systems, this idea has been slow to find traction in information security and privacy research.

In this paper, we argue that an experience-centered approach to privacy and security research is particularly appropriate, as many enduring concerns around understanding user behavior can only be explained experientially (e.g. user perceptions, mental models, trust, compliance etc.). For instance, people share passwords with partners, contrary to the conventional wisdom to not share passwords [18]; new user authentication systems that present security improvements over existing systems do not 'feel' secure [9], yet some supposedly antiquated and insecure systems do [38]. The difficulty in engaging with insights of this type using our predominant quantitative and qualitative methods means that we still have a lack of knowledge about the subjective yet fundamental ways that people make security and privacy decisions, reflect upon those decisions, and express needs. Of course, in this area, attackers have long been more attentive to the experiential underpinnings of digital technologies than designers themselves [23].

Attending to the challenge of studying and designing the experiential aspects of security and privacy technologies is difficult. Indeed, design problems in these domains can be thought of as wicked problems [30]: problems that are difficult to define; are interconnected with other problems; and have other complicating characteristics that inhibit overarching insights and all-encompassing solutions. Approaching problems of this type requires the application of research methods that embrace—rather

NSPW '14, September 15-18, 2014, Victoria, BC, Canada.

http://dx.doi.org/10.1145/2683467.2683475.

[1] User experience is a widely used/abused term. For our purposes the consideration of experience encompasses the practical and affective aspects of interaction with technology [22].

than abstract away—the complexity of modern day interactions with technology. Our contribution in this paper is to enhance the debate of the applicability of experience-centered methods to problems in security and privacy [20,21]. We firstly identify challenges currently facing empirical user research in this domain; secondly, we describe three case studies that developed and applied experience-centered methods to uncover security and/or privacy insights. In doing so we aim to invigorate discussion around *who* participates in our empirical research and indeed, *how* they participate. To conclude, we propose specific future challenges and opportunities that an experience-centered approach might bring to security and privacy research.

2. HCI FOR SECURITY AND PRIVACY

The evolution of the field of HCI's thinking about users in the context of security and privacy technologies has been widely recounted (e.g. [21]). Here we revisit it briefly as a foundation for describing our experience-centered approach.

Information security has its roots in the military, where users were treated principally as a source of threats. The pursuit of public-key cryptography carried with it the hopes of a future world of secure communications for everyone. This hope eroded in the 1970s with the realization that contextual factors could undermine the cryptography itself. The potential impact of usability upon security was noted in 1975 by Saltzer and Schroeder [31]; twenty-four years later and their concerns of designing security with the assumption of an 'expert user' were born out when Whitten and Tygar performed an evaluation of *Pretty Good Privacy* with damning usability results and significant security implications [41]. Further, Davis [5] suggested that public-key infrastructures were not suitable for non-expert users, and that many of their operational benefits were only brought about by this problematic assumption of expert users. Around the same time, Zurko and Simon [46] proposed that learning from techniques used in HCI could help the security community improve their ability to design systems suitable for the average user. Furthermore, the adoption of frameworks of usability appeared compatible with the mathematical roots of the field. The following years would confirm the value of usability as a critical consideration in the design and evaluation of user-facing privacy and security mechanisms [3].

2.1 Understanding Users in the field of Computer Privacy and Security

It is challenging to understand the needs and practices of users in the context of information security and privacy, as these dimensions of digital technology are considered to be secondary concerns for users [41]. Also, the technologies we design must fulfil the difficult task of warning users about abstract threats, or requesting decisions on matters that users may not fully understand. In response, research has focused upon a number of pressing areas including: persuading users to behave more securely [13]; preventing users from behaving insecurely [44]; scaffolding usable functionality around systems with poor usability [11]; proposing systems that take better account of human cognitive limitations [1] or to educate users about the threats they may face [33]. The particular research methods that are applied to judge the success of an intervention or to capture user requirements greatly influence the insights that will be revealed. For instance, it is widely known that behavioual research study designs are subject to a myriad of demand characteristics [26], particularly where they focused upon studying *what* people do, and *why* they do it. For example, participants may sense that a study is checking up on their security or privacy hygiene and may not wish to disclose any deviance from 'responsible' behavior as this might create opportunities for unwanted judgment of their personal values or routines. This is accompanied by the additional issue that participants may find it difficult to articulate their practices or needs on technical matters, or indeed may be embarrassed to reveal a lack of interest in such an apparently important topic. This reality can often be invisible to researchers due to the pervasive nature of verbal or written 'good practice' in society, which means that people with very little knowledge of the subject matter might still be able to assemble convincing accounts of highly conscientious practices, even if their personal understanding does not align with the vocabulary they are using. A qualitative approach, in and of itself, is not a solution, as such studies can suffer from the same biases too. As a result, we often see a dichotomy in terms of what people say they do, and what they actually do. These results are usually rationalized by asserting that users themselves are irrational and not aware of the importance of foregrounding these matters in their everyday lives. An alternative perspective could be that people have their own values in this area that are poorly understood and not yet valued in how privacy and security technologies are designed.

Of course, the problem of understanding and studying subjective preferences and tacit behaviors appears to be a class of problem often referred to as a wicked problem [30]. Problems with these characteristics are often referred to as being *"fuzzy"* in informal discourse. This outlook actually discounts that a number of core concerns in security and privacy have considerable wicked components. User authentication can be considered one such wicked problem; the problem of gaining secure access to a computer system. Indeed, the absence of a silver bullet authentication solution after extensive research over the years has forced reflection upon why the study of usability and security has so far not identified a successor to the password [16]. This multi-faceted problem encompasses the challenge of technical design (e.g. password entropy), policy design, user trust, perceptions of security, and uncertainty of how users might appropriate authentication technologies into their lives. User authentication -- like many digital security and privacy issues – reflects a hard social problem. The desire to design better technology in the face of such complexity requires conceptualising security and privacy technologies in much broader terms; and requires that researchers apply methods that capture hidden user needs or tacit practices related to how people treat security and privacy as an everyday problem [8], and as a collective practice [7].

