The Third Wave? Inclusive Privacy and Security

Yang Wang
Syracuse University
SALT Lab, School of Information Studies
Syracuse, New York
ywang@syr.edu

ABSTRACT

The field of security and privacy has made steady progresses in developing technical mechanisms, which I refer to as the first wave of security and privacy research. Since the 70's, human factors and usability have been recognized as a key property of effective security and privacy mechanisms. This is what I call the second wave of security and privacy research, focusing on usability. In this article, I propose and advocate for a third wave of research that I call *inclusive* security and privacy, which is concerned with designing security and privacy mechanisms that are inclusive to people with various characteristics, abilities, needs and values. I present a preliminary research framework and research agenda for advancing inclusive security and privacy.

CCS CONCEPTS

• **Security and privacy** → **Social aspects of security and privacy**; • **Human-centered computing** → *User centered design*; *Accessibility design and evaluation methods*;

KEYWORDS

Security; Privacy; Accessibility; Universal Design

ACM Reference format:
Yang Wang. 2017. The Third Wave? Inclusive Privacy and Security. In *Proceedings of 2017 New Security Paradigms Workshop, Santa Cruz, CA, USA, October 1–4, 2017 (NSPW 2017),* 9 pages.
https://doi.org/10.1145/3171533.3171538

1 INTRODUCTION

Over the past four or so decades, the security and privacy research community has made great strides in identifying security and privacy risks in information and communication technologies and designing various basic and applied countermeasures such as cryptography, encryption, access control, formal methods, secure computation, and privacy-preserving/enhancing techniques. I call this the first wave of security and privacy research, or *technical* security and privacy, which focuses on the technical mechanisms and continues to grow strongly as we move towards the Internet of Things and Quantum Computing.

Since Saltzer and Schroeder's seminal work in 1975 advocating for computer security mechanisms to be "psychologically acceptable" [47], the human factors and more specifically the usability of security and privacy mechanisms have become a key research topic for security and privacy research (e.g., [5, 28, 34, 96]). For instance, Whitten and Tyler conducted a well-known user study of PGP and found that it was difficult for ordinary people to use PGP and thus its value was limited, pointing to the importance of usability in security mechanisms. More broadly, usability has been considered as a first class design requirement for security and privacy designs. I call this the second wave of security and privacy research, or *usable* security and privacy, focusing on the usability of technical designs.

In this article, I propose a third wave of security and privacy research, taking human abilities and characteristics as first class design requirements and centering on designing mechanisms that are inclusive to the widest possible range of users. I call this *inclusive* security and privacy (inclusive S&P), the idea of *designing security and privacy mechanisms that are inclusive to different human abilities, characteristics, needs, identities, and values.*

My thinking behind these three waves of security and privacy research was in part inspired by Harrison et al.'s conceptualization of the three paradigms of Human-Computer Interaction (HCI) research: man-machine fit with a human factor underpinning, human brains as information processors with roots in cognitive science, and situated perspectives with roots in design science and social sciences such as anthropology and ethnomethodology [41]. They note that every wave or paradigm of HCI research represents a different but not necessarily exclusive orientation of research which highlights what kinds of research questions should be pursued, the methodologies for answering these research questions, and how the research outcomes should be evaluated.

Some exciting research has been done in the flavor of inclusive S&P, such as PassChords, an accessible smart phone authentication mechanism for blind users [9], or DigiSwitch, a device for older adults to monitor and control the collection and transmission of their health information [20]. These examples illustrate the prospect of making security and privacy designs more inclusive to marginalized populations. However, I would argue that is not enough because these research efforts, while being very valuable, are still in the peripheral of the field. The wide range of underserved populations deserve more attention and research in a more systematic way. Inclusive S&P needs a stronger presence to make it more mainstream, just like how usability has been elevated and widely recognized in the field of security and privacy. As such,

NSPW 2017, October 1–4, 2017, Santa Cruz, CA, USA

ACM ISBN 978-1-4503-6384-6/17/10…$15.00
https://doi.org/10.1145/3171533.3171538

inclusiveness should be expected in all security and privacy designs rather than being a property that only a few system designers espouse. One of the goals of this article is to advocate that inclusive S&P is more than a nuanced vision of usable S&P. Rather, inclusive S&P calls for some new conceptualizations and/or methodologies of security and privacy designs that can serve a broader range of users.

This article will highlight the limitations of the current framings/foci of security and privacy research and advocate for a new perspective of security and privacy research. In the remainder of this article, I will first describe a preliminary research framework to systematically pursue inclusive S&P research. I will then outline some promising areas of research for inclusive S&P.

2 A RESEARCH FRAMEWORK OF INCLUSIVE SECURITY AND PRIVACY

This section describes a preliminary framework of *inclusive security and privacy*, based on the relevant literature and my previous and ongoing work on this topic. The long-term research agenda of *inclusive security and privacy* is to design security and privacy mechanisms for *everyone*. This ambitious vision goes beyond making security and privacy designs usable. In addition to usability, inclusive security and privacy designs must be inclusive of different human abilities, characteristics, values and needs.

There are three key insights that guide this new research perspective. First, most security and privacy mechanisms were designed with the general population in mind, leaving many specific user groups under-studied and under-served such as people with disabilities. Second, studying these under-served populations' security and privacy practices will not only deepen our understanding of their needs and challenges but also create an opportunity to examine and re-think more broadly about current security and privacy conceptualizations, methodologies, and designs. Third, designing for these under-served populations will not only create security and privacy mechanisms that better support them but also potentially benefit everyone, an embodiment of universal design [62, 89, 90].

Universal design refers to "the design of products and environments to be usable by all people, to the greatest extent possible, without the need for adaptation or specialized design" [13]. This idea was originally developed in the field of architecture [62] and a set of principles have been proposed for universal design [13]. For instance, the principle of equitable use means that designs should be useful to people with different abilities [13]. One concrete guideline to achieve this principle is that the designs should provide the same means of use to all users regardless of their abilities [13]. For example, a building ramp can be used by different people and it will benefit those with and without wheelchairs (e.g. when people have strollers or luggage). More recently, universal design has also been adopted to digital tools. A telling example is voting systems (e.g., those developed and used in Los Angeles). By explicitly considering and designing accessibility into voting systems, they are more usable for people with or without disabilities [29, 35, 36, 46, 54]. Similarly, the main value of this research perspective is to guide inclusive security and privacy designs, supporting diverse user groups that previous designs fall short of.

For the remainder of this article, I will mainly focus on privacy. Given security and privacy are closely related, the research framework can also inform inclusive security designs.

