Editors: Heather Richter Lipford, richter@uncc.edu | Jessica Staddon, jessica.staddon@gmail.com

SOCIOTECHNICAL SECURITY AND PRIVACY

Inclusive Security and Privacy

Yang Wang | *Syracuse University*

Alex is blind and is in his 50s. He works as a librarian in a local public library. Part of his job is to help people with disabilities use library computers equipped with assistive technologies. Like many other people with visual impairments, Alex uses computers and browses the Internet via screen readers, a type of software that parses and reads aloud content displayed on a computer/device screen.

One day Alex was logging into Gmail on a library computer with the JAWS screen reader, and it took him more than five minutes to successfully log in. This was a frustrating experience not because he was unaware but because Gmail fell short of supporting people with visual impairments. In this particular case, Alex typed gmail.com in the browser address bar but could not find the field to type in his account name on the Gmail page after several attempts. Being an advanced user, he hypothesized that another user might have previously logged into Gmail on this computer. Next, he needed to confirm this hypothesis by identifying the name of the other user and finally did so after frustratingly combing his way through the page: "*OK, there it is…so that's her email.*" After finding the name of the other user, he then struggled to find the button he needed to log into his own account because he was unsure of the terminology used to describe the login area: "*sometimes it's 'log in as another user,' sometimes it's 'sign in as another user,' sometimes it's 'change user.'*" He felt that constantly changing the terminology of login elements introduces a new and steep learning curve regarding how to locate the authentication area quickly and efficiently: "*unfortunately, this is something that we run into a lot, you don't know what they call things, and every time they update the website, you have to re-learn how to do it.*" Alex eventually worked his way through the links to find the login page that asked him for his account name and password. He typed those in, and he was logged in. However, it was not readily clear to him that he had logged in and he had to go through the page to make that inference.

This was one of many challenging situations that we observed during our study on authentication experiences of people with visual impairments.[1] Alex is an advanced computer user, but even for him, a seemingly mundane authentication task can be both time consuming and error prone. He told us that many of his library patrons with disabilities were frustrated with current designs of computers and the Internet. What's worse, they blamed themselves rather than the technologies and gave up using technologies.

Unfortunately, this is just one example of the exclusion of users with disabilities. This is not an issue that only people with visual impairments or disabilities experience. This is an example of much broader, complex, and systematic issues associated with today's end-user privacy and security designs. The root problem is that our user-facing privacy and security designs have not paid enough attention to a wide range of under-studied users, such as children, older adults, people with disabilities, activists, journalists, victims of crimes or domestic violence, and people from non-Western or developing countries.

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. The importance of the human aspects of privacy/security has also long been recognized. Since Saltzer and Schroeder's seminal work in 1975 advocating for computer security mechanisms to be "psychologically acceptable,"[2] the human factors and more specifically the usability of security and privacy mechanisms have become a key research topic (see *Usable Security: History, Themes, and Challenges*[3] for a recent review). For instance, Whitten and Tyler conducted a well-known user study of Pretty Good Privacy (PGP), an encryption program, and found that it was difficult for ordinary people to use it. Thus, this study exposed the limited value of PGP and highlighted the importance of usability in security mechanisms. More broadly, usability has been considered a first-class design requirement for security and privacy designs.[4] For the past decade, the community of usable privacy and security (for instance, the annual Symposium on Usable Privacy and Security [SOUPS]) has been growing. However, something is worth noting inside and outside of that community.

In the field of psychology, an influential meta-study found that over 80 percent of published psychological studies focused on people from Western, Educated, 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.[5]

Unfortunately, I believe that a similar problem of not paying enough attention to the wide variety of user populations exists in the current usable privacy and security literature. Looking through the 13 years (2005–2017) of SOUPS conference proceedings, less than 10 percent of papers (about 20 out of 215 papers) had data about under-studied users (for instance, children, older adults, or people from non-WEIRD countries). This suggests that even though the privacy and security community has taken the human perspective seriously, it has narrowly focused on certain types of users. This is problematic because these under-studied user populations are essentially left out, and the current end-user privacy/security mechanisms fall short of supporting them to ensure their privacy and security.

