Chapter 15
Privacy and Vulnerable Populations

Nora McDonald and Andrea Forte

Abstract Vulnerable populations face unique privacy risks that not only challenge designers' preconceptions about privacy, these challenges are also frequently overlooked in decisions about privacy design and policy. This chapter defines and describes vulnerable populations and the challenges they face, as well as the research approaches that have traditionally been used to understand and design technologies that respect the privacy needs of vulnerable people. It describes how existing frameworks fail to account for the privacy concerns of people who experience heightened risk. It then introduces alternative ways of thinking about privacy that can help technologists, researchers, policy makers, and designers do a better job of serving the needs of the most vulnerable users of technology. We conclude with concrete guidance around identifying and integrating vulnerable populations into technology design for privacy.

15.1 Introduction

Section Highlights

- **We define vulnerable individuals as those who, because of their race, class, gender or sexual identity, religion, or other intersectional characteristics or circumstances**, are more susceptible to privacy violations that result in emotional, financial, or physical harm or neglect.
- **We consider some of these identities (e.g., LGBTQ, survivors of domestic abuse, and minority individuals and their intersections) in depth**, particularly the way these identities create some pressing and unique challenges.

N. McDonald (✉)
University of Cincinnati, School of Information Technology, Cincinnati, OH, USA

A. Forte
College of Computing and Informatics, Drexel University, Philadelphia, PA, USA
e-mail: aforte@drexel.edu

B. P. Knijnenburg et al. (eds.), *Modern Socio-Technical Perspectives on Privacy*,
https://doi.org/10.1007/978-3-030-82786-1_15

- **This chapter is comprised of six sections**, exploring how technologies exacerbate existing inequalities; what the specific privacy concerns and needs of certain vulnerable populations might encompass and current gaps in research; the role that social norms play in shaping privacy theory; a way forward that proposes intersectional approaches to some of the biggest challenges for vulnerable communities; and finally how technologists can identify and incorporate vulnerable populations into requirements gathering, testing, and policy making, including a thought experiment to help guide readers as they consider how to incorporate vulnerable users into their design process.

In this chapter, we define vulnerable individuals as people who are more susceptible to privacy violations that result in emotional, financial, or physical harm or neglect as a consequence of their race, class, gender or sexual identity, religion, or other intersectional characteristics or circumstances that marginalize them from society. While some legal scholars have identified misconceptions about privacy that traverse socioeconomic status, they also suggest that low-income, marginalized, and immigrant (particularly, foreign-born) communities are uniquely susceptible [1, 2] to these forms of privacy risk. We expand on this view of vulnerability to also include survivors of domestic abuse [3–5], people who have been incarcerated, immigrants [1, 6], activists, journalists [7], those who have been politically oppressed by society or their culture, those with HIV [8], LGBTQ [9–12], as well as the very young [13, 14] and very old [15], which are discussed in depth in Chapters 13 and 14. In this chapter, we demonstrate how the needs and experiences of these various identities are unique and often require different kinds of privacy protections than the general population.

Designing for privacy of *any* individuals poses considerable challenges for researchers and businesses who provide digital tools and infrastructure for users. Yet recent research on technology and privacy has surfaced what we already knew or intuited about vulnerable populations: inequalities that make people vulnerable offline are often replicated (or exacerbated) by networked technologies (cf. [2, 16–19]). The unique sensitivities that put vulnerable populations at risk frequently break designers' assumptions, which is compounded by our concern that vulnerable people are often overlooked (or not fully examined) as stakeholders in the design process—from requirements gathering, to ideation, to implementation and testing, and ultimately to policy making. In this chapter, we discuss why it is important to understand and empower vulnerable people and how to reflect their needs in policy and design.

In Chap. 2, the authors introduced various privacy frameworks applicable to digital spaces. Here, we focus on the evolution from individual-based theories, to norm-based theories, and, finally, to identity-based theories that consider structures of inequality. Identity-based theories and frameworks are useful for studying and designing for privacy with vulnerable populations because they are more attuned to the structural inequalities that make some individuals more susceptible to privacy violations. They also help explain why violations of privacy may be more dire for vulnerable individuals.