2.1 Privacy for Under-Studied/Under-Served Populations

In terms of privacy studies and designs, there are many under-studied and under-served user populations. Table 1 lists a few example populations and privacy studies thereof. These studies uncover alternative conceptualizations of privacy, specific and/or unique privacy requirements, and other (sometimes competing) values (e.g. safety) that must be fulfilled alongside privacy for these populations. I use the term under-served populations to cover a wide range of populations. This is much broader than vulnerable populations. For instance, veterans are an example of under-served populations but it can be offending to call them as a vulnerable population. I also would not assume people from a non-Western developing country as a vulnerable population. Nevertheless, they may be under-served in terms of supporting their security/privacy needs.

Visually impaired. People with disabilities face many challenges in protecting their security and privacy. Failure to support people with disabilities can not only make them more vulnerable to security/privacy risks but may also violate regulations. The Americans with Disabilities Act (ADA) of 1990 requires telecommunication companies in the U.S. to make their services accessible to people with disabilities. For instance, a website that does not provide ways in which people with disabilities can log into the site in an accessible manner may be deemed as violating ADA.

One example disability condition is visual impairments. Visual impairments range from partial to complete loss of vision. There are about 22.5 million (6.9%) adult Americans with vision loss and 8 million (2.5%) Americans with visual impairments [30, 67]. There is an estimated population of 285 million people worldwide with visual impairments (about 4% of global population), including 39 million living with blindness and 246 million having low vision [99].

Holman et al. conducted focus groups with blind users and identified their top 10 security challenges: (1) CAPTCHA, (2) auto logout, (3) auto refresh/reload webpage, (4) inaccessible PDF, (5) inaccessible anti-virus software, (6) auto install software, (7) auto software updates make software inaccessible, (8) SecureID (a random number display in the device used for logging in), (9) key loggers, and (10) spam [44]. Some of these are more general accessibility issues such as inaccessible PDF, and others such as key loggers are addressed by existing anti-virus software.

Visually impaired users also have privacy concerns about using mobile devices when they are in the speakerphone or screen-reading mode and generally in public because others can see or hear what they are speaking or doing [48, 66, 102]. Visually impaired users can wear earphones, but that is sometimes inconvenient [66] and could limit their abilities to hear or sense the nearby environment, making them vulnerable to attacks [6]. The iOS Screen Curtain allows iPhone users to blank their screen, but that does not address the privacy issues caused by the screen-reading mode, and visually impaired users may forget to activate the Screen Curtain feature. The use of assistive technology (e.g., a portable magnifier)

	Population
Disability	disability in general [11], visual [6, 7, 9, 102], cognitive [26, 60, 81], motor [48, 66]
Non-western/developing countries	Middle East [2–4, 31], Africa [74], India [49, 51, 64, 95], China [95]
Other under-served populations	older adults [20, 59], LGBT [14], children [2, 17, 27, 63, 88, 91, 93, 103], veterans [78], migrants [2, 75], refugees [75]

Table 1: Privacy of under-served populations

could attract unwanted attention and make users more noticeable to attackers [48, 79]. Visually impaired users often have to compromise their privacy for achieving independence and/or convenience.

Ahmed et al. have conducted two studies specifically investigating visually impaired adults' privacy needs and practices in online and offline settings [6, 7]. They found that visually impaired users face difficulties in detecting visual or aural eavesdropping, have physical security and privacy concerns (e.g., using ATM), and sometimes need to ask others (even strangers) to help (e.g. read documents, type pin in shopping) [7]. There are proposed solutions for specific tasks (e.g., accessible ATM [22]), but no generic solution to address the privacy risks that emerge from asking others to help. Visually impaired users also report difficulties in managing their social media sharing, citing the difficulties in using the privacy settings on social media sites (e.g., Facebook) [6]. These privacy settings have been found to be difficult for social media users in general [94].

Older adults. Another example under-served population is older adults. Older adults sometimes have difficulties in using computer technologies due to their declining motor and/or cognitive abilities [15, 53, 82]. As more older adults adopt computer technologies [45, 61], they also have many privacy concerns such as information leakage and sharing/use without their awareness and control [25, 58, 100]. Scholars suggest that older adults are more vulnerable to privacy risks because they have limited knowledge of privacy risks and protection tools [16, 39, 65, 71].

Youth. For youth (especially teens), there is a widely adopted perception that they do not care about privacy because the kinds of sensitive things they often post on social media (e.g., revealing pictures of themselves). However, many scholars have shown that teens do value privacy, for instance, girls are concerned about their parents knowing too much about their social lives [63]. They often disclose the intimate aspect of themselves to their peers because they have developmental needs - "need for social interaction, sharing of information, and personal expression" [93].

Culture. Besides factors related to abilities and demographics, cultural background is another factor. A meta-study found that over 80% of published psychological studies focused on people from Western, Industrialized, Educated, Rich, and Democratic (WEIRD) countries and thus it is highly questionable whether the results can be generalized to people in other non-WEIRD countries [42]. In terms of privacy, similar arguments may be made. For instance, recent studies found that the privacy conceptualization of people in the Middle East is heavily influenced by their Arabic culture - they perceive privacy around family reputation and thus the way to enact privacy is a collective act via participatory surveillance (e.g., family members monitor what each other posts on social media) [3, 4].

It is worth noting that under-served populations may experience improvements of life during a study (e.g., trying out a research prototype) but they are likely to revert back to their previous life after the study, which can be frustrating to say the least. Therefore, it is important for researchers to be mindful about this ethical challenge and how to address this challenge. For instance, the researchers may consider providing their participants the option of keeping the prototype after the study.

People from different under-served groups may have profoundly different needs and challenges for security and privacy. In fact, even people with the same disability condition can vary significantly in terms of their abilities, needs and technology uses. In addition, it would be valuable to study the intersections of these various groups rather than merely studying them individually. A person can have many characteristics. For instance, a large percentage of people with visual impairments are older adults. Thus, it would be beneficial to consider the relationships between these characteristics and how they might affect people's privacy needs and practices.

One reoccurring theme across many of these populations is people's pursuit of different (sometimes competing) values. Inclusive privacy designs need to consider the broader everyday context in which privacy is just one such value that people desire and people might have to trade privacy for other values (e.g., trust) depending on the situation.

2.2 Design for Inclusive Privacy

The design for inclusive privacy builds on several lines of research, including privacy design and accessible design.

Design for Privacy. There are many conceptualizations of privacy [8, 37, 69, 72, 83–85]. One recent conceptualization that has gained particular attention in the privacy literature is Helen Nissenbaum's theory of Contextual Integrity [68–70] which calls for context-based privacy management. She identifies two types of contextual norms for privacy: "norms of appropriateness, i.e., what information would be appropriate to be revealed in a context; and norms of flow or distribution, i.e., the flow of personal information in certain context needs to be reasonably justified. If either of these norms has been violated, then users' privacy is considered to be infringed." [69]

A number of approaches, principles, and frameworks have been proposed for designing privacy, but they have not explicitly considered people's varying abilities or characteristics. Privacy by Design

(PbD) is a privacy design approach developed by the Information and Privacy Commissioner of Ontario, Ann Cavoukian [23, 24]. She offers seven high-level principles of PbD [23]. For instance, privacy should be considered from the beginning rather than being an add-on after a system or service is developed [23]. While valuable, these principles can be too abstract for implementing privacy-preserving systems [86]. Another set of high-profile privacy principles are the Fair Information Practices (FIPs), proposed in a report of the US Department of Health, Education and Welfare in 1973 [92]. The report lists five key principles for FIPs: notice, choice, use limitation, access and security. For instance, use limitation means that user data collected for one purpose should not be used for another purpose without the user's consent. In addition, there are more design-oriented privacy frameworks [12, 40, 52, 57, 87]. For instance, Langheinrich advocates for enabling anonymity in privacy protections [52].