3. EXPERIENCE-CENTERED DESIGN AND SECURITY AND PRIVACY

In their call for experience-centered design, McCarthy and Wright [43] consider understanding human lived experience as a route to bridging the gap between those who design and those who live with technologies. Central to experience-centered design is the notion of empathy. Empathy in a design process is about remembering your own view of the world while seeing the world through the eyes of somebody else. Our ability to empathize with a person, to identify their feelings and understand their perspectives is challenging; particularly in contexts where we work with people who may find it difficult to recognize or articulate their own needs, or who may see the world very differently to the designer [42]. Much of what we know of the world, and our skilled behavior is tacit, and much of an

Figure 1: Online privacy discussion captured on a collage created in a railway station with engagement led by an actor.

experience-centered design process is about making this tacit knowledge visible. As such, an experience-centered approach prioritizes the need to develop a rich understanding of people's practices and lives.

Such an outlook provokes reflection upon how we currently ask users to contribute to security and privacy research. Users tend not to be experts on the subject, which creates an asymmetric relationship between designers and the users they encounter. This dynamic implicitly lends itself to a designer assuming the role of a 'protector', in that their values are quite likely to take precedence over the values of the user. We are not advocating that we should be blindly responsive to what users want in future technologies, but we do advocate that researchers should have a greater awareness of what users can contribute to the design of those technologies. As researchers, we bring expertise of security, privacy, and technology design, but users also bring expertise in terms of how they live their lives, how existing or proposed technologies fit into their routines, what is of value to them and what they aspire to in the future.

An experience-centered approach takes that dialogue is crucial to creating parity between designer and user. If we are to take the meaning of dialogue seriously, then it means more than simply interviewing and talking to potential users. Indeed, dialogue implies: (i) openness and creativity in how we engage with others; (ii) responsiveness to another's needs, aspirations and concerns; (iii) actively listening and withholding judgment [43]. Storytelling is a common vehicle to engage someone in dialogue—indeed, recent research has even suggested the value of user storytelling in relation to security issues [28]. Considering these three facets and the notion of storytelling, we can see how an interview protocol that runs through a list of pre-determined questions is not dialogue.

We suggest that security and privacy research should take seriously the ideas from experience-centered design where it must: develop an understanding of context-specific user practices (what they are, and why they happen); gain fundamental insights into subjective user perceptions of security or privacy; theorize about the fit of technologies into people's lives; or generate inspiration for new technology. Doing so may facilitate a more discursive approach to studying and exploring the behavior of users, and enable the research community to more actively probe the everyday relationship between people, security and privacy. In making this argument, we build upon Mathiasen and Bødker's [20] first articulation of the implications that human experience has to security. In this earlier work, a new method was proposed called 'acting out security' as a means to enable people to envision using a future payment system. Other archetypal methods proposed in this space include scenarios, role-plays, probes and experience prototypes [43]. While these are common methods that could be used already, our experience of using experience-centered design methods in sensitive contexts has highlighted how very often our methods of engagement must be tailored to the problem under investigation, and the user group of focus.

In the following we describe three case studies that provide examples of how experience-centered methods can be developed to yield non-trivial privacy and security insights and new perspectives on user participation in privacy and security research. These case studies are not intended to represent a gold standard in how to conduct this type of research. Indeed, every context should be considered differently. Instead we provide these examples as ways of articulating the benefits of using methods of experience-centered user engagement that take seriously the notions of openness, creativity, responsiveness and actively listening. In each case study the overall project motivations are briefly described, but we focus on an exemplar method of user engagement that was important as a means to facilitate dialogue around existing security or privacy practices.

4. CASE STUDY 1: VOME

Visualization and Other Methods of Expression (VOME) was an interdisciplinary project that focused on questions related to privacy, identity and consent in online services. From the start, VOME set out to engage with under-represented communities who, to date, had not been included in privacy design studies and therefore addressed the fundamental question 'Usable privacy for whom?'. The inclusion of local government authority as a project partner focused the project on privacy in the context of public service delivery, and many of the project's case studies and user participation came from economically deprived communities within the region. One such case study was the development of a series of new online services aimed at teenagers who were at risk of offending. This included new smartcard-based schemes where children from poor families were given credits that could be used to pay for 'positive activities' across the city. Issues of trust, conflicting perceptions of security and different perceptions of risk were amongst a number of issues that could not be teased out using traditional research methods.

4.1. Methods

In VOME, there was an emphasis on exploring experiences and feelings related to being online. The methods of engagement

Figure 2: Examples of speculative ideas for security technologies presented on 'questionable concept' cards [37]**: (i) Disappearing money; (ii) smart wallet; (iii) biometric pin thimble; (iv) content inside the card itself.**

developed in this project were chosen to explore how members of the public felt about security and encouraged a pluralist approach where different and often conflicting views were articulated. The findings from public engagements were used to develop thinking tools that helped users explore the privacy issues and decide how to respond to questions related to what information to share, when, and with whom.

4.1.1. Highlighted Method: Collage Building

The collage building approach is a participative activity in which four simple research questions were asked about topics related to online privacy using language that resonated with the participant groups. In some instances, rather than use researchers to ask initial questions, performance artists were used to engage participants and ask the initial questions. For example, one engagement was conducted in a railway station where participants were spontaneously recruited with the assistance of a performer (see Figure 1). Participants were asked four questions: what secrets do you keep online? What secrets do you look for online? Tell us something about yourself that nobody knows online; Tell us a secret about where you live. Participants could choose a minimum of two out of four methods of engagement to address these questions: drawing pictures of secrets, recording verbal answers, writing responses and taking photographs that visualized their response.

