Chapter 13
Accessible Privacy

Yang Wang and Charlotte Emily Price

Abstract End-user privacy mechanisms have proliferated in various types of devices and application domains. However, these mechanisms were often designed without adequately considering a wide range of underserved users, for instance, people with disabilities. In this chapter, we focus on the intersection of accessibility and privacy, paying particular attention to the privacy needs and challenges of people with disabilities. The key takeaway messages of this chapter are as follows: (1) people with disabilities face heightened challenges in managing their privacy; (2) existing end-user privacy tools are often inaccessible to people with disabilities, making them more vulnerable to privacy threats; and (3) design guidelines are needed for creating more accessible privacy tools.

13.1 Introduction

Existing end-user privacy mechanisms are often designed without considering the wide range of user populations. As a result, these designs often made assumptions about their users that may or may not hold for underserved populations, such as people with disabilities, children, older adults, and people from non-Western developing countries. These inappropriate assumptions could lead to significant challenges for the underserved users to utilize privacy mechanisms. The difficulties in effectively using these mechanisms could in turn make the underserved users more vulnerable to various privacy risks.

Y. Wang (✉)
University of Illinois at Urbana-Champaign, Champaign, IL, USA
e-mail: yvw@illinois.edu

C. E. Price
Syracuse University, Syracuse, NY, USA
e-mail: ceprice@syr.edu

The web browser lock icon is an example of how design may render privacy-enhancing tools unusable to someone with disabilities. The lock icon was designed to signal the use of secure (HTTPS) communication between the browser and the web server. This user interface design was built on an assumption that its users can easily recognize the icon. However, the lock icon is often inaccessible to people with visual impairments and screen reader users. CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a similar accessibility nightmare for people with visual impairments. Even the seemingly simple Android app permission interface can be confusing to users with little technical knowledge, who may not understand what an app permission means.

While this chapter focuses on privacy needs and challenges of people with disabilities, it is worth noting that there is a fundamental issue in privacy designs that fail to consider underserved populations beyond those with disabilities. In another profound example of an underserved population (i.e., victims of intimate partner abuses), Freed et al. studied how the abusers use technologies to violate the privacy of their victims through surveillance and manipulation [1]. Traditionally, the assumption about attackers is that they do not have easy and full access to victims' devices. However, this study shows that these abusers often have full access to victims' devices. In fact, in many cases, the abusers are the legal owners of these devices [1]. This finding challenges one of the long-held assumptions about the attackers. As such, the existing protection mechanisms would fall short because their underlying assumptions no longer hold for victims of intimate partner abuses. New protection mechanisms are needed to thwart this kind of attacks by intimate partner abusers. Interested readers can refer to the chapter on privacy of vulnerable populations.

Cultural values can also have a significant impact on how people conceptualize privacy and how technologies should be designed to support their privacy management. For example, Vieweg et al. examined Arabic women's social media usage and their associated privacy concerns [2]. This research suggests that unlike social media users in the Western developed countries where the main privacy issues are centered around individuals, Arabic women are more concerned about how their social media usage might put their family reputation at risk [2]. This is a very different kind of privacy concerns (i.e., concerns about one's family more than individuals) that existing social media privacy mechanisms fall short of supporting. Interested readers can refer to Chap. 12 for a more in-depth discussion.

The commonality of these examples is that existing privacy designs tend not to be inclusive to a wide range of user groups. This leads to the conceptualization of inclusive privacy, the idea of designing privacy mechanisms that are inclusive to a wide range of users with diverse abilities, characteristics, needs, and values. The goal of inclusive privacy is desirable, ambitious but also challenging to achieve. In this chapter, we mainly explore *accessible privacy*: designing privacy mechanisms that are accessible to people with disabilities.

In the remainder of this chapter, we will first explore some example groups of people with disabilities and their privacy challenges. We will then discuss why achieving privacy is difficult as well as promising approaches towards accessible privacy. We conclude by suggesting a few future research directions.

The key takeaway messages of this chapter are:

- **People with disabilities face heightened challenges** in managing their privacy.
- **Existing end-user privacy tools are often inaccessible** to people with disabilities, making them more vulnerable to privacy threats.
- **Design guidelines are needed** for creating more accessible privacy tools.

13.2   Privacy and Underserved Populations

In this section, we will explore a few specific underserved populations and their privacy challenges and needs. When we describe people with disabilities, we follow the ACM accessible writing guide [3]. We recognize the important role that language can play in the marginalization of people as well as the language we use may or may not reflect the norms within a particular disability community.

13.2.1   Models of Disability

There are many models (certainly more than three or four) of disability that have been recognized by disability scholars, such as the medical model, the social model, and the critical realist model.

Traditionally, the medical model has been used by scientific communities, but is often considered problematic. This model sees disability as something wrong with a person that must be "fixed" and has contributed to the oppression of people with disabilities. Disability rights activists then proposed social models of disability that identify disability as socially constructed and grounded in society and culture [4]. This refers to disability as a problem with a society's lack of inclusiveness rather than a personal issue [4]. This model also has been critiqued for its emphasis on independent living (which isolates the realities of many people with disabilities who require assistance), as well as supporting "normalization" rather than celebrating or acknowledging disability pride and difference [5]. The cultural/postmodern model was created to address the medical realities, lived experiences, and social elements for some people with disabilities [5]. This model sees disability as another way of being, a cultural standpoint or lifestyle [6]. The critical realistic perspective, which emerged from disability studies and was proposed to inform accessible technology design, also centers on rich, lived experiences of individuals with disabilities [7]. Sins Invalid, a group of artists with disabilities, proposed "A Disability Justice framework understands that all bodies are unique and essential, that all bodies have

strengths and needs that must be met... We understand that all bodies are caught in these bindings of ability, race, gender, sexuality, class, nation state and imperialism, and that we cannot separate them" [8]. It is important to note that these models of disability are often respected based on how an individual associates personally within these frameworks. Thus, researchers and designers need to recognize the complexity and personal tendencies and experiences attached to such models and will dissuade from bifurcating them (e.g., the medical model vs. other models).