Value-sensitive design (VSD) is a generic design approach that highlights and supports values in system design [32, 33]. Example values include user autonomy, freedom from bias, privacy and trust [32]. VSD has been applied to assess technologies or privacy designs. For instance, Xu et al. used VSD to conduct conceptual, technical and empirical investigations of a privacy-enhancing tool, examining how relevant theories inform the tool design, how the tool design can be technically implemented, and how end users would react to the tool [101]. In another example of using the VSD approach, Briggs and Thomas conducted workshops to understand people's perceptions of future identity technologies with six marginalized community groups: young people, older adults, refugees, black minority ethnic women, people with disabilities, and mental health service users [18]. They identified both common values and different impacting factors across these community groups regarding how people think about future identity technologies [18]. As shown in this example, VSD can be useful in identifying the underlying values that under-served user groups have and assessing whether these values have been supported in security and privacy designs.

Any design has embedded values either explicitly or implicitly. I advocate that *inclusiveness* is desirable, which is itself a value. Security/privacy designers need to make their value judgement and justify their design decisions, especially when there are conflicting values (e.g., national security and personal privacy).

Design for Accessibility. Insights from the field of accessible computing can also be useful in making security and privacy designs inclusive to a wide range of user populations. Accessible computing focuses on building technologies to improve the independence, access, and quality of life for people with disabilities. To achieve this goal, a number of design approaches have been proposed such as assistive technology [38], universal design [62, 89, 90], universal usability [55], inclusive design [50], ethically-aware design [1, 21], and ability-based design [98]. These approaches are helpful in conceptualizing inclusive privacy. For instance, universal design (UD) upholds that designers should consider a wide range of user characteristics so that the resulting designs benefit everyone including those both with and without disabilities [62, 89, 90]. Shneiderman noted that "Accommodating a broader spectrum of usage situations forces researchers to consider a wider range of designs and often leads to innovations that benefit all users" [80]. There are a number of UD design principles. For instance, perceptible information means the "design communicates necessary information effectively to the user, regardless of ambient conditions or the user's sensory abilities." [90] Inclusive design attempts to counter design exclusions - exclusion of users because of "subconscious biases and assumptions about users' abilities" [50].

Wobbrock et al. propose ability-based design, which shifts the view from focusing on people's disabilities to their abilities [98]. They propose seven ability-based design principles based on their extensive experiences in designing technologies for people with disabilities. These principles include ability, accountability, adaptation, transparency, context, and commodity [98]. For instance, the principle of ability states that "Designers will focus on ability not *dis*-ability, striving to leverage all that users *can* do" [98]. The principle of accountability means that designers should change the systems rather than the users if the systems do not perform well [98]. These principles have proven valuable for designing accessible technologies for people with disabilities and should be adopted for inclusive S&P designs that support a wide range of under-served user groups.

It is important to note that making security/privacy mechanisms accessible to a wide range of user populations requires careful HCI and security/privacy considerations. In other words, a HCI perspective alone is unlikely to address diverse populations' security/privacy needs. For instance, new interaction devices or modes can present new security/privacy attack surfaces and new threat vectors (e.g., augmented reality [56]). More generally, security and privacy are non-functional design requirements, which if not consider from the onset of the design process, would be much more difficult to address later.

Design for Inclusive Privacy. The idea of universally usable security and privacy aims to make security and privacy designs usable to a wide range of user populations but it seems to mainly focus on accessibility issues [43, 80]. As I discussed before, other factors such as cultural background should also be considered. As such, inclusive privacy is broader than universally usable privacy because it not only considers people's abilities/disabilities, but also their cultural background, identities and knowledge.

The design principles of privacy and accessibility are valuable for inclusive privacy. For instance, drawing from the ability-based design, inclusive privacy designs should focus on users' abilities, model their performance, and adapt the system to match users' abilities.

3 RESEARCH AGENDA

In this section, I will outline a preliminary research agenda of inclusive security and privacy. I will focus on privacy for people with visual impairements as a concrete example domain for this research agenda. Similar research topics could be conducted for the security and privacy needs of other under-served populations.

3.1 Inclusive privacy analysis

There is a large body of literature on people's privacy concerns, preferences and practices. However, there are relatively few studies that investigate privacy challenges or strategies of people with disabilities (visual [6, 7, 9, 66, 102], cognitive [26, 60, 81], and physical [48, 66]). These studies were either not designed for focusing on privacy issues, or used one-time interviews or surveys that might not capture visually impaired people's everyday experiences.

A valuable addition is to study their privacy and security experiences in their daily lives more naturally and longitudinally, for instance, using participant observation ("shadowing") and diary studies. Longitudinal diary study is a good method to understand people's mundane everyday experiences that they might forget to provide in an interview or a survey (e.g., [97]). Participants could be asked to submit a daily diary about anything they did or experienced on that day for which they felt their privacy was at risk or violated. These events can include visiting certain websites, using a shared/public computer, installing or using software (e.g., mobile apps), or asking someone to help them with a task (e.g., read a message or type a pin). Participants can submit their daily diary via emails, text messages, voice mails [73], or on a web form.

While the diary study approach can provide many insights into visually impaired users' everyday privacy challenges and practices, it has an important limitation - it's based on self-reported data. The extant literature has shown that visually impaired users face challenges in recognizing emergent privacy threats (e.g., shoulder surfing). Therefore, they may miss reporting privacy-invading incidents that they did not recognize. To address this methodological limitation, one could also conduct a light-weight ethnographic study to directly observe how people with visual impairments enact their privacy in their daily life but also help identify potential privacy risks that the participants did not recognize. A researcher will "shadow" a participant for an extended period of time (e.g., a few days) in the participant's home and/or workplace upon permission. The researcher will take notes during the observation on different aspects of potential privacy-related incidents. If the researcher notices a privacy threat (e.g., a web page with a login form where its SSL certificate expires and thus uses HTTP rather than HTTPS) that the participant did not recognize, the researcher will explain the threat to the participant and ask whether the participant has noticed that issue and why.