The insights gained from the collage building activities highlighted that for many of those to whom we spoke, a prominent concern is around secrets related to relationships and relationship management. This is also repeated in the recorded narratives that we collected. In contrast, participants regarded deception with regards to others gaining access to personal and biographical details such as age and name as routine and not of significance. In particular the collage brought out the important point of "playfulness" in the context of social media use and authentication. Traditionally, authentication technologies such as passwords and smart cards are evaluated in terms of their usability and in terms of their strength against guessing attacks. The responses on the collage show that in the case of social media, bypassing password mechanisms is a common activity in close relationships and seen as a playful activity.

The responses on the collage also illustrated the wicked problem of social media users being both the hunter and the hunted. Many contributions articulate how social media users like to keep secrets online but also find out the secrets of others. This highlights the playfulness of system subversion in certain contexts. This playful duality is an important point for consideration when designing online safety messages and online safety functionality. Current work in this area focuses on the social media user as a potential victim, ignoring the fact that the same individuals may also be willing to subvert the system and might regard both carrying out and being the target of such actions as a form of game. This further introduces the problem of these actions being interpreted and re-interpreted differently over time with actions that were once regarded as playful being re-interpreted as sinister if the relationship breaks down. An important principle that underpins the collage building as a method for experience-centered privacy is that it is constructed in a public place with participants controlling what is disclosed and how it is presented. Using this research approach, participation took place on the terms of the participants. The collage encouraged the use of language natural for the local community, and encouraged participants to talk about subjects on which they were familiar and knowledgeable. This method also leveraged participatory techniques to create a space in which researchers and participants could work together to draw out the more tacit aspects of information production and sharing.

5. CASE STUDY 2: BANKING FOR THE OLDER OLD

'New Approaches to Banking for the Older Old' was a project that examined the financial practices of 'eighty somethings' (people aged over 80 years) in the UK. The project's scope was to understand the ways in which this age group managed their finances and identify reasons why they may be excluded from benefitting from technological innovations to banking services and payment systems. During the time that the research was undertaken there were a number of important changes to how people received their state pensions in Britain. Those who had for years relied on cash were now being forced to open bank accounts in order to receive their weekly payments. Furthermore, the banking industry was at the same time threatening to withdraw cheques ('checks' in the USA and Canada) [38] from circulation—a payment method that large numbers of this age group relied upon. Many of the participants raised the latter as a primary issue of concern during workshops with researchers. As a result, much of the project focused on exploring the trust mechanisms underlying cheques and developing services and technologies that allowed people to keep using this payment method once the banks withdrew this service.

5.1. Methods

Providing a context where people felt comfortable talking about their personal finances with others was a fundamental issue the researchers had to address. The project began with typical ethnographic work, and a number of novel methodological approaches were developed to support engagement with participants. Noting that it would be difficult for people to discuss

Figure 3: Inspiration tokens with portrait pack and collage of photographs created by one of the women in the workshops [2]**.**

their finances with a stranger, the researchers used a 'financial biography' approach to interviewing participants. This focused on having participants talk about their life story with more focused follow-up questions about finances as they related key stages in their lives. Later in the project, techniques such as questionable concepts, and technology prototyping facilitated both public and private disclosures of financial and security practices.

5.1.1. Highlighted Method: Questionable Concepts

Questionable concepts [37] was a method used by the researchers to link their initial ethnographic fieldwork with later co-design sessions with new groups of eighty somethings. The concepts themselves were critical design responses to some of the problems revealed from the ethnography stage of the research. For example, one of the concepts, 'disappearing money', speculated the existence of intelligent banknotes where the Queen's face and the value of the note disappeared when handled by an unauthorized person. The idea, albeit deeply speculative, was grounded in issues emerging from the ethnographic data where housebound participants found themselves reliant on friends, neighbors and carers to pay for bills or purchase groceries on their behalf. It had been noticed that there was an implicit trust of those they handed money over to—yet there had been occasions where cash had gone missing, or where participants had shared their debit cards and PINs and had money stolen from their account. Therefore, 'disappearing money' was both a practical and questionable response to these problems. It speculated novel authentication approaches where money could be exchanged with an intermediary but only spent in specific shops or locations. Yet at the same time it challenged the very trust mechanisms that the eighty somethings valued. During meetings with participants, the discussion around speculative ideas like this gave the researchers insight into how participants formed mental models and perceptions of trust and security around the perceived qualities of future technological systems.

In order to link the ethnographic and the co-design phases of the project, the questionable concepts were placed onto cards that were given to participants to take away following an initial design workshop. The cards had an illustration of the concept on the front (see Figure 2 for an example). On the inside there was a brief description of the idea and a number of quotes from the financial biographies that the design was based upon. The remainder of the card posed a series of open questions for participants to respond to. These questions were intended to gauge how much these individuals shared the concerns and experiences of prior participants and for them to imagine future scenarios.

As a method for experience-centered security, questionable concepts was a valuable tool for a number of reasons. First, they offered participants an opportunity to reflect on the needs of others and empathize with how their personal circumstances were different to those we had worked with earlier in the project. Second, the sheer 'questionability' of the concepts presented numerous opportunities for critique. Participants would register their disdain for the ideas in a variety of ways—by scribbling over ideas, by writing *"wrong!"* or *"never!"* over the participant quotes; by writing long responses to questions pertaining to the deep problems within society that they associated with the suggested ideas; or by simply deciding not to answer any questions on specific cards. These criticisms, however, provided rich insight into what the participants truly valued. For example, negative reactions to the 'smart purse' lead to written responses and workshop discussions around the role of keeping meticulous records of financial transactions. It appeared that the effort of making these records and keeping them up to date provided a deep sense of security and comfort. Participants *"knew where they were"* money-wise at any point in time, and could challenge their banks if they felt there were inaccuracies in their computerized records. Responses to 'disappearing money' were similarly critical, where a number of participants noted that such sophisticated but non-digital payment methods already existed, referring to the paper cheque that was in the process of being abolished. The power of the method was in harnessing critiques in a way that allowed participants to articulate their existing practices (without interrogation) and state very clearly their meaning as with respect to these unusual ideas the research team presented to them.