This chapter is comprised of six main sections. In the second section below, we explore how technologies exacerbate existing inequalities. In the third, we go on to explore what the privacy concerns and needs of certain vulnerable populations might encompass and discuss current gaps in research that supports more equitable and more universally effective design. In the fourth section, we review the role that social norms play in shaping privacy theory. In the fifth section, we propose intersectional approaches to some of the biggest challenges for vulnerable communities. We go on in the sixth section to give concrete examples of how technologists can identify and incorporate vulnerable populations into requirements gathering, testing, and policy making. We explore potential applications of our recommendations through a thought experiment and offer closing thoughts about current design recommendations and future challenges.

15.2 How Technology Reinforces and Promotes Inequality

Section Highlights

- **Service providers (e.g., social networks and apps) have exacerbated inequalities** by adopting policies that remove (pseudo)anonymity and potentially harm vulnerable populations.
- **In particular, the popular "real-name" policies and secondary authentication** (e.g., with email or phone) limit individuals' ability to remain anonymous. These policies result in censorship and opportunity loss and may, indeed, be easily hacked.
- **Algorithms that have become ubiquitous in our society, which profile and harm low-income and marginalized individuals,** unleash discrimination in virtually every aspect of their lives from their social networks, to their shopping, to their jobs and job searches.

We are only beginning to learn how technologies can reinforce and/or exacerbate existing inequalities. Below, we discuss three key ways technology has changed in the last decade that influence inequitable outcomes. First, policies that remove the safety of (pseudo)anonymity that may be desired by vulnerable populations. Second, one specific way that service providers (those who provide the platform and tools for online networks) regulate identity information is by requiring the use of secondary authentication (e.g., with email or phone) or real names—even requesting that users verify accounts with mobile or photo ID—which limits individuals' ability to control their privacy. These measures have become standard under the rubric of safety and security. Developers and, perhaps, others with privileged identities may take for granted that relinquishing identity information to social networks (when they request ID verification) or apps is an accepted norm. Third, algorithmic biases reinforce existing inequalities and can even propagate discriminatory practices.

Research on anonymity offers some insight into how privacy can be critical in providing opportunities for safe disclosure and interaction that are not otherwise available [20–25]. Anonymity provides avenues for overcoming ineluctable social norms embedded in existing (offline) social structures. Research on adolescents who use Ask.fm found that anonymity created opportunities for authentic self-expression and self-discovery among other social goals [26]. Pseudonymity can also facilitate self-disclosures [21, 22] on a range of topics that are critical to a person's psychological well-being [27–29], for example, by sexual abuse survivors [20] and domestic abuse survivors [25]. Environments that provide (pseudo)anonymous safe havens for identity exploration seem to be diminishing. Sites like Reddit no longer make throwaway accounts an obvious (pseudo)anonymity strategy, and subreddits regularly remove posts from new accounts, making it difficult to post (pseudo)anonymously with a throwaway account. At the same time, platforms that promote more ephemeral communications [30] are gaining in popularity.

Meanwhile, the trend toward more "authentic" [31] Internet participation requiring the use of real names raises concerns for vulnerable groups. For example, Facebook's real name policy requires that people can be identified with all content they post; because of this constraint, people may refrain from discussing sensitive topics [32]. German courts have ruled Facebook's policy illegal, finding that it surreptitiously allows Facebook to obtain users' consent to share their real names [33]. As they are currently constructed and governed, it has been argued that social platforms require vulnerable individuals to "perform" their identity according to norms that have been established by primarily white, privileged systems designers and policy makers or else risk opportunity loss [34]. In peer-production projects like open source software or Wikipedia, obscuring identity may be viewed by contributors as self-protection against opportunity loss, harassment, and threats of violence [35]. Moreover, many services require users to provide email or phone number for authentication and security. These policies are packaged as standard security measures but assume more is better to provide security and customer service. Indeed, the two-factor authentication adopted by major services like Google and Yahoo has been demonstrated to be hackable.