Since "shadowing" can be privacy-invasive, the researcher can use two main strategies to address this potential issue. First, if a participant feels uncomfortable having the researcher observe certain activities, the researcher will excuse himself or herself upon the participant's request. Second, if the researcher finds that potential participants refuse to participate in the study because they feel uncomfortable being"shadowed" by a researcher (stranger), the researcher can try to recruit and train their trusted help givers (e.g., a close family member) to conduct the study. To get training, a "participant researcher" will shadow a researcher and follow the study protocol. Combining diary studies and "shadowing" could provide insights into visually impaired users' privacy and security practices in their everyday lives. These insights can in turn be useful to understand these people's abilities, characteristics, needs and challenges in protecting their privacy and security.

3.2 Inclusive privacy design and evaluation

The prior literature and the results of the inclusive privacy analysis can be fed into the design of inclusive privacy mechanisms. One example inclusive privacy design idea is creating a privacy threat reminder. The extant literature [6, 7, 9, 66, 102] and my own prior work [19] point to a heightened privacy challenge for people with disabilities - they have particular difficulties in recognizing emerging privacy threats in the environment. For instance, the fact that visually impaired users often wear headphones when using screen readers can affect their ability to identify visual and aural eavesdropping. The question is whether we can design a tool that can help people with visual impairments to identify these emerging privacy risks. Another example is to design multi-modal interfaces for privacy/security risk indicators since most of such indicators rely on visual cues (e.g., https lockpad icon), which are challenging for visually impaired users.

One promising design approach in this context is participatory design [76, 77] where the design team directly includes members of the target user population (e.g., visually impaired users) who will actively engage throughout the design process. These participatory design sessions should include people with or without visual impairments as well as help givers to represent a wide range of stakeholders. The first set of design sessions can start with everyone sharing their own privacy concerns and practices. Then the team will review together the major findings from the inclusive privacy analysis (e.g., diary studies and light-weight ethnographic studies), focusing on major privacy threats and their associated contexts (e.g., online/mobile tracking on different websites) as well as potential coping strategies (e.g., installing and using ad blockers such as Ghostery on a web browser or a smartphone). The subsequent design sessions can then focus on co-designing and quick testing of low-fidelity (e.g., paper prototypes), medium-fidelity (e.g., UI mock-ups in Illustrator), and high-fidelity prototypes (e.g., browser extensions or mobile apps). Once system prototypes are built, lab or field experiments can be conducted to evaluate the functionality, usability, and the broader user experience of these prototypes. However, it is important to note that the outcomes of participatory design often require designers or researchers to synthesize, select, adapt, implement, and evaluate in an iterative fashion.

3.3 Inclusive privacy design guidance development

The goal of this research direction is to develop design guidelines for creating privacy designs that are inclusive to different user abilities, identities and values. This research direction can include several components. First, it can evaluate the design guidelines (e.g., for privacy [12, 33, 40, 52, 57, 68, 87] and for accessibility and inclusion [55, 62, 98]), features, and implementations of the inclusive privacy prototypes. Second, it can include other under-served populations. Given that people from different under-served groups can differ drastically, tools designed for one under-served population may or may not be directly applicable to other under-served populations. In fact, different under-served populations may need to be studied separately and inclusive design principles may be derived inductively from studying and designing for several specific populations. For instance, researchers can interview people with cognitive impairments and older adults about their privacy needs, challenges and practices and have them test the inclusive privacy prototypes. The results of the interviews and user testing will inform whether these inclusive designs can be used without changes to support these other two under-served populations. If not, the results will suggest what changes are needed. Third, research can seek to provide further design guidance for supporting other under-served populations based on results from the interviews and user testing of inclusive privacy prototypes.

While it is desirable to derive inclusive security/privacy design patterns (i.e., what/how to do) and anti-patterns (i.e., what/how to avoid) that can be applied universally, practically this might be extremly difficult if not impossible due to the seeminly uncountable human characteristics. Partial rather than universal perspective is also valuable even though it can only be generalized to a limited number of under-served populations.

3.4 Making security and privacy more inclusive

An concrete example of inclusive S&P research is the line of work on making authentications more accessible to people with disabilities. For instance, Azenkot et al. first interviewed visually impaired users about their experiences with mobile devices and found that these users often chose not to use any device authentication because of inconvenience and that they desired ways to hide their device screens to prevent others from seeing their information or activities on the devices [9]. Drawing from these insights, the researchers then designed an authentication mechanism for this user group that allows the users to use their finger tapping on the screen as a password, which is easy for the users to remember but difficult for others to observe [9].

My own research has found that visually impaired computer users often face a number of challenges in using authentication mechanisms (e.g., textual passwords), such as having difficulties in locating the login elements, typing the correct passwords, verifying successful authentication, or logging into web services on a public or shared computer [19]. Inspired by these insights, we then designed a smart device-based password manager that allows visually impaired users to more easily manage their accounts and passwords and use public computers [10]. Both of these two aforementioned research projects started with foundational user studies to understand an under-served population and then used the insights from those studies to inform the subsequent design.

More broadly, there are several ways in which current security and privacy research could be extended to make them more inclusive. For instance, user studies of security and privacy should include more under-served populations. Similarly, privacy risk assessments (e.g., privacy impact assessment) should explicitly consider under-served populations (e.g., an assessment of a social media platform should consider youth and older adults as its users). In the design and evaluation of S&P technologies, especially those that involve human efforts, should include different under-served populations.

3.5 Inclusive S&P community building

Community building is an important aspect of supporting this new wave of research. There is an emerging community of researchers and practitioners interested in inclusive S&P. Examples of community building activities include two workshops on inclusive privacy and security I co-organized at SOUPS2015[1] and SOUPS2017[2]. In addition, a new web site is under development to support this emerging research community: http://www.inclusiveprivacy.org.

4 CONCLUSION

The current mainstream research in security and privacy tends to focus on technical mechanisms and usability. In this article, I highlight that while these two perspectives are invaluable, they fall short of paying enough attention to other equally important issues such as accessibility and needs of many under-served user populations. The idea behind inclusive security and privacy elevates the important consideration of people's abilities, characteristics, needs and values as first-class design requirements for security and privacy mechanisms. I encourage security and privacy researchers and practitioners to think about whether their designs or technical solutions can support or empower various under-served populations to protect their security and privacy. I suggest inclusive security and privacy as a promising third wave of research that both challenges and complements the dominate foci on making security and privacy mechanisms technically sound and usable.

5 ACKNOWLEDGEMENT

I would like to thank the anonymous reviewers, the shepherds Anil Somayaji and Olgierd Pieczul, as well as the NSPW attendees for their thoughtful feedback on this manuscript. I am also grateful to many colleagues such as Kevin Crowston, Jason Dedrick, Apu Kapadia, Yun Huang, Alfred Kobsa, Dan Cosley, Mike Just, Larry Koved, Karyn Moffatt, Lynne Coventry, Jeffrey Bigham, Amy Hurst, Aaron Steinfeld, Lorrie Cranor, Jason Hong, Blase Ur, Norman Su, Jordan Hayes, Natã Barbosa, Huichuan Xia, Yaxing Yao, Xiao Li, Bryan Dosono and Anuj Shah for discussions that helped shape my ideas on this topic. This work was supported in part by the National Institute on Disability, Independent Living, and Rehabilitation Research (NIDILRR Grant 90DP0061-01-00) and the National Science Foundation (NSF Grant CNS-1652497).