Crucially, the insights generated from the questionable concept cards led to new design directions focusing on the experiential phenomena surrounding banking and finances. For example, a community-based cheque service was developed with participants that privileged the need for record keeping and provided a payment method that could be kept within a local community of trusted payees and service providers [36].

6. CASE STUDY 3: PRIVACY IN ABUSIVE RELATIONSHIPS

The final project was a long-term collaboration between an international women's center and charity in the UK that provides counseling, social support and education for women leaving abusive relationships. Our first phase of research was to understand how women that come to the center managed privacy in light of their changes in circumstance. Our focus was in identifying tensions and conflicts in their use of photo taking and sharing technologies. The study was developed against a backdrop of increased government support through the Ministry of Justice advocating the value of social networks for women leaving abusive relationships.

Increasingly, staff at the center were aware of digital content being appropriated as a means of continued control asserted by the perpetrator. At the same time, staff highlighted that women also enjoyed taking digital photographs and sharing them among one another as a means of building friendships. The research then largely focused on understanding photo-practices in the center through action research and participatory art practice and techniques. Through a series of workshops, women who used the center shared photographs that were meaningful for them while avoiding disclosing private information online to others and discussing their concerns in a safe trusted environment.

6.1. Methods

Understanding what privacy means for women in the context of moving on from abusive relationships presented a number of methodological challenges. Conducting interviews would have been difficult since the women were often nervous around people who were unfamiliar and were particularly suspicious of people from large institutions such as universities. Initial fieldwork and a digital storytelling project was initiated to engage the women in building relationships and confidence with the researcher around their common experiences. These early engagements underlined an awareness of the consequences of disclosing what might be perceived as inappropriate visual imagery to friends, family and center staff and an acute awareness of the importance of presenting the right kind of positive image. Following this we developed an approach we called digital portraits, which extended the storytelling process to specifically consider how photo-sharing practices were managed by privacy concerns.

6.1.1. Highlighted method: Digital portraits

The digital portraits approach was used as a design method, akin to the *cultural probe* [14], but with an extended period of engagement with a small group of women at the center. The approach built upon our earlier fieldwork and digital storytelling sessions, highlighting creativity, adaptability, and resilience in the women's abilities in managing complexity. Rather than focusing on the managing of photographic privacy as a problem, we underlined the more generative potential of privacy as an issue of personal appropriate choices, choices that were highly attuned to each individual woman's circumstances.

The approach served as a means of paying particular attention to how the women visually negotiated their privacy preferences in the context of the center. Like cultural probes, a portrait pack (see Figure 3) was created that contained a portrait frame and a set of inspiration tokens, a digital sound recorder and digital camera in a velvet bag with a set of instructions. The instructions asked the women to take photographs of the things in their lives they valued and use the tokens for inspiration if they were stuck for ideas. The women were encouraged to only bring photographs to workshops that they were comfortable sharing with others. Over several weeks, each of the participants created a collage and video sequence with the photographs they had chosen. They wrote words or chose music to go alongside their images, reviewed their videos and made changes in light of sharing these with staff, other women at the center and the researchers. Finally, a selection of statements was presented back to the women and the center's staff for further reflection and discussion.

Digital portraits was a valuable method to gain nuanced insights for experience-centered privacy, which would have been overlooked using more traditional privacy heuristics. Participants were encouraged to reflect on their sharing preferences in response to a practical and situated task and reflect on those choices dynamically over a number of weeks. In doing so, tacit decision-making processes in relation to images were tried out and changed in response to other women's choices and the context. The longitudinal nature of the work also enabled trust to be built between researchers and participants. This meant the women became more comfortable disclosing issues and concerns associated with the sharing of the photographs that otherwise may not have been shared.

Most importantly the method challenged researcher and staff assumptions on what privacy meant in the context of photo-sharing in the center, in particular on how logical, rational choices were difficult to make. Furthermore it encouraged a re-thinking of photographic material as more than just data or information. Focusing on visual representation and decision making to create photographic content emphasized the value the women placed on their image making capacity and their ability for meanings to change over time. This eventually led to the design of a digital photo-album for use at the center that enabled a more situated negotiation of privacy over photographs on the display that also supported sociality and discussion.

7. REFLECTIONS

The three projects we have described generated security or privacy insights by using methods tailored specifically to the participants and settings involved. These methods were chosen to create an appropriate context within which the participants would feel comfortable to explore the issues the researchers had in mind; particularly important given the potential vulnerability of some of the participants. Broadly speaking, the goal in each project was to reduce the distance between the designer and the user, to allow the designer to become exposed to the lived experiences that have shaped the person throughout their life, and that in turn have shaped their relationship with security and privacy facing technologies. The methods we have described require an inter-disciplinary approach to research. They also require being open to appreciating that the life experiences of specific individuals can mean people see and make sense of the world quite differently to a designer of security or privacy technologies. Grounding a design discussion on a particular group of individuals and understanding their goals in life, enables a concrete yet rich and vivid discussion of how technology might fit into their lives and the trade-offs that might be acceptable for that particular group. This contrasts to a discussion around the needs of an abstracted user, where, in the worst case, the lack of concreteness created in discussion around user needs and goals can increase the temptation for designers to make design decisions favorable only to themselves.