Additionally, government agencies can employ technologies that remove human decision-makers from social service administration, which has been shown to accelerate discriminatory practices [17]. Stereotypes about welfare recipients being "lazy" can be reinscribed in automated social welfare or healthcare systems that use failure to comply as signal of ineligibility in a way that increases the probability that welfare recipients will be rejected for beneficial services and subject to invasive visits by government officials and services [17]. For instance, Eubanks describes how a disabled girl loses Medicaid benefits for failing to cooperate in establishing eligibility—what amounts to a minor computer mistake—or how parents are flagged by social services for neglect because of an ignorant or vindictive neighbor or for failure to pay for medications: in other words, their crime was having a disabled child and being poor.

Other examples include the way in which technologies of surveillance, such as gang databases, re-encode perceptions of black and Latino young men as "deviant." That has consequences for arrests and sentencing but also affects the mindset of individuals who are criminalized [36]. Rios describes a system of ubiquitous punitive social control where family, schools, police, and prohibition systems interact to systematically criminalize marginalized youth in a way that shapes their worldview and identities [36]. Other literature also points to differences in how people engage with technologies along socioeconomic dimensions (e.g., [37, 38]). Ames and Burrell [39] found that even when trying to compensate for inequities in access to Internet technologies, individuals still face structural challenges stemming from socioeconomic circumstances, as well as bias because of their race and gender identities in their experience of technologies.

These same biases or stereotypes baked into algorithms can also undermine privacy design, for example, when low-income mothers are required to share irrelevant information about their sexual history and personal relationships as a requirement of receiving social services [16]. For example, Bridges describes how some states justify invasive questionnaires given to low-income mothers applying for benefits arguing that a history of drug abuse or domestic violence is a proxy for child neglect or abuse. Biases (including dirty policing and civil rights violations) make their way into invasive predictive policing technologies more often than not [40].

Pervasive surveillance technologies that rely on algorithms are required merely to take part in many aspects of society. Examples include systems that track individuals' online purchases [41, 42], social networks [2], job seekers [43], workplace [44, 45], and social services [2, 16, 17], and they inevitably disproportionately harm vulnerable and low-income populations.

The ways in which identities that are linked to race, sexuality, and socioeconomic status are often used to profile and punish and deny privacy rights are an insight that should lead us to consider the role that identities have in shaping vulnerable individuals' privacy needs and strategies. If we wish to develop technologies that do not exacerbate inequalities, it is critical to understand what kinds of unique privacy concerns vulnerable populations bring to their use of technology. In the next section, we will talk through some privacy concerns that can help orient technologists, policy makers, researchers, and designers to unique privacy vulnerabilities.

15.3 Who Is Vulnerable: Defining Unique Privacy Concerns

Section Highlights

- **The risks of emotional harm and physical violence loom large for LGBTQ individuals** even though the Internet has created new safe places for historically marginalized or stigmatized sexual identities.
- **Privacy is a challenge for domestic abuse victims and survivors** because it is easy for the target's partner to get access to their technology.
- **Being black and Hispanic is correlated with privacy vulnerabilities** and lack of trust in institutions that collect and store data.
- **A number of intersecting factors can compound the vulnerabilities** of already vulnerable groups.

There are many reasons why vulnerable individuals may require more privacy. In this section, we specifically consider examples related to sexuality, domestic abuse, and race that represent some of the most widespread experiences of vulnerability. Other vulnerabilities that are often adjacent include, but are not limited to, poverty, homelessness [46, 47], immigration [1, 6], stigmatized illnesses like HIV [8], and age—for instance, when it contributes to limited familiarity with scams or workplace technologies as discussed in Chap. 13. You will see that, in fact, in this section, discussions of race, ethnicity, and sexual identity (in particular) are inextricable with experiences of poverty and homelessness such that the research we cite inevitably (or unavoidably) captures those intersections. Notably, some of the most important research on privacy vulnerabilities sees poverty (in particular) and race as central [1, 2]. Privacy challenges for youth and aging populations are covered in Chapters 13 and 14.