REFERENCES

[1] Julio Abascal and Colette Nicolle. 2005. Moving Towards Inclusive Design Guidelines for Socially and Ethically Aware HCI. *Interact. Comput.* 17, 5 (Sept. 2005), 484–505. https://doi.org/10.1016/j.intcom.2005.03.002

[2] Norah Abokhodair. 2015. Transmigrant Saudi Arabian Youth and Social Media: Privacy, Intimacy and Freedom of Expression. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '15)*. ACM, New York, NY, USA, 187–190. https://doi.org/10.1145/2702613.2702629

[3] Norah Abokhodair, Sofiane Abbar, Sarah Vieweg, and Yelena Mejova. 2016. Privacy and Twitter in Qatar: Traditional Values in the Digital World. In *Proceedings of the 8th ACM Conference on Web Science (WebSci '16)*. ACM, New York, NY, USA, 66–77. https://doi.org/10.1145/2908131.2908146

[4] Norah Abokhodair and Sarah Vieweg. 2016. Privacy & Social Media in the Context of the Arab Gulf. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems (DIS '16)*. ACM, New York, NY, USA, 672–683. https://doi.org/10.1145/2901790.2901873

[5] Anne Adams and Martina Angela Sasse. 1999. Users Are Not the Enemy. *Commun. ACM* 42, 12 (1999), 40–46.

[6] Tousif Ahmed, Roberto Hoyle, Kay Connelly, David Crandall, and Apu Kapadia. 2015. Privacy Concerns and Behaviors of People with Visual Impairments. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 3523–3532. https://doi.org/10.1145/2702123.2702334

[1] https://cups.cs.cmu.edu/soups/2015/wips.php

[2] https://www.usenix.org/conference/soups2017/workshop-program/wips2017

[7] Tousif Ahmed, Patrick Shaffer, Kay Connelly, David Crandall, and Apu Kapadia. 2016. Addressing Physical Safety, Security, and Privacy for People with Visual Impairments. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/ahmed

[8] Irwin Altman. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding.* Brooks/Cole Publishing Company, Monterey, California.

[9] Shiri Azenkot, Kyle Rector, Richard Ladner, and Jacob Wobbrock. 2012. PassChords: Secure Multi-touch Authentication for Blind People. In *Proceedings of the 14th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS '12).* ACM, New York, NY, USA, 159–166. https://doi.org/10.1145/2384916.2384945

[10] Natã Barbosa, Jordan Hayes, and Yang Wang. 2016. UniPass: Design and Evaluation of A Smart Device-Based Password Manager for Visually Impaired Users. In *Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp 2016).* https://doi.org/10.1145/2971648.2971722

[11] Scott Beach, Richard Schulz, Julie Downs, Judith Matthews, Bruce Barron, and Katherine Seelman. 2009. Disability, Age, and Informational Privacy Attitudes in Quality of Life Technology Applications: Results from a National Web Survey. *ACM Trans. Access. Comput.* 2, 1 (May 2009), 5:1–5:21. https://doi.org/10.1145/1525840.1525846

[12] Victoria Bellotti and A. Sellen. 1993. Design for Privacy in Ubiquitous Environments. In *The Third European Conference on Computer-Supported Cooperative Work (ECSCW'93).* Kluwer, Milan, Italy, 77–92.

[13] Bettye Rose Connell, Mike Jones, Ron Mace, Jim Mueller, Abir Mullick, Elaine Ostroff, Jon Sanford, Ed Steinfeld, Molly Story, and Gregg Vanderheiden. 1997. *The Principles of Universal Design.* Technical Report. The Center for Universal Design, North Carolina State University. https://www.ncsu.edu/ncsu/design/cud/about_ud/udprinciplestext.htm

[14] Courtney Blackwell, Jeremy Birnholtz, and Charles Abbott. 2015. Seeing and being seen: Co-situation and impression formation using Grindr, a location-aware gay dating app. *New Media & Society* 17, 7 (2015), 1117–1136. https://doi.org/10.1177/1461444814521595

[15] Naomi Bloch and Bertram C Bruce. 2011. Older Adults and The New Public Sphere. In *Proceedings of the 2011 iConference.* ACM, 1–7.

[16] Vanessa Boothroyd. 2014. *Older Adults' Perceptions of Online Risk.* Ph.D. Dissertation. Carleton University Ottawa.

[17] Danah Boyd and Alice E. Marwick. 2011. Social Privacy in Networked Publics: Teens Attitudes, Practices, and Strategies. University of Oxford, 1–29. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128

[18] Pam Briggs and Lisa Thomas. 2015. An Inclusive, Value Sensitive Design Perspective on Future Identity Technologies. *ACM Trans. Comput.-Hum. Interact.* 22, 5 (Aug. 2015), 23:1–23:28. https://doi.org/10.1145/2778972

[19] Bryan Dosono, Jordan Hayes, and Yang Wang. 2015. "I'm Stuck!": A Contextual Inquiry of People with Visual Impairments in Authentication. In *Symposium on Usable Privacy and Security (SOUPS).*

[20] Kelly E. Caine, Celine Y. Zimmerman, Zachary Schall-Zimmerman, William R. Hazlewood, L. Jean Camp, Katherine H. Connelly, Lesa L. Huber, and Kalpana Shankar. 2011. DigiSwitch: a device to allow older adults to monitor and direct the collection and transmission of health information collected at home. *Journal of Medical Systems* 35, 5 (Oct. 2011), 1181–1195. https://doi.org/10.1007/s10916-011-9722-1

[21] Roberto Casas, ÃĄlvaro Marco, Jorge L. FalcÃş, JosÃľ I. Artigas, and Julio Abascal. 2006. Ethically Aware Design of a Location System for People with Dementia. In *Computers Helping People with Special Needs*, Klaus Miesenberger, Joachim Klaus, Wolfgang L. Zagler, and Arthur I. Karshmer (Eds.). Number 4061 in Lecture Notes in Computer Science. Springer Berlin Heidelberg, 777–784. http://link.springer.com/chapter/10.1007/11788713_114

[22] Brendan Cassidy, Gilbert Cockton, and Lynne Coventry. 2013. A Haptic ATM Interface to Assist Visually Impaired Users. In *Proceedings of the 15th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS '13).* ACM, New York, NY, USA, 1:1–1:8. https://doi.org/10.1145/2513383.2513433

[23] Ann Cavoukian. 2009. Privacy by design: The 7 foundational principles. *Information and Privacy Commissioner of Ontario, Canada* (2009). https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

[24] Ann Cavoukian. 2011. *Privacy by Design: Strong Privacy Protection - Now, and Well into the Future.* Technical Report. Office of the Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/english/Resources/Reports-and-Submissions/Reports-and-Submissions-Summary/?id=1125

[25] Rajarshi Chakraborty, Claire Vishik, and H Raghav Rao. 2013. Privacy Preserving Actions of Older Adults on Social Media: Exploring The Behavior of Opting Out of Information Sharing. *Decision Support Systems* 55, 4 (2013), 948–956.