The VOME project sought to encourage the participation in research of those who might otherwise be hard to reach in a typical participant recruitment process. Collage building enabled data collection in a public place with high public traffic. In addition, the project created a space to enable participants to feel confident to talk about topics they were comfortable with, and enabled them to drive the direction of the conversation. Dialogue was supported here through the multiplicity of voices that started to be built up along the collage—we saw how people would comment and respond to content contributed from others. The project focused upon financial practices also actively engaged participants that would not typically be involved in the design of new technologies. Due to the particular experiences that that age group had with technology, new methods were required to support the participants to envision future systems and develop awareness

of the needs they currently had with respect to making payments. In these workshops, dialogue was supported through the commentary and critique of the ideas developed in response to the earlier ethnographic work on the project. Frequently, participants would comment on the practices of others that were in sharp contrast to their own—be these fellow participants, the quotes on the cards from earlier participants, and indeed the younger researchers who facilitated the workshops. In these workshops, actively listening to people's stories related to finances was appreciated and encouraged, as was being open to the idea that personal finances is a highly personalized matter. The project related to privacy and abusive relationships also aimed to reach a group not typically accounted for in the design of digital technologies and gain insights into privacy after such a disruptive life event. The highly sensitive nature of this work demanded a longitudinal engagement in order to create an environment where issues to do with privacy could be probed and observed. This project highlighted the importance of responsiveness—in this case, responding to the sensitive subject manner through a method of engagement and subtle probing techniques that meant issues of privacy emerged but were not the focal point of the research activity.

Each case study engaged with groups that have amplified needs in some sense. It is an accepted tenet of security research to study the most challenging threat model for a particular system. As such it is likely that studying a challenging group of users can lead to similarly useful insights that would benefit future system design for the wider population. Despite this, an increasing amount of research in the usable privacy and security community takes place on crowdsourcing platforms such as MTurk which supports the spontaneous conducting of large remote studies with statistical consensus as their core concern. While this has eradicated issues of sample size in experiment design, what is also achieved is more distance between those who design security and privacy technologies and those that use them. This is to say that researchers must be careful in choosing and developing appropriate methods that balance the need to obtain statistical consensus (mindful of the limitations of null hypothesis significance testing [4]) and adequately capture the voices of those who might encounter the technologies that we design.

Each case study aimed to address a very local agenda with respect to security and privacy. Typically in computer science, our empirical work is subject to concerns of generalizability. These case studies do not provide generalizable results; however, there are big questions about useful the generated insights might have been without this intense, and sometimes very messy, engagement with people [15]. In each case, the process of the research including the building of intermediate prototypes and designing our engagement with people supports the generation of knowledge around that specific context and the people in it. In this way, the research process is not just a means to end, but is a crucial process that generates knowledge. Hayes [15] continues to describe how scientific rigor is achieved by this approach through discussion around the *trustworthiness* of results rather than *generalizability*; where trustworthiness is composed of credibility, transferability, dependability, and confirmability [35]. The goal has to be to build a interpretative yet cumulative discipline around our understanding of users, and to employ a mix of methods to generate evidence to argue that our security and privacy technologies will be useful in the long-term in the real world.

8. CHALLENGES AND OPPORTUNITIES

"I am suggesting that some of the past and current importance attached to user interface design for information appliances may be due to the low user value of the appliances themselves. If this is so, then designers would be better employed in creating useful appliances than in trying to make valueless ones easy to use." [6]

The quote above by Derrett [6] was made after arguing that a bassoon, while totally unusable in the traditional sense, can still be: highly valued; used regularly (by choice); be aligned with the aspirations of the user; and support a particular social identity. Derrett's argument hints that usability should not be considered as an end in and of itself, but should form part of a broader perspective of what makes technology successful in people's lives. This argument creates a quandary for security and privacy researchers due to one common mantra that their technologies are a secondary concern for users, and that researchers have the burden to design technologies that people do not want to use (e.g. [41]). However, following Derrett's point for a moment requires us to immediately confront interesting questions such as: can user-facing security and privacy technologies be considered 'useful' and 'high value' to people? To begin to answer this question is no small task, however does require us to broaden our perspectives on studying users, and take seriously the need to understand people's lived experiences with security and privacy technologies.

Having provided some examples of experience-centered research approaches that aimed to capture and study people's experiences of security and privacy, we can now consider some potential future research directions. New collaborations must likely be forged to explore these proposals (user experience can be composed of as many as 6 disciplines [24]). The challenge that this paper sets out is to understand how these proposed directions (and others with similar goals) might best help to build more successful secure or privacy-respectful systems that must be used by people.

8.1. Design in security and privacy research

One of the tenets that accompanied the initial wave of user-centered security research was the rejection of 'one size fits all' approaches to system design. The impact of this thinking has prompted the design and evaluation of a myriad of different system designs to approach pressing security problems, but much less work on the trade-offs required to align or fine-tune technologies with specific deployment contexts or specific groups of people. Such trade-offs are made in a process of design. While design work can be conducted without user involvement e.g. *generative design* (arguably typical in security and privacy research), where technology is designed according to pre-existing rules or heuristics, each of our case studies highlight how eventual end-users can be more proactively engaged in the process at an early stage of research. Indeed, Mathiasen and Bødker [21] have proposed that participatory design is one design approach that would be beneficial in a security context. This means that users actively contribute to the design of a system so that the resulting system accounts for their practices and expertise. While taking an experience-centered approach does not necessarily mean undertaking participatory design, there is a shared appreciation that an individual's experience and values must be accounted for at the early stages of a project. Additional challenges brought about by the context of privacy and security include that it may be challenging to identify the concrete design implications that allow us to work towards a meaningful and useful technology. Of course, incorporating user-centered design activities (including

usability evaluation) into the design cycle has long been a concern in the design of secure and usable systems [12]—but it is likely that this debate needs to be renewed by the proposal of additional complexity of early user involvement in a design process. Norman [24] advocates a "*design-it-in*" rather than a "*test-it-in*" approach to developing new technology, due to the fact that user testing typically occurs late in a project, and discovering the need for significant system modifications may not be welcome to project stakeholders at that late stage.