15.3.1 Sexuality as Vulnerability

Gender identity and sexual orientation create vulnerabilities for individuals offline and online. For instance, simply being LGBTQ or female can cause individuals to seek more privacy or withdraw altogether [35, 48]. For their part, some social networks have become more inclusive when it comes to gender identification, with Facebook introducing over 50 gender options in 2014 [49] and Tinder allowing users to type in their own description of their gender identity [50]. But research has demonstrated that sexual orientation creates struggles of all kinds that require strict privacy management and even then still invite enhanced risks. That is, simply being more inclusive does not safeguard users against abuse and privacy risks. For this section, we focus primarily on LGBTQ as a vulnerability as they are often subject to the greatest harms. Other sexual preferences and gender identities exist that make people vulnerable but are not covered in this section.

LGTBQ populations are more likely to intersect with low-income populations, and these conditions of poverty are more often tied to experiences of discrimination in the workplace [51]. LGBTQ youths report overwhelmingly that they are not accepted in their community, and nine in ten experience negative messages about being LGBTQ but find that they can be more honest about themselves online (73%) [52]. For LGBTQ individuals, disclosure of sexual identity is carefully considered, and context collapse—when people from different social worlds interact, for example, when family meet friends—presents complex privacy challenges both online and offline [53].

Some research has looked at the disclosure strategies of LGBTQ young adults [10, 54] and parents [53]. Scheuerman et al. found that transgender individuals' experience of harm through social media is complex and multi-fronted arising as either targeted or incidental and both from insiders (those who are consider part of the "community") and from outsiders (those on the Internet who spread vitriol) [12]. According to Blackwell et al., LGBTQ parents worry about accidental disclosures to family, friends, and coworkers (some of whom are not even on these social networks but learn secondhand through those who are) [53]. LGBTQ parents feel both an obligation to be open about their lifestyle and an obligation to a collective social movement, to shoulder advocacy and the risk of their safety and privacy. On the one hand, broadcasting positive experiences, sharing adversity, and publicly "coming out" are all forms of advocacy—and part of an obligation to a politicized identity. On the other hand, in an environment where social views and values are in flux, "privacy stewardship" takes on greater urgency. LGBTQ parents worry that ever-shifting social views and dynamic networks leave them (and their children) susceptible to unforeseen future threats. As networks evolve, parents find themselves constantly on the lookout for "disapproval" within those social networks, and therefore, what constitutes a "safe space" online requires perpetual reassessment. Consequently, LGBTQ parents feel compelled to be both more private and more public than others.

Other studies have point to the risks faced by LGBTQ individuals that can lead to censorship online [55]. Notably, researchers in the Human-computer Interaction (HCI) and Computer-supported Cooperative Work (CSCW) community also point out that little research has focused on the specific harms transgender individuals (historically, some of the most vulnerable populations in the LGBTQ community) face online [12].

While the Internet has created new safe places for historically marginalized or stigmatized sexual identities, the risks of emotional harm and even violence loom large. Some HCI and CSCW researchers have argued that service providers consider accessibility of posts and user control [55]. According to Scheuerman et al., transgender individuals point to platforms like Twitter as examples of designs that do not take into account their needs, arguing that they allow for "trolling." They also point to the way that Facebook unwittingly (or not) can out individuals through its advertising (i.e., if others were to see their screen). While giving users greater control over their privacy settings is certainly critical, it is important that designers also not place burden on individuals to police others and safeguard themselves. Moreover, it is critical to understand these experiences from the perspective of these individuals since policies like those adopted by Twitter and Facebook (while perhaps well placed) have not offered sufficient protection from or remediation for harm.

15.3.2 Domestic Abuse as Vulnerability

One in four women and one in nine men have experienced intimate partner (physical) violence [56]. In addition to this intersection with gender, intimate partner violence may disproportionately affect LGBTQ individuals but has been somewhat little studied among this group [57]. Yet the ways in which this group has historically been underserved are most obviously in providing them with the protection they need as well as sensitivity to the nuanced issues that prevent women from seeking or finding help [58].