[26] Raymundo Cornejo, Robin Brewer, Caroline Edasis, and Anne Marie Piper. 2016. Vulnerability, Sharing, and Privacy: Analyzing Art Therapy for Older Adults with Dementia. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (CSCW '16).* ACM, New York, NY, USA, 1572–1583. https://doi.org/10.1145/2818048.2819960

[27] Lorrie Faith Cranor, Adam L. Durity, Abigail Marsh, and Blase Ur. 2014. ParentsâĂŹ and TeensâĂŹ Perspectives on Privacy In a Technology-Filled World. In *Symposium on Usable Privacy and Security (SOUPS).* https://www.usenix.org/conference/soups2014/proceedings/presentation/cranor

[28] Lorrie Faith Cranor and Simson Garfinkel. 2005. *Security and Usability: Designing Secure Systems that People Can Use* (1 edition ed.). O'Reilly Media, Beijing ; Sebastapol, CA.

[29] Shanee Dawkins, Wanda Eugene, Tamirat Abegaz, and Juan E. Gilbert. 2015. Toward Private and Independent Accessible Write-In Voting: A Multimodal Prediction Approach. In *Universal Access in Human-Computer Interaction. Access to the Human Environment and Culture*, Margherita Antona and Constantine Stephanidis (Eds.). Number 9178 in Lecture Notes in Computer Science. Springer International Publishing, 171–181. http://link.springer.com/chapter/10.1007/978-3-319-20687-5_17 DOI: 10.1007/978-3-319-20687-5_17.

[30] W. Erickson, C. Lee, and S. von Schrader. 2016. *Disability Statistics from the 2014 American Community Survey (ACS).* Technical Report. Cornell University Yang Tan Institute (YTI), Ithaca, NY. www.disabilitystatistics.org

[31] Maha Faisal and Asmaa Alsumait. 2011. Social Network Privacy and Trust Concerns. In *Proceedings of the 13th International Conference on Information Integration and Web-based Applications and Services (iiWAS '11).* ACM, New York, NY, USA, 416–419. https://doi.org/10.1145/2095536.2095620

[32] Batya Friedman. 1996. Value-sensitive Design. *Interactions* 3, 6 (Dec. 1996), 16–23. https://doi.org/10.1145/242485.242493

[33] Batya Friedman, Peter H. Kahn, and Alan Borning. 2008. Value Sensitive Design and Information Systems. In *The Handbook of Information and Computer Ethics*, Kenneth Einar Himma Associateessor, JD and Herman T. Tavaniessor Lecturer visiting scholar/ethicist (Eds.). John Wiley & Sons, Inc., 69–101. http://onlinelibrary.wiley.com/doi/10.1002/9780470281819.ch4/summary

[34] Simson Garfinkel and Heather Richter Lipford. 2014. *Usable Security: History, Themes, and Challenges.* Morgan & Claypool Publishers.

[35] Juan E. Gilbert, Joshua I. Ekandem, Shelby S. Darnell, Hanan Alnizami, Aqueasha M. Martin, and Wanda Johnson. 2011. Accessible Voting: One Machine, One Vote for Everyone. In *CHI '11 Extended Abstracts on Human Factors in Computing Systems (CHI EA '11).* ACM, New York, NY, USA, 517–518. https://doi.org/10.1145/1979742.1979549

[36] Juan E. Gilbert, Yolanda McMillian, Ken Rouse, Philicity Williams, Gregory Rogers, Jerome McClendon, Winfred Mitchell, Priyanka Gupta, Idong Mkpong-Ruffin, and E. Vincent Cross. 2010. Universal access in e-voting for the blind. *Universal Access in the Information Society* 9, 4 (Feb. 2010), 357–365. https://doi.org/10.1007/s10209-009-0181-0

[37] Erving Goffman. 1959. *The Presentation of Self in Everyday Life* (1 ed.). Anchor.

[38] Gregg C. Vanderheiden. 1998. Universal Design and Assistive Technology in Communication and Information Technologies: Alternatives or Complements? *Assistive Technology* 10, 1 (June 1998), 29–36. https://doi.org/10.1080/10400435.1998.10131958

[39] Galen A Grimes, Michelle G Hough, Elizabeth Mazur, and Margaret L Signorella. 2010. Older Adults' Knowledge of Internet Hazards. *Educational Gerontology* 36, 3 (2010), 173–192.

[40] Seda GÃijrses, Carmela Troncoso, and Claudia Diaz. 2011. Engineering Privacy by Design. (Jan. 2011). https://lirias.kuleuven.be/handle/123456789/356730

[41] S Harrison, D Tatar, and P Sengers. 2007. The Three Paradigms of HCI.

[42] Joseph Henrich, Steven J. Heine, and Ara Norenzayan. 2010. The weirdest people in the world? *The Behavioral and Brain Sciences* 33, 2-3 (June 2010), 61–83; discussion 83–135. https://doi.org/10.1017/S0140525X0999152X

[43] Harry Hochheiser, Jinjuan Feng, and Jonathan Lazar. 2008. Challenges in Universally Usable Privacy and Security. In *SOUPS2008.* http://citeseerx.ist.psu.edu/viewdoc/citations; jsessionid=61FCF04E085C097EA6DD9733C51636E2?doi=10.1.1.206.3380

[44] J. Holman, J. Lazar, and J. Feng. 2008. Investigating the Security-related Challenges of Blind Users on the Web. In *Designing Inclusive Futures*, Patrick Langdon BSc, CEng John Clarkson MA MIEE, and Peter Robinson MA Ceng (Eds.). Springer London, 129–138. http://link.springer.com/chapter/10.1007/978-1-84800-211-1_13 DOI: 10.1007/978-1-84800-211-1_13.

[45] Chris Jay Hoofnagle, Jennifer King, Su Li, and Joseph Turow. 2010. How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policies? (2010).

[46] E. Vincent Cross Ii, Shanee Dawkins, Jerome McClendon, Tony Sullivan, Greg Rogers, Arit Erete, and Juan E. Gilbert. 2009. Everyone Counts: Voting Accessibility. In *Universal Access in Human-Computer Interaction. Applications and Services*, Constantine Stephanidis (Ed.). Number 5616 in Lecture Notes in Computer Science. Springer Berlin Heidelberg, 324–332. http://link.springer.com/chapter/10.1007/978-3-642-02713-0_34 DOI: 10.1007/978-3-642-02713-0_34.