The good news is that some privacy/security research has started to pay attention to these under-studied users. For instance, UniPass is an accessible password manager for blind users,[6] and DigiSwitch is a device for older adults to monitor and control the collection and transmission of their health information.[7] These examples illustrate the prospect of making security and privacy designs more inclusive to under-served populations. However, these research efforts, while very valuable, are still in the peripheral of the field. The wide range of under-served populations deserve more attention and research in a more systematic way.

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—is a perspective that takes human abilities and characteristics as first-class design requirements and aims to design mechanisms that are inclusive to the widest possible range of users. Inclusive S&P needs a stronger presence to make it more mainstream, similar to the way usability was elevated and is now widely recognized in the field of security and privacy. Thus, inclusiveness should be expected in all security and privacy designs rather than being a property that only a few system designers espouse.

This article highlights the limitations of the current framings/foci of security and privacy research and advocates for a new perspective of security and privacy research.

A Research Framework of Inclusive Security and Privacy

The long-term research agenda of inclusive S&P 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 S&P designs encompass 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 rethink 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*.[8]

Research Challenges

The vision of universal design is design for everyone. In practice, this is very difficult if not impossible. Several empirical studies investigate the privacy/security concerns and practices of certain under-served populations such as children, older adults, people with disabilities, and people from non-Western or developing countries (see "The Third Wave?: Inclusive Privacy and Security"[9] for a recent review). For instance, Ahmed and colleagues interviewed people with visual impairments and found that they face difficulties in detecting visual or aural eavesdropping, have physical security and privacy concerns (for instance, using an ATM), and sometimes need to ask others (even strangers) to help (for instance when reading documents or typing in a PIN while shopping).[10] There are very few studies that attempt to study multiple under-served populations (for an example, see "An Inclusive, Value Sensitive Design Perspective on Future Identity Technologies"[11]).

People from different under-served groups may have profoundly different needs and challenges for security and privacy (Figure 1). In fact, even people with the same disability condition can vary significantly in terms of their abilities, needs, and technology uses. The scholarship from black feminist theories has proposed *intersectionality*, the idea that every person has a multifaceted identity consisting of race, class, gender, and sexuality.[12] This body of literature warns against over-generalization and advocates paying attention to individuals' complex identity structures and lived experiences.

Figure 1. The neurodiversity sign symbolizes the diversity of human abilities, needs, characteristics, and values.

Ethical challenges also exist. Some of these under-served populations may be considered vulnerable (for instance, children) and thus require researchers/designers to be extra cautious about how to preserve these users' interests. When working with under-served populations, researchers/designers might subconsciously bring their own biases especially when they are not part of the under-served groups. Feminist scholars have proposed the notion of *positionality*,[13] highlighting that research/design process is power laden, and urge researchers/designers to examine and mitigate their own biases. It is also worth noting that under-served populations may experience improvements of life during a study (for instance, trying out a research prototype), but they are likely to revert back to their previous life conditions after the study, which can be frustrating to say the least. Therefore, it is important for researchers to be mindful about addressing this challenge. For instance, the researchers may consider providing their participants the option of keeping the prototype after the study.

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

Design for Inclusive Security and Privacy

The design for inclusive security and privacy can build on several lines of research, such as value-sensitive design (VSD) and accessible design. VSD is a generic design approach that highlights and supports values in system design such as user autonomy, freedom from bias, privacy, and trust.[14] It has been applied to assess technologies or privacy designs. For instance, 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.[11] They identified both common values and different impacting factors across these community groups regarding how people think about future identity technologies.[11] 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 judgments and justify their design decisions, especially when there are conflicting values (for instance, national security and personal privacy).

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. Wobbrock and colleagues propose ability-based design, which shifts the view from focusing on people's disabilities to their abilities.[15] They offer seven ability-based design principles based on their extensive experiences in designing technologies for people with disabilities. These principles include ability, accountability, adaptation, transparency, performance, context, and commodity.[15] For instance, the principle of ability states that "Designers will focus on ability not dis-ability, striving to leverage all that users can do."[15] The principle of accountability means that designers should change the systems rather than the users if the systems do not perform well.[15] 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.