8.2. A local agenda for security and privacy

When designing security and privacy technologies, there is a tendency to think about designing for large numbers of users, and the generalizability of solutions is often an important criteria of its perceived utility. Focusing upon a large group of users can make it easy to become detached from the implications of user-hostile design decisions. One interesting and provocative research direction could involve designing systems that are bespoke for much smaller groups of people. The benefit of this approach would be that a deep understanding of a small group would need to be obtained, and the burden would be upon the researcher to enter into dialogue with a group of people to generate ideas for a new technology, and fit the technology into the lives of that group (that can be realistically assembled in the same room). This might provide a useful design exercise that provides a different perspective to how we design security and privacy more generally, and reduce the pressure upon researchers to focus upon developing technologies scalable to hundreds of thousands (or millions) of people. This can raise interesting questions, such as what would bespoke user authentication look like across the devices of a specific user? How would privacy interfaces look if they were designed to support a specific cultural norm? How different is the collaboratively designed technology from the conventional solution to a particular problem? And, did we discover design features from this exercise that would benefit much larger groups?

8.3. An indirect focus upon privacy & security

One of our case studies was not originally intended to explore security or privacy issues explicitly. However, in each example, issues such as trust, security and privacy often emerged, and became foregrounded in the interactions with participants. As computing has long since diffused out of the workplace and into most aspects of our lives, it is likely that insights can be gained by the study of contexts that do not, on the surface, have strong security or privacy connotations. Such an approach can expose researchers to the myriad of new ways that security and privacy is handled by people as an everyday practical problem [8], where participants will not feel defensive about their security and privacy practices or the workarounds they develop. One striking example of this is provided by Pritchard et al. [27] who conducted interviews with London bus drivers focused upon how new deployments of location-based services on buses had affected their ability to drive buses to a time schedule. Amongst other things, the interviews actually uncovered a pervasive awareness of the technology being used to conduct surveillance on the drivers, and the workarounds drivers employed to subvert the surveillance structures that the technology facilitated. Research in these contexts can provide an opportunity to take fresh perspectives upon how security and privacy technologies are appropriated and provide opportunities for design where there may not be an overbearing legacy of best practice to address the problems uncovered.

8.4. Security and privacy across the life-course

There is soon to be born a generation of people (if they haven't been born already) who will experience a complete lifespan in the digital age. For these individuals, attitudes to privacy and security will likely be informed by their early experiences with digital technologies. This creates the need to understand the earliest experiences that individuals have encountering and managing personal privacy and security, but also how these attitudes and practices are shaped across the life course either naturally or through significant life events. Important transitions in life such as entering teenage years, marriage, and even encountering or contemplating the death of a loved one [19], can lead to long-held values being questioned and reconfigured by the new circumstances. Work in this area appears to be on the increase. Work has described how children are increasingly encountering digital technologies at a young age which challenges our traditional notions of privacy or security [32]. Research has also started to explore the role that children can play in the participatory design of the security features of children's technologies [29]. Some work has explored how older adults build trust in seemingly antiquated paper payment technologies [38] and first explorations of how security and privacy technologies affect the bereaved have taken place [19]. These insights can potentially facilitate discourse around how experiences and perceptions of privacy and security change through life events and the ways in which systems experienced earlier in life influence preferences later in life.

8.5. 'In the wild' & 'extreme' contexts

Conducting field studies of security and privacy technologies has recently emerged as an important avenue of research. The emergence of mobile devices has made field studies a much more necessary evaluation approach e.g. [45]. However, it is likely that we can make further use of field studies to capture experiential insights into attitudes and behaviors. Research and practice focus has traditionally placed the organization as the defining context in security and privacy research (although this is changing). Organizational contexts can be characterized by people being of working age (i.e. roughly 18-65 years old), being of moderate intelligence and IT proficient, and with employee behavior being malleable to some extent by employers. While insights in this context are important, other contexts can be considered much more volatile, yet their study can serve to help us question our own values of what we as researchers consider to be important in security and privacy design. For example, ethnographic work has provided insights into how remote islanders delegate payments to one individual who boards a plane to the Australian mainland to carry out the banking for a entire village [34], or the trust practices of older adults who were dependent upon strangers to manage and obtain cash to live their everyday lives [10]. In such contexts it might be impossible to make appropriate trade-offs to design reasonably secure and useful systems. However, studying such contexts can make researchers increasingly sensitive to the assumption-breaking contexts in which their technologies might be deployed. A typical concern might relate to the generalizability of such contexts, however, such scenarios tend to make more pronounced the needs that many of us have anyway.

8.6. Probing security and privacy experiences

Finally, we need to consider new ways in which we may engage people in articulating concerns and experiences surrounding privacy and security. We noted earlier that people can have fine-tuned practices around privacy and security but may be reluctant

or have difficulty to explicitly explain those practices and their associated motivations. Storytelling is an important feature of experience-centered design, and there are already examples of using stories to elicit insights from users in relation to security and privacy (e.g. [28]). But we may also think about the ways technologies may be explicitly designed and deployed to provoke reaction and reflection upon personal practices. One such approach might be to develop technology probes [17], which are *"technologies deployed to find out about the unknown"*. These are not technology 'solutions' in the traditional sense, but are designed to reveal information about the context and relationships between the people with whom it is deployed. The deployment serves to collect data about the people using it and the context, to test technology prototypes, and to stimulate new ideas for future iterations, and ultimately to support theorizing around the requirements for a new technology in that context. This is a technique that could be deployed at an early stage of a design process to gather some early data from the field study to inform later prototypes. While these probes can be relatively benign in nature, these probes could be provocatively designed to deliberately conflict with some aspect of the user's values. Vines et al. [36] designed the Digital Chequebook, which was intended to confront the resistance of their group of older users to modern payment technologies; Vlachokyriakos et al. [39] created a digital voting probe. The purpose of such development and deployment is to create use contexts around technology in which users are prompted to share, defend, or reconsider their values.