In summary, there are many models of disabilities, such as:

- **Medical model: disability is medicalized** as being deviate from the normal biological functions [9].
- **Social model: disability is socially constructed** as being a problem with a society's lack of inclusiveness rather than a personal issue [4].
- **Critical realist model: "disability as an interaction between individual and structural factors"** where individual factors can include impairments and structural factors can include others' attitudes towards disabilities [7].

13.2.2   *People with Visual Impairments*

There are a wide range of disability conditions. Our first example focuses on people with visual impairments. Visual impairments exist on a spectrum, ranging from partial to complete loss of vision. In clinical settings, the term "visual impairment" refers to a "visual acuity of 20/70 or worse in the better eye with best correction, or a total field loss of 140 degrees" [10]. "Blindness" means that a person cannot see anything, whereas "low vision" denotes "sight that may be severe enough to hinder an individual's ability to complete daily activities such as reading, cooking, or walking outside safely, while still retaining some degree of usable vision" [10]. A person can have visual impairments since birth or after birth (e.g., due to accidents, medical conditions, or aging).

While computers and smartphones help improve the independence and quality of life of people with visual impairments, these technologies (particularly the mouse, visual input/output, and touch-based user interfaces) also pose significant accessibility challenges for this user group. In turn, people with visual impairments (especially those living with blindness) often use screen readers (e.g., JAWS, Window-Eyes, NVDA, VoiceOver) on their computers or phones to parse and read the information from the screen. Screen readers usually read a screen sequentially but also support keyboard shortcuts to allow users to skip certain elements of a page or extract a list of hyperlinks on a page for faster navigation. People with visual impairments (especially those with low vision) also use screen magnifiers (e.g., ZoomText, MAGic) to zoom into certain parts of the screen to make it more readable.

People with visual impairments face many accessibility challenges with information and computing technologies and are likely to struggle with current mainstream privacy user interfaces (e.g., https padlock), which heavily rely on visual representations.

Existing literature has highlighted a number of privacy concerns of people with visual impairments:

- **Shoulder surfing** (e.g., during their usage of ATM).
- **Aural eavesdropping** (e.g., screen reader reading aloud private content).
- **Asking others even strangers to read** inaccessible documents (e.g., mails).
- **Using assistive technologies can attract unwanted attention** and make people with visual impairments more noticeable to attackers.
- **Difficulty in using end-user privacy/security mechanisms** (e.g., privacy settings).
- **Taking or sharing images/videos** that might contain private or sensitive content.

These and other related privacy and security concerns/needs of people with visual impairments have been identified. 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 (i.e., the PDF is not marked up with tags that can be read by a screen reader), (5) inaccessible antivirus software, (6) auto install software, (7) auto software updates make software inaccessible, (8) SecurID (a random number display in the device used for logging in), (9) keyloggers, and (10) spams [11]. Some of these are more general accessibility issues such as inaccessible PDF; others are addressed by existing antivirus or anti-spam software. In terms of challenges related to CAPTCHA and authentication, there are a number of mechanisms proposed to improve or replace them (e.g., [12–14]).

People with visual impairments have privacy concerns about using mobile devices when they are in the speakerphone or screen-reading mode or generally in public because others can see or hear what they are speaking or doing [15–17]. People with visual impairments can wear earphones, but that is sometimes inconvenient [16] and could limit their abilities to hear or sense the nearby environment, making them vulnerable to attacks [18]. The iOS Screen Curtain allows iPhone users to blank their screen, but that does not help with the privacy issues caused by the screen-reading mode and users with visual impairments may forget to activate that feature. The use of assistive technology (e.g., a portable magnifier) could attract unwanted attention and make users more noticeable to attackers [15, 19]. People with visual impairments often have to compromise their privacy for achieving independence and/or convenience.

Ahmed et al. have conducted two interview studies specifically investigating the privacy needs and practices of people with visual impairments in online and offline settings [18, 20]. They found that these users face difficulties in detecting visual or aural eavesdropping, have physical privacy and security concerns (e.g., using ATM), and sometimes need to ask others (even strangers) to help (e.g., read documents, type pin in shopping) [20]. There are proposed solutions for specific tasks (e.g.,

accessible ATM [21]), but no generic solution to address the privacy risks emerged from asking others to help.

These 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) [18]. These privacy settings have been found to be difficult for social media users in general [22]. Furthermore, we have found that people with visual impairments were also concerned about online tracking (i.e., their data or web browsing activities being collected by companies or governments) [23], which has been shown as a privacy concern of the general population [24]. There are browser extensions such as script blockers (e.g., NoScript) and ad blockers (e.g., Ghostery) that block third-party content or scripts on a webpage, but they have usability issues for general Internet users [25].

A few studies have focused on privacy/security issues for people with visual impairments. Many privacy/security threats arise from the use of accessible technology, as these devices inadvertently generate new avenues for passersby to learn personal information. People with visual impairments have concerns about aural and visual eavesdropping in public when using screen readers and screen magnifiers, respectively [26–29]. Prior work also suggests that this user group may not notice privacy/security risks in their environment or inherent in the technology they use [30]. The use of accessible technologies can also draw unwanted attention and potential exploitation [31]. To mitigate some of these issues, people with visual impairments use privacy features (e.g., iOS Screen Curtain) and wear headphones to mitigate problems with screen readers [32]. Ahmed et al. identified privacy/security concerns or challenges people with visual impairments face such as difficulties verifying the security of banking or shopping websites, maintaining privacy on social media, asking strangers for help [18] and physical safety/security challenges in public spaces and at home [20]. Our most recent ethnographic research with people with visual impairments and their allies in their everyday lives found that they often work cooperatively to protect the privacy and security of people with visual impairments, yet most existing privacy/security mechanisms fall short of supporting this kind of cooperative behaviors [23].