Research Agenda

This preliminary research agenda of inclusive security and privacy focuses on privacy for people with visual impairments as a concrete example domain. Similar research topics could be conducted for the security and privacy needs of other under-served populations as well as the intersectionality of these populations.

Inclusive Security/Privacy Analysis

The extant literature on people's security and privacy concerns, preferences, and practices tends to focus on interviews or surveys that might not capture people's everyday experiences as they enact their privacy and security. As suggested by the literature on intersectionality, a particularly valuable addition is to study people's 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.

While the diary study approach can provide many insights into the everyday privacy challenges and practices of people with visual impairments, it has an important limitation—it's based on self-reported data. For instance, studies have shown that people with visual impairments face challenges in recognizing emergent security/privacy threats (for instance, shoulder surfing). Therefore, they may miss reporting privacy-invading incidents that they did not recognize. To address this methodological limitation, one could also conduct lightweight ethnographic studies to directly observe how people enact their security and privacy in their daily life but also help identify potential risks that the participants did not recognize. A researcher will "shadow" a participant for an extended period of time (for instance, a few days) in the participant's home and/or workplace upon permission.

In addition, critical and participatory approaches that center on people who are under-served, collect their personal stories, and conduct meta-analyses of studies would be very valuable in understanding these people's security/privacy needs and practices.

Inclusive Design and Evaluation

The prior literature and the results of the inclusive security and privacy analysis can be fed into the design of inclusive security and privacy mechanisms.

One promising design approach in this context is participatory design[16] where the design team directly includes members of the target user population (for example, children) who will actively engage throughout the design process. These participatory design sessions should engage a wide range of stakeholders including people from different under-served groups. These design sessions can be structured to explore everyone's own security and privacy concerns and practices, co-design, and pilot-test low-fidelity designs. 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. 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.

Inclusive Design Guidance Development

The goal of this research direction is to develop design guidelines for creating security and privacy designs that are inclusive to different user abilities, identities, and values. This research direction can include several components. First, inclusive security and privacy prototypes can be evaluated by existing design guidelines for privacy (such as in "Privacy as Contextual Integrity"[17]) and for accessibility and inclusion (such as in "Ability-Based Design: Concept, Principles and Examples"[15]). 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. Third, research can seek to provide further design guidance for supporting other under-served populations based on evaluation results of inclusive security and privacy prototypes.

While it is desirable to derive inclusive security/privacy design patterns (that is, what/how to do) and anti-patterns (that is, what/how to avoid) that can be applied universally, practically this might be extremely difficult if not impossible due to the seemingly 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.

Making Security and Privacy Tools More Inclusive

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

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.

Several colleagues and I have co-organized a series of workshops on inclusive privacy and security (WIPS) at the SOUPS conferences. We discussed a wide range of user groups (such as children, older adults, people with disabilities, crime victims, and people who have little education or low socioeconomic status) and application domains (such as authentication, CAPTCHA, banking/shopping, browser security, and wearables). We also created various scenarios and conducted group design activities for these scenarios. One observation is that we still do not have a systematic methodology to support inclusive design. As discussed earlier, this is a crucial component for future research and development. In addition, a website has been launched to support this emerging research community including a curated bibliography on this topic: *www.inclusiveprivacy.org*.

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 can support or empower various under-served populations to protect their security and privacy. This article supports inclusive security and privacy as a promising new wave of research that both challenges and complements the dominate foci on making security and privacy mechanisms technically sound and usable.