9. CONCLUSION

As the contexts where technology is experienced change, so does the way people value and interact with security and privacy technologies. In this paper we have argued that an experience-centered [20,21] design approach to the study and design of security and privacy technologies is valuable here. By describing three case studies we highlighted how innovative non-typical research methods can yield insights into experiences of security and privacy and facilitate user creativity in envisioning future technologies for their own benefit. Finally, we suggest a number of areas to focus future research activity to bring an experiential perspective on old, long-standing problems, and ultimately serve as a tool for researchers to capture and design for the complexities of the experiential aspects of privacy and security technologies.

10. WORKSHOP DISCUSSION

During the workshop, many interesting questions were raised around the paper, a few of which we find helpful to capture in this section of the paper.

10.1 Is this new paradigm simply suggesting that we should just ask people different kinds of questions in our studies?

The new paradigm is the prioritization of people's subjective experiences of security and privacy technologies as the focus of study. This places people and their lived experience as core item of curiosity rather than just their performance using a new technology. Different research methods have different affordances. Traditional interviews and surveys tap into a very rational mode of human thinking, which can elicit self-descriptions of practices that depict an ideal that is seldom met [25]. Experience-centered design takes that to explore and understand lived experiences (which are innately subjective) we need a different class of methods based upon *dialogue* that must recognize: people's behavior is interesting and won't be judged; the need to develop ways to help people articulate tacit behaviors to researchers; researchers must work together with people to make sense of the insights that emerge. Much of our skilled behavior is not conscious, and an experience-centered design process is about applying methods that make that subjective, tacit knowledge visible. *Experience-centered privacy and security* is about understanding how the methods of experience-centered design can help us do better user-facing security and privacy.

10.2 Designing security and privacy is different from any other technology design due to the presence of an adversary. How is this accounted for in this paradigm?

It is true that security and privacy designers must contend with two classes of users; i) the target users; ii) the adversaries. Historically, security research was born out of a focus upon the adversary, and the area of usable privacy and security came about to help redress this imbalance. Overall it is necessary to strike a balance between the consideration of both groups. In this paper, we have focused very much on the target users, but that is not to say that future experience-centered privacy and security cannot contribute to discussion around the role of the adversary.

Experience-centered methods acknowledge that people have their differences, and seeks to understand how groups of people might see the world differently. While we clearly would not wish to design technologies to support adversaries, it is always valuable to understand users better. The book of Kevin Mitnick [23] stands as one classic resource that presents insights into the motivations and activities of a motivated and clever adversary. Today however, the distinction between the two user groups can be more nuanced; in our first case study we described how social network users – non-experts in computer security -- could be both the hunter and the hunted when conducting themselves online, and would promiscuously seek information about others, without any reflection on this as a negative or anti-social behavior. A greater curiosity around this phenomenon (for example) could provide new opportunities to study how and why people switch between these two roles in their everyday lives.

Promising work already exists that seeks to uncover people's understanding of the difference between the two user groups. Wash [40] explored how one group of users (the target group) conceptualized the other group (the adversaries) in discussions around botnets and viruses.

10.3 Given a project with finite time and money, how can we incorporate such research methods into the development lifecycle?

All three of the methods we describe in this paper were applied longitudinally. However, all research methods represent a compromise in terms of time and money. Some methods require more time to apply or are more high risk than others, regardless of the methodology. The goal in any research is to apply an appropriate mix of methods that take account of resource constraints, yet still make a meaningful contribution towards answering the research questions. There are a variety of experience-centered methods that can be called upon that require a much shorter time commitment [43].

11. ACKNOWLEDGEMENTS

This work was funded by Research Councils UK Digital Economy theme Social Inclusion through the Digital Economy Research

Hub (EP/G066019/1) and New Approaches to Banking for the Older Old (EP/H042997/1) project, and the EPSRC, ESRC and TSB funded Visualisation and Other Methods of Expression (EP/G00255X/1) project. Writing the "workshop discussion" section was greatly aided through the excellent note-taking ability of Bob Blakley.