There are a number of privacy-enhancing technologies (PETs) designed for people with visual impairments:

- **Accessible authentication** (e.g., PassChords [12], UniPass [33])
- **Accessible CAPTCHAs** (e.g., more accessible audio CAPTCHAs [34])
- **Privacy-enhancing assistive features** (e.g., Apple's Screen Curtain)
- **General assistive tools** making content more accessible and people with visual impairment more independent (e.g., screen readers)

Prior research efforts primarily those from the field of accessible computing have proposed different mechanisms to support people with visual impairments in various privacy and security-related tasks. One notable example is more accessible CAPTCHA (i.e., Completely Automated Public Turing test to tell Computers and Humans Apart) designs, for instance, using pairs of images and sounds [35, 36] as well as moving the controls for audio CAPTCHAs within the answer textbox of the

authentication interface [13]. Another notable area is authentication. For instance, Azenkot et al. designed a password scheme that utilizes patterns of finger taps on a touchscreen [26]. Barbosa et al. designed a password manager that allows visually impaired users to easily transfer their login credentials from their mobile devices to web-based services [37].

Previous research has also elicited feedback on proposed solutions to physical privacy and security threats. Ahmed et al. found that their visually impaired participants appreciated the idea of devices that could detect the number of people in their vicinity, assist them with navigation, and prevent shoulder surfing attacks [18]. In their follow-up study, participants endorsed the idea of knowing others' proximity, identity, and activities, as well as inferences about the intentions of others' actions [20].

13.2.3 Are Existing Privacy-Enhancing Technologies Sufficient?

While there is not much research on the experiences of people with visual impairments in using privacy-enhancing technologies, there are anecdotes that suggest the existing PETs are insufficient for this user group. For instance, privacy/security indicators (e.g., the https lock icon in web browsers) might not be very accessible to people with visual impairments who use screen readers. Privacy settings have also been shown to be difficult for people with visual impairments [18]. Some of these are difficult to use for the broader population. It is also worth noting that some assistive technologies can introduce privacy issues. For instance, visual question and answer tools such as Be My Eyes and VizWiz [38] allow blind users to take pictures and ask questions about the pictures to crowd workers or volunteers (who can be total strangers). These pictures might contain private or sensitive content (e.g., credit cards, medicine details) [39].

13.2.4 Intersectional Privacy

Empirical research on people with visual impairments in general and their privacy and security practices in particular tend to focus on their visual impairments, which often are, however, a single aspect of their multifaceted and intersectional marginalized identities. In our own experiences of working with people with visual impairments, we found that many of them often have other aspects of marginalized identities such as other disabilities, minoritized race, and gender identities [23]. These multifaceted and intersectional marginalized identities often contribute to their challenges and influence their privacy and security practices [23].

Intersectionality is a key analytic framework proposed by Kimberlé Williams Crenshaw in the late 1980s and is situated in the lived experiences of black women, women of color, and intersecting identity structures of race, class, gender, and sexuality [40]. Crenshaw's intersectionality arose from a legal perspective regarding a case in which an African American woman sued a company for discrimination in not hiring her. The judge dismissed the case because the company claimed to hire African Americans and women. In response, Crenshaw problematized this claim because African American women have multifaced identities including both gender and racial identities, and suggested that the company did not hire African American women. Crenshaw wrote, "I used the concept of intersectionality to denote the various ways in which race and gender interact to shape the multiple dimensions of Black women's employment experiences" [40]. Among this initial definition, Crenshaw has specified three kinds of intersectionality: structural, political, and representational. Structural intersectionality refers to how "the location of women of color at the intersection of race and gender" informs identity and marginalized positions [40]. Political intersectionality highlights how "feminist and antiracist politics have, paradoxically, often helped to marginalize the issue of violence against women of color." Representational intersectionality refers to cultural norms that create certain minoritized positions regarding identities [40]. It is important to note that the concept of intersectionality encompasses many important factors beyond race and gender such as class and sexuality (e.g., used in queer studies by LGBTQ+ activists).

Since the term intersectionality has been coined, it has been adapted by a large number of feminist, critical race, critical disablty, and queer studies scholars as a research framework to examine complex identity and social structures. While retaining the black feminist foundation of this framework, critical disability scholars such as Rosemarie Garland-Thomson have proposed a disability axis on an "intersectionality nexus" which views disability not only as socially constructed but also intrinsically multifaceted [41]. In this foundational scholarship, she connects disability, race, gender, class, and queer theory [41]. Specifically, she considers disability along these complex and multifaceted elements such as political, social, and personalized understandings of disability identity [41]. As such, her ability/disability system is meant to show another identity perspective to Crenshaw's notion of intersectionality [42].

Intersectionality has been a recent topic in human-computer interaction (HCI) scholarship with the call for inclusion of critical theories such as feminism (e.g., [43]) and critical race (e.g., [44]). This line of work advocates that by using intersectional analyses, people can be better understood, thus leading to richer data and more ethical methodologies and designs (e.g., [44]). For instance, Schlesinger et al. point out that besides race, gender, and class, other dimensions such as disability or age are also good for intersectional analysis [44].

In our studies on visual impairments, we found many of our participants to have intersectional identities along with the visual impairments that shaped their experiences [23]. Therefore, we adopted intersectionality as an analytic lens to unpack the everyday privacy/security experiences of people with visual impair-

ments. Our intersectional analysis is akin to *intracategorical intersectionality* [45], which "focuses on a single identity category...and then analyze other dimensions of identity within the target community" [44]. We focused on people with visual impairments while considering their overlapping identity dimensions (e.g., age, gender identity, and other disabilities) [23].