[47] JEROME H. SALTZER and MICHAEL D. SCHROEDER. 1975. The Protection of Information in Computer Systems. *Proceedings of IEEE* 9 (1975), 1278–1308. http://www.cs.virginia.edu/~evans/cs551/saltzer/

[48] Shaun K. Kane, Chandrika Jayant, Jacob Wobbrock, and Richard Ladner. 2009. Freedom to roam: a study of mobile device adoption and accessibility for people with visual and motor disabilities. (2009), 115–122. https://doi.org/10.1145/1639642.1639663

[49] Ruogu Kang, Stephanie Brown, Laura Dabbish, and Sara B. Kiesler. 2014. Privacy Attitudes of Mechanical Turk Workers and the US Public.. In *SOUPS*. 37–49.

[50] Simeon Keates and P. John Clarkson. 2003. *Countering Design Exclusion: An Introduction to Inclusive Design* (2004 edition ed.). Springer, London.

[51] Ponnurangam Kumaraguru and Lorrie Cranor. 2005. Privacy in India: Attitudes and Awareness. *Proceedings of the 2005 workshop on privacy enhancing technologies (PET05)* (2005). http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.109.3325

[52] Marc Langheinrich. 2002. A Privacy Awareness System for Ubiquitous Computing Environments. In *the 4th International Conference on Ubiquitous Computing*. G\Ãűteborg, Sweden, 237–245.

[53] Patricia A Larkin-Lieffers. 2000. The Older Adult and Public Library Computer Technology: A Pilot Study in A Canadian Setting. *Libri* 50, 4 (2000), 225–234.

[54] Sharon J. Laskowski, Marguerite Autry, John Cugini, William Killam, and James Yen. 2004. Improving the usability and accessibility of voting systems and products. (2004). http://user-centereddesign.com/files/NISTHFReport.pdf

[55] Jonathan Lazar. 2007. *Universal usability: Designing computer interfaces for diverse user populations*. John Wiley & Sons. http://books.google.com/books?hl=en&lr=&id=BeHo0XPylDAC&oi=fnd&pg=PR7&dq=Universal+usability+Lazar&ots=junLeIDi90&sig=nZU3dj1wnXVAuqLkybW8UqhAqHE

[56] K. Lebeck, K. Ruth, T. Kohno, and F. Roesner. 2017. Securing Augmented Reality Output. In *2017 IEEE Symposium on Security and Privacy (SP)*. 320–337. https://doi.org/10.1109/SP.2017.13

[57] Scott Lederer, I. Hong, K. Dey, and A. Landay. 2004. Personal privacy through understanding and action: five pitfalls for designers. *Personal Ubiquitous Comput.* 8, 6 (Nov. 2004), 440–454. https://doi.org/10.1007/s00779-004-0304-9

[58] Vilma Lehtinen, Jaana Näsänen, and Risto Sarvas. 2009. A Little Silly and Empty-Headed: Older Adults' Understandings of Social Networking Sites. In *Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology*. British Computer Society, 45–54.

[59] Lesa Lorenzen-Huber, Mary Boutain, L. Jean Camp, Kalpana Shankar, and Kay H. Connelly. 2010. Privacy, Technology, and Aging: A Proposed Framework. *Ageing International* 36, 2 (Dec. 2010), 232–252. https://doi.org/10.1007/s12126-010-9083-y

[60] Yao Ma, Jinjuan Feng, Libby Kumin, and Jonathan Lazar. 2013. Investigating User Behavior for Authentication Methods: A Comparison Between Individuals with Down Syndrome and Neurotypical Users. *ACM Trans. Access. Comput.* 4, 4 (July 2013), 15:1–15:27. https://doi.org/10.1145/2493171.2493173

[61] Wiebke Maaß. 2011. The Elderly and The Internet: How Senior Citizens Deal with Online Privacy. In *Privacy online*. Springer, 235–249.

[62] Ronald L. Mace, Graeme J. Hardie, and Jaine P. Place. 1990. *Accessible environments: Toward universal design*. Center for Accessible Housing, North Carolina State University.

[63] Wendy March and Constance Fleuriot. 2006. Girls, technology and privacy: "is my mother listening?". In *Proceedings of the SIGCHI conference on Human Factors in computing systems*. ACM, 107–110. https://doi.org/10.1145/1124772.1124790

[64] Bryan A. Marshall, Peter W. Cardon, Daniel T. Norris, Natalya Goreva, and Ryan DâĂŹSouza. 2008. Social networking websites in India and the United States: A cross-national comparison of online privacy and communication. *Issues in Information Systems, IX* 2 (2008), 87–94. http://iacis.org/iis/2008/S2008_911.pdf

[65] Andrew R McNeill, Lynne Coventry, Jake Pywell, and Pam Briggs. 2017. Privacy Considerations When Designing Social Network Systems to Support Successful Ageing. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 6425–6437.

[66] Maia Naftali and Leah Findlater. 2014. Accessibility in Context: Understanding the Truly Mobile Experience of Smartphone Users with Motor Impairments. In *Proceedings of the 16th International ACM SIGACCESS Conference on Computers & Accessibility (ASSETS '14)*. ACM, New York, NY, USA, 209–216. https://doi.org/10.1145/2661334.2661372

[67] National Center for Health Statistics. 2015. *Tables of Summary Health Statistics for U.S. Adults: 2014 National Health Interview Survey*. Technical Report. http://www.cdc.gov/nchs/nhis/shs/tables.htm

[68] Helen Nissenbaum. 2004. Privacy as Contextual Integrity. *Washington Law Review Association* 79 (2004), 119–158. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=534622

[69] Helen Nissenbaum. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford Law Books.

[70] Helen Nissenbaum. 2011. A Contextual Approach to Privacy Online. *Daedalus* 140, 4 (Sept. 2011), 32–48. https://doi.org/10.1162/DAED_a_00113

[71] Daniela Oliveira, Harold Rocha, Huizi Yang, Donovan Ellis, Sandeep Dommaraju, Melis Muradoglu, Devon Weir, Adam Soliman, Tian Lin, and Natalie Ebner. 2017. Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 6412–6424.