Domestic abuse victims and survivors represent challenging cases precisely because it is so easy for the target's partner to get access to their technology with little technological effort [4], which increasingly allows them to stalk and track. A high-profile example of design that failed to take into account potential vulnerabilities emerged in 2010 when Google introduced Buzz, a social network site that was intended to compete with Facebook. To overcome the critical mass problem of starting with an empty network, Google used frequent contacts from their other services like Gmail and chat to populate users' public list of connections. The practice of testing products only with Google employees rendered many vulnerable populations invisible in the process [59]. For example, one blogger noted that when she signed up, her abusive ex-husband suddenly had access to her location and recent online activity [60]. Users feared that contact with lawyers, doctors, psychologists, and other sensitive relationships might suddenly become public information.

Domestic abuse victims require specific technology training to ensure their physical safety [3–5]; however, designs like Buzz and the process that produced it exacerbate the problem. Google scholars note that despite the obvious life-threatening concerns, this particular group is not readily represented in technology design [5]. While domestic violence shelters have worked together with the anonymous browser, Tor, to provide victims with a reliable form of protection [3], more needs to be done to include the needs of the 10 million people in the United States who experience intimate partner violence each year [56].

15.3.3 Race as Vulnerability

Being black and Hispanic is correlated with privacy vulnerabilities and lack of trust among institutions that collect and store data and often intersects with being low income [1]. Indeed, race is at the intersection of so many central vulnerabilities that it can be hard to parse from any of those we explore in this section—and certainly with respect to amplified risk, which is why we later introduce intersectionality as such an important way of thinking about privacy. Even while the findings discussed in this section about minority populations and privacy intersect ineluctably with low socioeconomic status and other vulnerabilities, qualitative research that includes intersections of race, gender, and class/socioeconomics also seems to suggest that race alone can, for instance, impact online strategies for self-presentation and censorship [34].

Another intersection is race, crime, and socioeconomics. In their study of young people with low socioeconomic status, predominately of color, Marwick et al. (who even caveat "the pitfall of conflating race and class") find that marginalized social positions amplify risks online and contribute to avoidance of social media and self-censorship [61]. They make a parallel finding that youths of color with low socioeconomic status often experience structural racism in the form of policing and physical surveillance. Their study portrays these youth as well aware of the connection between Facebook posts and online or offline consequences (e.g., being doxed, bullied, or fired) but nevertheless prone to take the normative stance that they have “nothing to hide” [62, 63]. As a consequence, these youths self-censor or disengage altogether. Marwick et al. contrast this “individual responsibility,” which makes teens censor online, with the paradoxical experience (shared by these same young adults) of being exposed to police surveillance and brutality from which there is no escape. They are aware that they have everything to fear because privacy violations are inevitable. This framing, the authors argue, helps to circumvent the “victim-blaming narrative of some media literacy efforts” that have traditionally placed responsibility on individuals to secure their privacy [61]. We echo Marwick et al. in arguing that designers should not place so much burden on users to remedy their own privacy concerns.

Recent research has suggested that people of color and people from high-crime neighborhoods may be more worried than white or higher-income counterparts about police use of social media in crime prevention [64]. Underlying these concerns is a heightened sense of fear about the repercussions of violating social norms, the consequences of being perceived of as a snitch or of information getting into the wrong hands, and abuse of power.

Yet another intersection is race and gender. Pitcan et al. [34] found that to avoid opportunity loss, black women downplay sexuality and try to otherwise appear non-threatening to avoid white American stereotypes. In their findings, white and privileged class appear inextricable, suggesting that designers need to consider how their perspective-taking shapes their designs—in this case to mitigate risks of opportunity loss for women of color.

15.3.4 Intersections of Vulnerabilities

A number of intersecting factors can compound the vulnerabilities of already vulnerable groups. Those who are LGBTQ and black are also more likely to experience violence and encounter the highest incidence of fatal violence within the LGBTQ community [65]. Black children of same-sex couples are twice as likely as black children in heterosexual households to experience poverty and over four times as likely as white children of heterosexual households [65]. LGBTQ young adults are more likely to experience homelessness than their non-LGBTQ counterparts.[1] Homelessness presents a whole host of impediments to privacy (e.g., inability to find quarters that secure physical privacy, dependence on facilities for their access to services and info, and often that access is public and potentially less secure).