For instance, one of our participants unfortunately lost her sight in an accident. She is a mother and self-identifies with having bipolar disorder and a learning disability. She lives with her children and mother. She often asks their help with many things from emailing to managing her bank account. We observed that her privacy and security needs and practices were often influenced by these multifaceted and intersectional aspects of her identity. She gave a hypothetical example where it would be difficult for her to have another male friend to illustrate her inability to hide her phone conversations, which might in turn lead to misunderstanding from her boyfriend. She wants to control the visibility of the conversations on her phone herself, but she found the technologies too overwhelming to learn. There are typically functionalities such as deleting phone call records, text messages, or the contact information that allow phone owners to protect their privacy and communication on the phone. However, there is no simple one-click feature that "[hides] conversations on a phone." In practice, users need to understand and use a combination of technical features to clean their conversations (in various apps) on the phone. This participant said she had a hard time knowing and learning how to use all these features. One key insight here is that the combination and intersection of her visual impairments, bipolar disorder, and learning disability probably all played a role in her challenges in using the technologies and achieving her privacy/security goals on her own [23].

13.2.5 *People with Hidden Disabilities*

We use the term "hidden disabilities" as an umbrella term to cover a wide range of disabilities such as learning disabilities (e.g., dyslexia), autism spectrum, and attention deficit hyperactivity disorder (ADHD) as well as psychosocial, internal conditions such as chronic pain, and mobility disorders as well as anything "not obvious" to others. Disability and HCI research tend to focus on physical disabilities such as visual and motor impairments rather than hidden disabilities. Even fewer studies have been done to understand people with hidden disabilities and their privacy and security needs.

In our own research, we conducted focus groups with people with hidden disabilities to understand their information disclosure practices, in particular the disclosure of their disability identities. Similar to our study on visual impairments, we found that people with hidden disabilities often also have multiplicity in identity. In addition, since their disabilities are often not obviously visible to others, their (marginalized) identity disclosure is a key aspect of their everyday privacy practices.

We identified two main domains (i.e., professional and informal/social) in which our participants with hidden disabilities make decisions about whether, when, and how to disclose their disability identities. Professional domains include academic or job settings, whereas informal/social domains include online (particularly social media) and in-person settings (e.g., family and friends). We observed that our participants exhibited various types of identity disclosure behaviors in these two domains. We adopted MacDonald-Wilson et al.'s definitions for these different disclosure behaviors:

- **Forced disclosure** (e.g., students with disabilities requesting accommodations)
- **Selective disclosure** (i.e., a person with disabilities chooses when and whom to disclose which aspects of the disabilities)
- **Nondisclosure** (i.e., a person with disabilities chooses not to disclose any aspects of the disabilities)
- **Disclosure by others** (e.g., a friend or family member discloses one's disabilities often without one's permission)

Forced disclosure refers to a situation where individuals are "required by circumstances" to disclose their disability identity to another person, typically an employer or a supervisor, "or in the need for accommodation" [46]. *Selective disclosure* denotes "sharing information with specific or a limited number of people, or sharing specific or limited information with others" [46]. MacDonald-Wilson et al. also consider selective disclosure as being "used to access protections under the ADA [Americans with Disabilities Act] while minimizing risks related to stigma, and allows the person the option to 'blend in' or 'pass for normal'" [46]. *Nondisclosure* means "a choice made by individuals to keep private any information" regarding their disability identity, which they mention "may result in additional stress and lower self-esteem because one is hiding an aspect of one's life, but it also protects the individual from potential stigma and discrimination" [46].

We found that disclosure by others was more prevalent in informal social settings. For instance, one participant explained an unpleasant experience: "Yeah, I think the experiences that I have mostly had with that-with people telling other people without my permission-is with my family. I know that they have good intentions, but I'd prefer not to go to a family gathering and have everyone come up to me saying, 'Oh, I'm sorry you had a breakdown yesterday.' That's a little awkward for me, not knowing where that information is going to. I know that my mom tells her twin sister, they're really close so she feels like she can share that kind of information. But when it comes back to me, or she texts me, they have good intentions, but I'd prefer to be able to come to them when I feel like I want to." As noted, this participant did not mind sharing her disability condition but did not accept nonconsensual disclosure because she lost the agency in controlling her information.

Academic and professional settings, on the other hand, often exhibit forced disclosure or nondisclosure of their disability identities. Many of our participants felt forced to disclose their disabilities in schools to get accommodation or at workplaces to perform their work and to ensure their supervisors or colleagues that they are not lazy. For instance, one participant shared, "The other times when I've

had pressure to disclose was when I was at work and I would have crazy anxiety. No one could tell because I'm extroverted introvert, no one could tell. So I'd be like, 'ok, I have anxiety.' Or I'm not meeting deadlines, and I know I have a problem, but again, I don't have a formal ADHD diagnosis so I don't really know how to explain it. There are times when I really think I've gotten in some trouble because of my disability, but I wasn't able to advocate because I wasn't able to express that, you know, I'm not lazy." Sometimes, our participants experienced the opposite where they felt "forced" not to disclose their disabilities by their families, who believed that disclosing the disabilities would, for instance, negatively affect one's chance of employment.

Our participants also disclosed specific disabilities and other marginalized identities differently. In general, the participants were comfortable disclosing their physical disabilities more than their hidden disabilities, citing stigma associated with hidden disability identity disclosure. One participant said, "I post about when I'm in pain, physically. I don't post about being emotionally in pain, but I have posted about my history with suicide a little bit." Some participants segmented social media platforms and used different platforms/accounts for different purposes. For instance, one participant had three Instagram accounts and used one of them, a private account, to relate to her disabilities. She explained, "For Instagram, I actually have three accounts for Instagram. I have a public account that I rarely ever post on, and I rarely ever look at, but it's just nice pictures of me doing things. And then I have a private Instagram account, where I follow a lot of chronic illness accounts, I don't post anything personally about my own chronic illnesses, usually, but I'll follow and comment and stuff. Then I also have a service dog one that's private where I can talk to other service dog handlers, but both of those are closed so I have control over who I allow to see those." Even though she shared nothing about her disability, she understood that the pages she follows can be visible to others and hence preferred another account rather than using the same one. Anonymity on these accounts also helped. If the target audience did not know about their real identities, the participants felt more comfortable sharing about their disability. In terms of future design, designers should explore ways to further support these users to avoid forced disclosures and to facilitate selective and nondisclosure as well as "blending in" or "passing" if these users choose to.