[72] Leysia Palen and Paul Dourish. 2003. Unpacking "privacy" for a networked world. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, Ft. Lauderdale, Florida, USA, 129–136. https://doi.org/10.1145/642611.642635

[73] Leysia Palen and Marilyn Salzman. 2002. Voice-mail Diary Studies for Naturalistic Data Capture Under Mobile Conditions. In *Proceedings of the 2002 ACM Conference on Computer Supported Cooperative Work (CSCW '02)*. ACM, New York, NY, USA, 87–95. https://doi.org/10.1145/587078.587092

[74] Anicia N. Peters, Heike Winschiers-Theophilus, and Brian E. Mennecke. 2015. Cultural influences on Facebook practices: A comparative study of college students in Namibia and the United States. *Computers in Human Behavior* 49 (Aug. 2015), 259–271. https://doi.org/10.1016/j.chb.2015.02.065

[75] Lisa Quirke. 2012. Information Practices in Newcomer Settlement: A Study of Afghan Immigrant and Refugee Youth in Toronto. In *Proceedings of the 2012 iConference (iConference '12)*. ACM, New York, NY, USA, 535–537. https://doi.org/10.1145/2132176.2132278

[76] Elizabeth B.-N. Sanders and Pieter Jan Stappers. 2008. Co-creation and the new landscapes of design. *CoDesign* 4, 1 (March 2008), 5–18. https://doi.org/10.1080/15710880701875068

[77] Douglas Schuler and Aki Namioka. 1993. *Participatory Design: Principles and Practices*. CRC Press.

[78] Bryan C. Semaan, Lauren M. Britton, and Bryan Dosono. 2016. Transition Resilience with ICTs: 'Identity Awareness' in Veteran Re-Integration. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 2882–2894. https://doi.org/10.1145/2858036.2858109

[79] Kristen Shinohara and Jacob O. Wobbrock. 2011. In the Shadow of Misperception: Assistive Technology Use and Social Interactions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. ACM, New York, NY, USA, 705–714. https://doi.org/10.1145/1978942.1979044

[80] Ben Shneiderman. 2000. Universal usability. *Commun. ACM* 43, 5 (May 2000), 84–91. https://doi.org/10.1145/332833.332843

[81] Carmit-Noa Shpigelman and Carol J. Gill. 2014. How do adults with intellectual disabilities use Facebook? *Disability & Society* 29, 10 (Nov. 2014), 1601–1616. https://doi.org/10.1080/09687599.2014.966186

[82] Richard A Sit. 1998. Online Library Catalog Search Performance by Older Adult Users. *Library & Information Science Research* 20, 2 (1998), 115–131.

[83] H. Jeff Smith, Tamara Dinev, and Heng Xu. 2011. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly* 35, 4 (Dec. 2011), 989–1016. http://dl.acm.org/citation.cfm?id=2208940.2208950

[84] Daniel Solove. 2002. Conceptualizing Privacy. *California Law Review* 90, 4 (July 2002), 1087. http://scholarship.law.berkeley.edu/californialawreview/vol90/iss4/2

[85] Daniel Solove. 2006. A Taxonomy of Privacy. *University of Pennsylvania Law Review* 154, 3 (2006), 477–564.

[86] Sarah Spiekermann. 2012. The Challenges of Privacy by Design. *Commun. ACM* 55, 7 (July 2012), 38–40. https://doi.org/10.1145/2209249.2209263

[87] Sarah Spiekermann and Lorrie Faith Cranor. 2009. Engineering Privacy. *IEEE Transactions on Software Engineering* 35, 1 (Jan. 2009), 67–82. https://doi.org/10.1109/TSE.2008.88

[88] Valerie Steeves. 2006. ItâĂŹs not childâĂŹs play: the online invasion of childrenâĂŹs privacy. *University of Ottawa Law and Technology Journal* 3, 1 (2006), 169–188.

[89] Ed Steinfeld. 1994. The concept of universal design. In *Proceedings of the Sixth Ibero-American Conference on Accessibility*. http://www.envcom.jp/pdf/12p132.pdf

[90] Molly Follette Story. 1998. Maximizing usability: the principles of universal design. *Assistive technology* 10, 1 (1998), 4–12. http://www.tandfonline.com/doi/abs/10.1080/10400435.1998.10131955

[91] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2014. Intruders versus intrusiveness: teens' and parents' perspectives on home-entryway surveillance. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, 129–139. http://dl.acm.org/citation.cfm?id=2632107

[92] U.S. Department of Health, Education and Welfare. 1973. *U.S. Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens*. Technical Report.

[93] Valerie Steeves and Priscilla Regan. 2014. Young people online and the social value of privacy. *Journal of Information, Communication and Ethics in Society* 12, 4 (Nov. 2014), 298–313. https://doi.org/10.1108/JICES-01-2014-0004

[94] Yang Wang, Gregory Norcie, Saranga Komanduri, Alessandro Acquisti, Pedro Giovanni Leon, and Lorrie Faith Cranor. 2011. "I regretted the minute I pressed share": A Qualitative Study of Regrets on Facebook. In *Proceedings of the Seventh Symposium on Usable Privacy and Security (SOUPS '11)*. ACM, New York, NY, USA, 10:1–10:16. https://doi.org/10.1145/2078827.2078841

[95] Yang Wang, G. Norice, and L. Cranor. 2011. Who Is Concerned about What? A Study of American, Chinese and Indian Users' Privacy Concerns on Social Network Sites. *Trust and Trustworthy Computing* (2011), 146–153.

[96] Alma Whitten and Doug Tygar. 1999. Why Johnny CanâĂŹt Encrypt: A Usability Evaluation of PGP 5.0.. In *Ninth USENIX Security Symposium*.

[97] Pamela Wisniewski, Heng Xu, Mary Beth Rosson, Daniel F. Perkins, and John M. Carroll. 2016. Dear Diary: Teens Reflect on Their Weekly Online Risk Experiences. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*

(CHI '16). ACM, New York, NY, USA, 3919–3930. https://doi.org/10.1145/2858036.2858317

[98] Jacob O. Wobbrock, Shaun K. Kane, Krzysztof Z. Gajos, Susumu Harada, and Jon Froehlich. 2011. Ability-Based Design: Concept, Principles and Examples. *ACM Trans. Access. Comput.* 3, 3 (April 2011), 9:1–9:27. https://doi.org/10.1145/1952383.1952384

[99] World Health Organization (WHO). 2014. *Visual impairment and blindness Fact Sheet 282.* Technical Report. http://www.who.int/mediacentre/factsheets/fs282/en/

[100] Bo Xie, Ivan Watkins, Jen Golbeck, and Man Huang. 2012. Understanding and Changing Older Adults' Perceptions and Learning of Social Media. *Educational Gerontology* 38, 4 (2012), 282–296.

[101] Heng Xu, Robert E. Crossler, and France BÃĬLanger. 2012. A Value Sensitive Design Investigation of Privacy Enhancing Tools in Web Browsers. *Decis. Support Syst.* 54, 1 (Dec. 2012), 424–433. https://doi.org/10.1016/j.dss.2012.06.003

[102] Hanlu Ye, Meethu Malu, Uran Oh, and Leah Findlater. 2014. Current and Future Mobile and Wearable Device Use by People with Visual Impairments. In *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 3123–3132. https://doi.org/10.1145/2556288.2557085

[103] Seounmi Youn. 2009. Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *Journal of Consumer Affairs* 43, 3 (Sept. 2009), 389–418. https://doi.org/10.1111/j.1745-6606.2009.01146.x