[1] Limitations on education and income, which themselves constitute vulnerability, are also major predictors of homelessness [66]. Poverty alone goes hand in hand with certain vulnerabilities, for example, greater reliance on mobile technologies.

While the privacy concerns and needs of an LGBTQ person or a person of color are not necessarily the same as, for instance, a victim of domestic abuse, the experience of more than one of these identities increases your chances of experiencing poverty, homelessness, discrimination, violence, and other inequalities.

In the face of a growing privacy literature that focuses on technology users who are young, privileged, white, and cisgender, some researchers have undertaken the task of examining the challenges for those who fall outside of those privileged categories. Instruments for measuring technology literacy (e.g., [67–69]) have been used to explore what kinds of knowledge are associated with privacy practices (e.g., [70, 71]), which can have huge implications for vulnerable communities [6]. But this perspective potentially overlooks the way in which structural inequalities and experience conspire to make privacy threats and practices fundamentally different, not better or worse. For instance, living in poverty can amplify the consequences of a privacy violation; if, for example, a potential employer can find embarrassing (or simply unedited) information about a job seeker, the economic impact of opportunity loss may have devastating consequences for someone who is just getting by. The severity of the threat emanates not from a limited set of skills but from the condition of poverty associated with these identities. To come at privacy with a literacy framing is to suggest that if only users who are vulnerable had better skills, they would be fine, but the real difference is that privacy violations impact vulnerable groups in qualitatively different ways.

Consider the user who experiences or hears of a privacy scam that results in a loss of $4000 [71]. For someone living below the poverty line, that could be nearly half of their income. Perhaps it goes without saying that anything you do to mitigate against that threat will far surpass the type of activities we assign to the "digitally literate." These are potentially life-altering events that might leave fearful of ever using the Internet again. Measuring the effects of these events with "digital literacy" as a tool misses critical motivations and user experiences.

The experiences of those who are subject to surveillance and privacy threats on a daily basis because of their race and class can serve as a starting point for reframing privacy in ways that relieve victims of responsibility for privacy violations [61]. Instead of blaming people for the way they use limited privacy toolkits and for their reliance on shared infrastructures that mimic other oppressive systems, a growing narrative in the research literature suggests that infrastructures and services can be designed to better serve the needs of vulnerable groups. Thinking out of the box, could service providers offer insurance or compensation for users abused on their platform? The idea is not so radical given that other vendors are responsible for user experience.

15.4 Privacy, the Self and Social Norms

Section Highlights

- **Individualistic privacy theories, which focus on how people regulate information about themselves**, give way to normative approaches, ways of thinking about shared privacy expectations.
- **However, norm-based approaches overlook the increasingly ubiquitously networked environments in which we live,** in which boundaries are permeable and overlapping, and the way in which normative frames fail to meet the needs of individuals who reside outside the norm.
- **We challenge the view that privacy vulnerabilities are the result of lack of literacy** so much as sense of loss of agency and overwhelming exposure to less expensive and, by extension, vulnerable technologies, scams, predatory marketing, and exploitative sites [2].
- **Privacy threats are highly idiosyncratic**, suggesting that frameworks for addressing privacy problems should be sensitive to the stigma of vulnerable identities as well as the intersectional circumstances of individuals.

As discussed in Chap. 2 of this book, interpersonal boundary regulation [72, 73] lays a foundation for individualistic privacy theories that focus on understanding how people regulate information about the self, with an emphasis on personal exploration and self-presentation. For instance, Altman's framework of interpersonal boundary regulation characterizes privacy in an analog, pre-Internet world [72]. Taking ownership of privacy as an individual becomes more complicated as we consider the move to mediated interactions and as online systems become more complex, interconnected, and extensible [73]. Scholars have found that tending boundaries is part of everyday online practice [74], but that these strategies are complex and unique to the individual [75–80]. There is an inherent tension between the concerns of individuals seeking to protect their personal information (e.g., in order to safely self-disclose or participate in online spaces without fear of harassment) and the degree to which online platforms appear willing or able to afford those protections, leading to potential constraints on participation and self-censorship.