13.2.6 People with Other Disabilities

While there is a large body of research that demonstrates various web accessibility challenges for people with other disabilities (e.g., motor impairments, cognitive impairments), little is known about their privacy challenges and needs. There is some empirical evidence that people with Down syndrome struggle with remembering mnemonic passwords [47] and people with intellectual disabilities had difficulties remembering passwords [48]. Future research is needed to uncover additional privacy challenges for these user groups.

13.3   Why Is Accessible Privacy Difficult?

While more scholars and practitioners are starting to recognize the importance of making privacy mechanisms more accessible to a wide range of users, there are a number of challenges.

Designing accessible privacy mechanisms is difficult for a number of reasons. First, the designers need to understand the specific underserved group's privacy challenges and needs as well as their broader technology usage and social contexts. Traditional interviews and surveys are helpful, but they may fall short of providing sufficient contextual nuances of the group's everyday social settings. Ethnographic research is one way that may help fill the gap. However, conducting passive observation is also not easy for underserved populations because they are often close-knit communities that external parties including researchers may not have access to. Our experiences have been that many years of volunteering in local disability communities help us to establish trustworthy relationships with underserved groups, who were engaged in our various research efforts.

Second, there is often considerable variance within an underserved group. For instance, visual impairments range from low vision to complete loss of vision. This matters because they may have quite different technology usage. For instance, while blind users often use screen readers, users with low vision might not use screen readers and might use screen magnifiers.

Third, we need to respect and consider the complex and intersectional nature of people's marginalized identities. In our own research, we found that many of our participants with visual impairments also self-identified with other disabilities (e.g., cognitive impairments) and other marginalized identities such as LGBTQ+. Their privacy and security practices are also influenced by these multifaceted and intersectional identities. How to design to support the combinatory and intersectional nature of their privacy/security needs and practices is particularly difficult because these intersectional characteristics are complex and nuanced.

Fourth, there are a large (or even infinite) number of marginalized user groups. If the goal is to truly achieve universal design where every person is supported, then the design needs to accommodate everybody including all the marginalized user groups. Supporting the practices of one particular marginalized user group might put unduly burden or conflict with the practices of another user group. If one were to pursue a largest common denominator approach, it is unclear what design options are still available.

Last but not least, some recent work shows that even accessibility features could introduce unintended privacy/security vulnerabilities. For instance, audio CAPTCHA, which was supposed to be a more accessible alternative to image CAPTCHA, could be bypassed by over-the-counter speech recognition algorithms, effectively defeating the purpose of CAPTCHA and making the system more vulnerable [49]. Future designs that aim to improve accessibility need to go through privacy/security reviews and testing to identify any potential vulnerabilities.

In summary, some of the main challenges in designing for accessible privacy include:

- **Need to understand the target underserved users'** privacy challenges and needs.
- **There are often considerable within-group variances** of an underserved population.
- **Need to consider the complex and intersectional nature** of people's disability/marginalized identities.
- **There are a large (or even infinite) number of marginalized groups** (that one can study).
- **Assistive technologies that were designed to improve accessibility for people with disabilities might pose privacy risks** to these users.

13.4   Working Towards Accessible Privacy

Best Practices Working with people from marginalized groups is both fulfilling and challenging. Because of their marginalized identities, researchers and designers need to be extra thoughtful about how to engage with the target user groups in an ethical and empowering manner. Unfortunately, there is a dark history of marginalized groups being taken advantage of or even abused in the name of research (e.g., the abuse of people with disabilities in the Nazi experiments). Therefore, it is perhaps not surprising that marginalized groups are often close-knit and keep a distance of the outside even to academic researchers. In order to closely work with marginalized groups, researchers need to build a trustworthy relationship with the target user populations. In our own experiences of working with people with disabilities, we found that one productive way is volunteering in the local organizations that serve people with disabilities. We were able to interact/help with the local community and build relationships with them after a few years of volunteering.

It might seem trivial, but it is actually quite important to create accessible and inclusive research/study materials. When we were working with people with visual impairments, it took us a while to improve our study materials that used icons (for users with low vision) and nontechnical language in our study fliers and consent form. We also created videos with caption to explain our study. Besides, we used index cards for participants to answer Likert scale questions (i.e., pointing to a card with an answer on the table, e.g., strongly agree). The PDFs of study materials were also made accessible to screen readers. All of these efforts lowered the barriers for people with visual impairments to participate in our studies.

Research Methodologies One promising design approach in this context is participatory design [50] where the design team directly includes members of the target user population (e.g., children) who will actively engage throughout the design process. These participatory design sessions should engage a wide range

of stakeholders including people from different underserved 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.

Several scholars have conducted studies using a *participatory action research* method with the goal of bringing their target population to the center and empowering them to actively involve themselves in the movement for necessary change to meet their needs. Balcazar et al., for example, designed and facilitated a PAR study specifically directed at individuals with disabilities and highlighted four key principles: (1) direct participation from individuals with disabilities in problem identification and solution generation, (2) such direct interaction and involvement provides a more holistic view of the research from the perspective of individuals with disabilities, (3) the participatory action research process has the ability to raise awareness of participants' strengths, resources, and abilities, and ultimately (4) PAR is designed to improve the overall quality of life for individuals with disabilities [51]. The researchers cite examples from participants in their study to illustrate each of the four principles in action, demonstrating how each principle worked to improve participants' experiences [51]. They also address the challenges of PAR, which include difficulty developing and maintaining lasting relationships with their participants, the ability to sustain and develop the research over time, the duration of the entire research process, and the potential unintended consequences resulting from conducting participatory action research [51].

Duarte et al. conducted a study involving young forced migrants that combined participatory design and participation action research elements [52]. The authors argued that using participatory action research allowed for the inclusion of their participants in an active role regarding the conduct of the studies themselves and creating a safe space, which they realized was also a limitation of their research [52]. Used well with inclusive participatory design practices, conducting research such as this allows for participants to bring their expertise and unique needs to the forefront while fostering change that would help them in the long run.