Acknowledgments

This article builds upon a paper previously published in the New Security Paradigms Workshop (NSPW 17). I thank Heather Lipford, Jessica Staddon, Christine Anthony, and Charlotte Price for their help and feedback on this article. I am also grateful to many colleagues such as Anil Somayaji, Olgierd Pieczul, Apu Kapadia, Alfred Kobsa, Dan Cosley, Mike Just, Larry Koved, Karyn Moffatt, Lynne Coventry, Jeffrey Bigham, Amy Hurst, Aaron Steinfeld, John Zimmerman, Lorrie Cranor, Lujo Bauer, Jason Hong, Blase Ur, Norman Su, Jordan Hayes, Natã Barbosa, Yaxing Yao, Yun Huang as well as the NSPW 17 attendees and many colleagues at Syracuse University for discussions that helped shape my ideas. 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. B. Dosono, J. Hayes, and Y. Wang, "I'm Stuck: A Contextual Inquiry of People with Visual Impairments in Authentication," *Symposium on Usable Privacy and Security* (SOUPS), 2015.
2. J.H. Saltzer and M.D. Schroeder, "The Protection of Information in Computer Systems," *Proceedings of IEEE*, vol. 9, 1975, pp. 1278–1308; www.cs.virginia.edu/~evans/cs551/saltzer.
3. S. Garfinkel and H.R. Lipford. *Usable Security: History, Themes, and Challenges*, Morgan & Claypool Publishers, 2014.
4. A. Whitten and D. Tygar. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," *Ninth USENIX Security Symposium*, 1999.
5. J. Henrich, S.J. Heine, and A. Norenzayan, "The Weirdest People in the World?," *The Behavioral and Brain Sciences* vol. 33, nos. 2–3, 2010, pp. 61–83; doi.org/10.1017/S0140525X0999152X.
6. N. Barbosa, J. Hayes, and Y. Wang, "UniPass: Design and Evaluation of A Smart Device-Based Password Manager for Visually Impaired Users," *Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing* (UbiComp 16), 2016.
7. K.E. Caine et al., "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*, vol. 35, no. 5, 2011, pp. 1181–1195; doi.org/10.1007/ s10916-011-9722-1.

8. R.L. Mace, G.J. Hardie, and J.P. Place, "Accessible Environments: Toward Universal Design," Center for Accessible Housing, North Carolina State University, 1990.
9. Y. Wang. "The Third Wave?: Inclusive Privacy and Security," *Proc. of the 2017 New Security Paradigms Workshop* (NSPW 17), 2017, pp. 122–130; doi.org/10.1145/3171533.3171538.
10. T. Ahmed et al., "Addressing Physical Safety, Security, and Privacy for People with Visual Impairments," SOUPS, 2016; https://www.usenix.org/conference/soups2016/technical-sessions/ presentation/ahmed.
11. P. Briggs and L. Thomas, "An Inclusive, Value Sensitive Design Perspective on Future Identity Technologies," *ACM Trans. Comput.-Hum. Interact.*, vol. 22, no. 5, 2015, pp. 23:1–23:28; doi.org/10.1145/2778972.
12. K. Crenshaw, "Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color," *Stanford Law Review*, vol. 43, no. 6, 1991, pp. 1241–1299; doi.org/10.2307/1229039.
13. D. Haraway, "Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective," *Feminist Studies*, vol. 14, no. 3, 1988, pp. 575–599; doi.org/10.2307/3178066.
14. [7] Batya Friedman. 1996. Value-sensitive Design. Interactions 3, 6 (Dec. 1996), 16–23. https://doi.org/10.1145/242485.242493
15. J.O. Wobbrock et al., "Ability-Based Design: Concept, Principles and Examples," *ACM Trans. Access. Comput.*, vol. 3, no. 3, 2011, pp. 9:1–9:27; doi.org/10.1145/ 1952383.1952384.
16. D. Schuler and A. Namioka, *Participatory Design: Principles and Practices*, CRC Press, 1993.
17. H. Nissenbaum, "Privacy as Contextual Integrity," *Washington Law Review Association*, vol. 79, 2004, pp. 119–158; papers.ssrn.com/sol3/papers.cfm? abstract_id=534622.

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

For our digital library

Abstract: The mainstream security and privacy mechanisms often do not consider the wide variety of users. As a result, these mechanisms fall short of empowering many under-served populations such as children, older adults, people with disabilities, and people from non-Western developing countries to effectively protect their security and privacy. In this article, I advocate for a new wave of research that centers on *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.

KEYWORDS: security, privacy, inclusive, accessibility, universal design, intersectionality, Sociotechnical Security and Privacy