REFERENCES

1. Biddle, R., Chiasson, S., and van Oorschot, P. Graphical Passwords: Learning from the first twelve years. *ACM Computing Surveys 44*, (2011).
2. Clarke, R., Wright, P., Balaam, M., and McCarthy, J. Digital portraits: photo-sharing after domestic violence. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM (2013), 2517–2526.
3. Cranor, L. and Garfinkel, S., eds. *Security and Usability: Designing Secure Systems That People Can Use*. O' Reilly, 2005.
4. Cumming, G. The New Statistics: Why and How. *Psychological Science*, (2013).
5. Davis, D. Compliance defects in public-key cryptography. *Proceedings of the 6th conference on USENIX Security Symposium, Focusing on Applications of Cryptography - Volume 6*, USENIX Association (1996), 17.
6. Derrett, N. Heckel's Law: Conclusions from the User Interface Design of a Music Appliance -the Bassoon. *Personal Ubiquitous Comput. 8*, 3-4 (2004), 208–212.
7. Dourish, P. and Anderson, K. Collective Information Practice: Emploring Privacy and Security As Social and Cultural Phenomena. *Hum.-Comput. Interact. 21*, 3 (2006), 319–342.
8. Dourish, P., Grinter, E., de la Flor, J., and Joseph, M. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal Ubiquitous Comput. 8*, 6 (2004), 391–401.
9. Dunphy, P., Heiner, A.P., and Asokan, N. A closer look at recognition-based graphical passwords on mobile devices. *Proceedings of the Sixth Symposium on Usable Privacy and Security*, ACM (2010), 3:1–3:12.
10. Dunphy, P., Monk, A., Vines, J., Blythe, M., and Olivier, P. Designing for Spontaneous and Secure Delegation in Digital Payments. *Interacting with Computers 10.1093/iw*, (2013).
11. Dunphy, P. and Yan, J. Is FacePIN secure and usable? *Proceedings of the 3rd symposium on Usable privacy and security*, ACM (2007), 165–166.
12. Flechais, I., Mascolo, C., and Sasse, M.A. Integrating security and usability into the requirements and design process. *Int. J. Electron. Secur. Digit. Forensic 1*, 1 (2007), 12–26.
13. Forget, A., Chiasson, S., van Oorschot, P.C., and Biddle, R. Improving text passwords through persuasion. *Proceedings of the 4th symposium on Usable privacy and security*, ACM (2008), 1–12.
14. Gaver, B., Dunne, T., and Pacenti, E. Design: Cultural probes. *interactions 6*, 1 (1999), 21–29.
15. Hayes, G.R. The Relationship of Action Research to Human-computer Interaction. *ACM Trans. Comput.-Hum. Interact. 18*, 3 (2011), 15:1–15:20.
16. Herley, C. and Oorschot, P. Van. A Research Agenda Acknowledging the Persistence of Passwords. *IEEE Security and Privacy 99*, PrePrints (2011).
17. Hutchinson, H., Mackay, W., Westerlund, B., et al. Technology Probes: Inspiring Design for and with Families. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM (2003), 17–24.
18. Kaye, J. "Jofish." Self-reported password sharing strategies. *Proceedings of the 2011 annual conference on Human factors in computing systems*, ACM (2011), 2619–2622.
19. Locasto, M.E., Massimi, M., and DePasquale, P.J. Security and Privacy Considerations in Digital Death. *Proceedings of the 2011 Workshop on New Security Paradigms Workshop*, ACM (2011), 1–10.
20. Mathiasen, N.R. and Bødker, S. Threats or threads: from usable security to secure experience? *Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges*, ACM (2008), 283–289.
21. Mathiasen, N.R. and Bødker, S. Experiencing security in interaction design. *Proceedings of the 2011 annual conference on Human factors in computing systems*, ACM (2011), 2325–2334.
22. McCarthy, J. and Wright, P. *Technology as Experience*. The MIT Press, 2007.
23. Mitnick, K. *The Art of Deception*. John Wiley & Sons, 2003.
24. Norman, D. *The Invisible Computer*. MIT Press, 1999.
25. Norman, D. *Emotional Design: Why We Love (or Hate) Everyday Things*. Basic Books, 2005.
26. Orne, M.T. On the social psychology of the psychological experiment: With particular reference to demand characteristics and their implications. *American Psychologist 17*, 11 (1962), 776–783.
27. Pritchard, G., Vines, J., Briggs, P., Thomas, L., and Olivier, P. Digitally Driven: How Location Based Services Impact the Work Practices of London Bus Drivers. *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems*, ACM (2014), 3617–3626.
28. Rader, E., Wash, R., and Brooks, B. Stories as informal lessons about security. *Proceedings of the Eighth Symposium on Usable Privacy and Security*, ACM (2012), 6:1–6:17.
29. Read, J.C. and Beale, R. Under my pillow: designing security for children's special things. *Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology*, British Computer Society (2009), 288–292.
30. Rittel, H.W.J. and Webber, M.M. Dilemmas in a General Theory of Planning. *Policy Sciences 4*, (1973), 155–169.
31. Saltzer, J. and Schroeder, M. The Protection of Information in Computer Systems. *IEEE 63*, 9 (1975), 1278–1308.
32. Schechter, S. The User IS the Enemy, and (S)he Keeps Reaching for that Bright Shiny Power Button! *Workshop on Home Usable Privacy and Security (HUPS)*, (2013).
33. Sheng, S., Magnien, B., Kumaraguru, P., et al. Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish. *Proceedings of the 3rd Symposium on Usable Privacy and Security*, ACM (2007), 88–99.
34. Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G., and Furlong, M. Password sharing: implications for security design based on social practice. *Proceedings of the SIGCHI*

conference on Human factors in computing systems, ACM (2007), 895–904.

35. Stringer, E.T. *Action Research*. Sage, 2014.
36. Vines, J., Blythe, M., Dunphy, P., et al. Cheque Mates: Participatory Design of Digital Payments with Eighty Somethings. *ACM Conference on Human Factors in Computing (CHI')*, (2012), 1169–1178.
37. Vines, J., Blythe, M., Lindsay, S., Dunphy, P., Monk, A., and Olivier, P. Questionable Concepts: Critique as a Resource for Designing with Eighty Somethings. *ACM Conference on Human Factors in Computing (CHI')*, (2012), 1169–1178.
38. Vines, J., Dunphy, P., Blythe, M., Lindsay, S., Monk, A., and Olivier, P. The joy of cheques: trust, paper and eighty somethings. *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work*, ACM (2012), 147–156.
39. Vlachokyriakos, V., Dunphy, P., Taylor, N., Comber, R., and Olivier, P. BallotShare: An exploration of the design space for digital voting in the workplace. *Computers in Human Behavior*, (2014).
40. Wash, R. Folk models of home computer security. *Proceedings of the Sixth Symposium on Usable Privacy and Security*, ACM (2010), 11:1–11:16.
41. Whitten, A. and Tygar, J.D. Why Johnny can't encrypt: a usability evaluation of PGP 5.0. *Proceedings of the 8th conference on USENIX Security Symposium - Volume 8*, USENIX Association (1999), 14.
42. Wright, P. and McCarthy, J. Empathy and experience in HCI. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM (2008), 637–646.
43. Wright, P. and McCarthy, J. *Experience-Centered Design: Designers, Users, and Communities in Dialogue*. Morgan and Claypool Publishers, 2010.
44. Yan, J.J. A note on proactive password checking. *Proceedings of the 2001 workshop on New security paradigms*, ACM (2001), 127–135.
45. Von Zezschwitz, E., Dunphy, P., and De Luca, A. Patterns in the Wild: A Field Study of the Usability of Pattern and Pin-based Authentication on Mobile Devices. *Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services*, ACM (2013), 261–270.
46. Zurko, M.E. and Simon, R.T. User-centered security. *Proceedings of the 1996 workshop on New security paradigms NSPW 96*, ACM Press (1996), 27–33.