Design Approaches *Value-sensitive design* (VSD) is a generic design approach that highlights and supports values in system design [53, 54]. Example values include user autonomy, freedom from bias, privacy, and trust [53]. 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 [55]. 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 [56]. They identified both common values and different impacting factors across these community groups regarding how people think about future identity technologies [56]. As shown in this example, VSD can be useful in

identifying the underlying values that underserved user groups have and assessing whether these values have been supported in security and privacy designs.

Ability-based design proposed by Wobbrock et al., shifts the view from focusing on people's disabilities to their abilities [57]. 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 [57]. For instance, the principle of ability states that "Designers will focus on ability not *dis*-ability, striving to leverage all that users *can* do" [57]. The principle of accountability means that designers should change the systems rather than the users if the systems do not perform well [57]. These principles have proven valuable for designing accessible technologies for people with disabilities and should be adopted for accessible security and privacy designs that support a wide range of underserved user groups.

Ethical Considerations Some of these underserved populations may be considered vulnerable (e.g., children) and thus require the researchers/designers to be extra cautious about how to preserve these users' interests. When working with underserved populations, researchers/designers might subconsciously bring their own biases especially when they are not part of the underserved groups. Feminist scholars have proposed the notion of positionality [58], which highlights that research/design process is power laden and urges the researchers/designers to examine and mitigate their own biases. It is also worth noting that underserved 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.

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

Accessibility and Privacy Considerations Accessibility has been widely recognized as a key concern in IT and web design. Accessibility laws such as Section 508 of the Rehabilitation Act of 1973 and the Americans with Disabilities Act (ADA) in the USA may require IT and websites to be accessible to people with disabilities. These legal requirements as well as industry standards (e.g., W3C web accessibility standards) have played an important role in improving IT accessibility. Making privacy mechanisms accessible is a desirable goal, and we have seen some promising examples in technologies and laws. For instance, the California Consumer Privacy Act (CCPA) requires privacy policies or notices to be accessible. However, it is worth repeating that accessible or assistive technologies might introduce new privacy risks (e.g., making user with disabilities more noticeable to

attackers). Therefore, one cannot assume that technologies designed for improving accessibility would always have a positive or neutral impact on user privacy. One ought to conduct both accessibility and privacy risk assessment when designing for accessible privacy.

13.5   Future Directions

We advocate for a list of future directions for researchers and practitioners.

Cooperative Privacy One promising direction is designing to support people especially those from marginalized groups to collaborate in privacy management. Privacy and security mechanisms are often focused on the individual's perspective, for instance, a privacy or security warning that a user can act on. In contrast, cooperative privacy fosters interdependence, which is especially beneficial for the everyday privacy management of people with visual impairment. What would a "cooperative" warning look like? Perhaps it could have built-in support for people to seek help or get feedback from others (e.g., allies), for instance, an option on the warning to ask for help. One possible cooperative privacy design could take the form of a mobile app or a website where users with visual impairments could choose to share only with specific allies they invite to the system any information about them, such as schedules and common tasks they perform. If users felt their privacy/security is at risk, they can request help from selected allies, requesting a chat session in real time where allies would be providing assistance as needed.

Users would have full control over the disclosure of any private information that they share via the system. This is just one example of a rich yet largely untapped design space for cooperative privacy and security mechanisms. These types of designs will not only be helpful for people with visual impairments and their allies but also computer users more generally (e.g., technically savvy users and novice users).

Personalized Privacy While most existing privacy mechanisms were designed to be "one size fits all," there is increasing recognition that personalized mechanisms that cater to individuals are a promising direction for future privacy design. It is particularly promising for accessible privacy because of its potential in supporting complex and intersectional nature of individuals' marginalized identities and needs.

Design Principles Since there are a large number of marginalized or underserved user groups, how can we systematically study and understand these groups as well as explore the design space? Given that there are an increasing number of scholars across multiple disciplines that are interested in designing for various specific groups, one strategy is to identify common as well as unique challenges, needs, and practices across these groups.

The goal of this research direction is to develop design guidelines for creating security and privacy designs that are accessible to different user abilities, identities, and values. This research direction can include several components. First, accessible

security and privacy prototypes can be evaluated by existing design guidelines for privacy (e.g., [59]) and for accessibility and inclusion (e.g., [57]). Second, it can include other underserved populations. Given that people from different underserved groups can differ drastically, tools designed for one underserved population may or may not be directly applicable to other underserved populations. In fact, different underserved 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 underserved populations based on evaluation results of accessible security and privacy prototypes.

While it is desirable to derive accessible 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 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 underserved populations.

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 accessible privacy. There are a series of workshops on inclusive privacy and security (WIPS): https://inclusiveprivacy.org/workshops.html. We discussed a wide range of user groups (e.g., children, older adults, people with disabilities, crime victims, and people who have little education or low socioeconomic status) and application domains (e.g., 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.

There are also an increasing number of scholars from the more traditional computer/network security community that are interested in this topic. There will be a convergence of scholars and practitioners from different fields and countries that explore different aspects of accessible privacy and security.

In summary, we advocate the following future directions:

- **Design to support both independence and interdependence** (cooperation between marginalized users and their allies) in privacy management.
- **Design to support personalized or customizable** privacy management.
- **Systematization of knowledge about the privacy challenges and needs** of different marginalized user groups.
- **Develop design principles** that can guide the development of accessible privacy mechanisms for a wide range of marginalized user groups.
- **Build a community of scholars and practitioners** from various disciplines such as disabilities, ethics, laws, cybersecurity, privacy, human-computer interaction, and design.

References

1. Freed, Diana, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise": How intimate partner abusers exploit technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, CHI '18*, 667:1–667:13. New York, NY: ACM.
2. Vieweg, Sarah, and Adam Hodges. 2016. Surveillance & modesty on social media: How Qataris navigate modernity and maintain tradition. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing, CSCW '16*, 527–538. New York, NY: ACM.
3. Vicki, L. October 2015. Hanson, Anna Cavender, and Shari Trewin. Writing about accessibility. *Interactions* 22 (6): 62–65.
4. Shakespeare, Tom. 2006. The social model of disability. In *The Disability Studies Reader*, ed. Lennard J. Davis, 2–197. Hove, East Sussex: Psychology Press.
5. Mankoff, Jennifer, Gillian R. Hayes, and Devva Kasnitz. 2010. Disability studies as a source of critical inquiry for the field of assistive technology. In *Proceedings of the 12th International ACM SIGACCESS Conference on Computers and Accessibility, ASSETS '10*, 3–10. New York, NY: ACM.
6. Waldschmidt, Anne. 2018, June. Disability–Culture–Society: Strengths and weaknesses of a cultural model of dis/ability. *Alter* 12 (2): 65–78.
7. Frauenberger, Christopher. 2015. Disability and technology: A critical realist perspective. In *Proceedings of the 17th International ACM SIGACCESS Conference on Computers & Accessibility, ASSETS '15*, 89–96. New York, NY: ACM.
8. Sins Invalid. 2018. *Sins invalid | An unshamed claim to beauty in the face of invisibility.*
9. Corker, Mairian, and Tom Shakespeare. 2002. *Disability/postmodernity: Embodying Disability Theory*. London; New York: Continuum. OCLC: 47237980.
10. American Foundation for the Blind. Key Definitions of Statistical Terms, 2008.
11. Holman, J., J. Lazar, and J. Feng. 2008. Investigating the security-related challenges of blind users on the web. In *Designing Inclusive Futures*, ed. Patrick Langdon, CEng John Clarkson, and Peter Robinson, 129–138. London: Springer.
12. Azenkot, Shiri, 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*, 159–166. New York, NY: ACM.
13. Bigham, Jeffrey P., and Anna C. Cavender. 2009. Evaluating existing audio CAPTCHAs and an interface optimized for non-visual use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1829–1838. New York, NY: ACM.
14. Sauer, Graig, Jonathan Lazar, Harry Hochheiser, and Jinjuan Feng. 2010, June. Towards a universally usable human interaction proof: Evaluation of task completion strategies. *ACM Transactions on Accessible Computing* 2 (4): 15:1–15:32.
15. 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, 115–122.

16. Naftali, Maia, 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*, 209–216. New York, NY: ACM.

17. Ye, Hanlu, Meethu Malu, Oh. Uran, 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*, 3123–3132. New York, NY: ACM.

18. Ahmed, Tousif, Roberto Hoyle, Kay Connelly, David Crandall, and Apu Kapadia. 2015. Privacy concerns and behaviors of people with visual impairments. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI2015*, 3523–3532. New York, NY: ACM.

19. Shinohara, Kristen, 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*, 705–714. New York, NY: ACM.

20. Tousif Ahmed, Patrick Shaffer, Kay Connelly, David Crandall, and Apu Kapadia. 2016. Addressing physical safety, security, and privacy for people with visual impairments. In *SOUPS2016*, 341–354.

21. Cassidy, Brendan, 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*, 1:1–1:8. New York, NY: ACM.

22. 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*, 10:1–10:16. New York, NY: ACM.

23. Jordan Hayes, Smirity Kaushik, Charlotte Emily Price, and Yang Wang. 2019. *Cooperative Privacy and Security: Learning from People with Visual Impairments and Their Allies*.

24. Ur, Blase, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012. Smart, useful, scary, creepy: Perceptions of online behavioral advertising. In *Proceedings of the Eighth Symposium on Usable Privacy and Security, SOUPS '12*, 4:1–4:15. New York, NY: ACM.

25. Pedro G. Leon, Blase Ur, Rebecca Balebako, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012. Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising. In *Proceeding of the SIGCHI Conference on Human Factors in Computing Systems*, Austin, Texas.

26. Azenkot, Shiri, Kyle Rector, Richard E. Ladner, and Jacob O. Wobrock. 2012. PassChords: Secure multi-touch authentication for blind people. In *Assets '12 Proceedings of the 14th International ACM SIGACCESS Conference on Computers and Accessibility*, 159–166. New York, NY: ACM.

27. Bryan Dosono, Jordan Hayes, and Yang Wang. 2015. "I'm Stuck!": A contextual inquiry of people with visual impairments in authentication. In *Proceedings of the 11th Symposium On Usable Privacy and Security (SOUPS)*, 151–168.

28. Shaun K. Kane, Chandrika Jayant, Jacob O. Wobbrock, and Richard E. Ladner. 2009. Freedom to Roam: A study of mobile device adoption and accessibility for people with visual and motor disabilities. In *ASSETS'09, October 25–28, 2009, Pittsburgh, Pennsylvania, USA*, 115–122.

29. Naftali, M., and L. 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 and Accessibility – ASSETS 2014*, 209–216. New York, NY: ACM.

30. Brady, Erin, and Jeffrey P. Bigham. 2015, November. Crowdsourcing accessibility: Human-powered access technologies. *Foundations and Trends in Human-Computer Interaction* 8 (4): 273–372.

31. Kristen Shinohara, and Jacob O. Wobbrock. 2011, May. In the Shadow of misperception: Assistive technology use in social interactions. In *Proceedings of the 29th Annual Conference on Human Factors in Computing Systems – CHI 2011*, 705–714.

32. Ye, Hanlu, Meethu Malu, Oh. Uran, and Leah Findlater. 2014, April. 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 2014*, 3123–3132. New York, NY: ACM.

33. Nata Barbosa, Jordan Hayes, and Yang Wang. 2016. Uni-Pass: 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)*.

34. Fanelle, Valerie, Sepideh Karimi, Aditi Shah, Bharath Subramanian, and Sauvik Das. 2020. *Blind and human: Exploring more usable audio CAPTCHA designs*, 111–125. Berkeley: USENIX Association. isbn: 9781939133168.

35. Jonathan Holman, Jonathan Lazar, Jinjuan Heidi Feng, and John D'Arcy. 2007. Developing usable CAPTCHAs for blind users. In *Proceedings of the 9th International ACM SIGACCESS Conference on Computers and Accessibility*, 245–246.

36. Sauer, Graig, Jonathan Lazar, Harry Hochheiser, and Jinjuan Feng. 2010. Towards a universally usable human interaction proof: Evaluation of task completion strategies. *Information Sciences* 2 (4): 15.

37. Natã M Barbosa, Jordan Hayes, and Yang Wang. 2016. UniPass: Design and evaluation of a smart device-based password manager for visually impaired users. In *UbiComp*, 49–60.

38. Jeffrey P. Bigham, Chandrika Jayant, Hanjie Ji, Greg Little, Andrew Miller, Robert C. Miller, Robin Miller, Aubrey Tatarowicz, Brandyn White, Samual White, and others. 2010. VizWiz: Nearly real-time answers to visual questions. In *Proceedings of the 23nd Annual ACM Symposium on User Interface Software and Technology*, 333–342. New York, NY: ACM.

39. Stangl, Abigale, Kristina Shiroma, Bo Xie, Kenneth R. Fleischmann, and Danna Gurari. 2020, October. Visual content considered private by people who are blind. In *The 22nd International ACM SIGACCESS Conference on Computers and Accessibility, ASSETS '20*, 1–12. New York, NY, USA: Association for Computing Machinery.

40. Crenshaw, Kimberle. 1991. Mapping the margins: Intersectionality, identity politics, and violence against women of color. *Stanford Law Review* 43 (6): 1241–1299.

41. Garland-Thomson, Rosemarie. 1997, January. *Extraordinary bodies: Figuring physical disability in American culture and literature*. New York: Columbia University Press.

42. ———. 2002. Integrating disability, transforming feminist theory. *NWSA Journal* 14 (3): 1–32.

43. Bardzell, Shaowen, and Jeffrey Bardzell. 2011. Towards a feminist HCI methodology: Social science, feminism, and HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '11*, 675–684. New York, NY: ACM.

44. Ari, Schlesinger, W. Keith Edwards, and Rebecca E. Grinter. 2017. Intersectional HCI: Engaging identity through gender, race, and class. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, CHI '17*, 5412–5427. New York, NY: ACM.

45. McCall, Leslie. 2005. The complexity of intersectionality. *Signs* 30 (3): 1771–1800.

46. MacDonald-Wilson, Kim L., Zlatka Russinova, E. Sally Rogers, Chia Huei Lin, Terri Ferguson, Shengli Dong, and Megan Kash MacDonald. 2011. Disclosure of mental health disabilities in the workplace. In *Work Accommodation and Retention in Mental Health*, 191–217. New York: Springer.

47. Ma, Yao, Jinjuan Heidi Feng, Libby Kumin, Jonathan Lazar, and Lakshmidevi Sreeramareddy. 2012, October. Investigating authentication methods used by individuals with down syndrome. In *Proceedings of the 14th International ACM SIGACCESS Conference on Computers and Accessibility, ASSETS '12*, 241–242. New York, NY: Association for Computing Machinery.

48. Buehler, Erin, William Easley, Amy Poole, and Amy Hurst. 2016, April. Accessibility barriers to online education for young adults with intellectual disabilities. In *Proceedings of the 13th Web for All Conference, W4A '16*, 1–10. New York, NY: Association for Computing Machinery.

49. Solanki, Saumya, Gautam Krishnan, Varshini Sampath, and Jason Polakis. 2017. In (Cyber)Space bots can hear you speak: Breaking audio CAPTCHAs Using OTS speech recognition. In *Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security, AISec '17*, 69–80. New York, NY: ACM. Event-Place: Dallas, TX.
50. Schuler, Douglas, and Aki Namioka. 1993, March. *Participatory Design: Principles and Practices*. Boca Raton: CRC Press.
51. Balcazar, Fabricio E., Christopher B. Keys, Daniel L. Kaplan, and Yolanda Suarez-Balcazar. 1998. Participatory action research and people with disabilities: Principles and challenges. *Canadian Journal of Rehabilitation* 12: 105–112.
52. Duarte, Ana Maria Bustamante, Nina Brendel, Auriol Degbelo, and Christian Kray. 2018. Participatory design and participatory research: An HCI case study with young forced migrants. *ACM Transactions on Computer-Human Interaction (TOCHI)* 25 (1): 3.
53. Friedman, Batya. 1996, December. Value-sensitive design. *Interactions* 3 (6): 16–23.
54. Friedman, Batya, Peter H. Kahn, and Alan Borning. 2008. Value sensitive design and information systems. In *The Handbook of Information and Computer Ethics*, ed. Kenneth Einar Himma and Herman T. Tavaniessor, 69–101. Hoboken: John Wiley & Sons.
55. Xu, Heng, Robert E. Crossler, and France BéLanger. 2012, December. A value sensitive design investigation of privacy enhancing tools in web browsers. *Decision Support Systems* 54 (1): 424–433.
56. Briggs, Pam, and Lisa Thomas. 2015, August. An inclusive, value sensitive design perspective on future identity technologies. *ACM Transactions on Computer-Human Interaction* 22 (5): 23:1–23:28.
57. Wobbrock, Jacob O., Shaun K. Kane, Krzysztof Z. Gajos, Susumu Harada, and Jon Froehlich. 2011, April. Ability-based design: Concept, principles and examples. *ACM Transactions on Accessible Computing* 3 (3): 9:1–9:27.
58. Haraway, Donna. 1988. Situated knowledges: The science question in feminism and the privilege of partial perspective. *Feminist Studies* 14 (3): 575–599.
59. Nissenbaum, Helen. 2004. Privacy as contextual integrity. *Washington Law Review Association* 79: 119–158.