Approaches that emphasize social norms as a way of understanding privacy expectations are challenged by the permeable overlapping nature of online spaces. Yao explains that "in the physical world, for example, observable objects and symbols usually mark the boundaries between private and public domains, and the size of personal space can be neared in units of distance. ... in the virtual online world, the concept of 'space' is merely a metaphor ... To make things more complicated, people from different cultures, often with drastically different privacy beliefs and norms, co-occupy this abstract and metaphorical space. In such a virtual environment, the normative rules and expectations related to personal privacy are irrelevant" (p. 114) [81]. Even when privacy norms in online environments become established, they cannot take into account the values (or realities) of all individuals who inhabit them.

The difficulty of using traditional physical analogies, social norms, and common approaches like threat modeling to inform thinking about privacy for people with heightened risk is evident in the ways that technologies fail to meet the needs of vulnerable populations. For example, intimate partner violence (IPV) defies typical threat models because abusers often have access to victims' phones and can carry out injurious, albeit unsophisticated, attacks by directly accessing their devices and information, rather than through installing malicious software [4]. The challenges for IPV victims provide an analogy to the broader problems for privacy and security faced by experts: *Privacy threats are highly idiosyncratic, and as a result, so too are the specific mitigation strategies that individuals at risk must employ to counter them.* Mitigation strategies must, therefore, take account of not only the stigma or vulnerability that creates the need for heightened privacy but also other aspects of their individual circumstances, including their personal history, needs, and use of technology.

15.4.1 How Existing Privacy Frameworks Are Inadequate

The challenge of adapting a general theory of privacy in the face of rapidly changing networked information technologies gives way to new group and communitarian perspectives. For example, Lampinen et al. shift attention to the idea that boundaries are regulated as part of a group process [82–84]. Group perspectives allow participation in popular networked communities to be conceptualized as a trade-off between aspirations of personal privacy and benefits of social or participatory optimization. For example, to avoid tensions between different groups, individuals might divide the platform into separate spaces, creating private groups for some interactions. People might also self-censor or choose other channels (private or elsewhere) if they perceive a communication might be problematic.

As discussed extensively in Chap. 2, contextual integrity, an approach to thinking about privacy introduced by Helen Nissenbaum, describes privacy as a function of the social expectations of a given context, pushing beyond individual privacy to privacy as a function of norms in distinct situations [85]. Contextual integrity expands privacy theories to account for contexts in which social expectations dictate privacy violations, how information should flow, and who should have access to it. For example, Nissenbaum uses the example of healthcare environments, in which a healthcare provider may appropriately inquire about a patients' sexual behavior while that same inquiry would not be acceptable directed to the provider by the patient. Contextual integrity treats social norms as expectations of what people ought to do or what is socially appropriate to do, in contrast with a descriptive definition of norms, which are what people typically do.

Still, others point out that the two ideas (privacy and social participation) need not be positioned as alternative values if precautions are taken on an individual level. For example, when social network sites tailor privacy to fit the specific needs of individual users, they feel more socially connected [86]. This is reassuring news.

There are aspects of our identity that might stigmatize or cause users to self-censor or even abandon social networks [87, 88], and we might not be taking account of them and thus designing for them. Interestingly, scholars have argued for the queering of communitarian theories to account for unique (and radical individual identity) while also supporting local norms [89]. In our final section, we hope to resolve this tension between individual and group or communitarian needs.

What all these theories or research frameworks have in common is that they do not provide tools for considering vulnerabilities, for example, class- and race-based struggles. We are primarily concerned with theories and frameworks that directly address the privacy concerns reported by vulnerable individuals (e.g., non-white [90] and LGBTQ [91, 92]) whose vulnerability to online harassment has been documented. Only then can we design platforms that are hospitable to vulnerable individuals. We believe that frameworks that rely on social norms (e.g., that I have nothing to fear by giving up my identity to strangers) fall short because prevailing social norms assume that, for instance, one's identity does not make them the target for privacy violations that lead to threats and opportunity loss [93]. Recently scholars have questioned whether indeed frameworks based on norms about consumer pragmatism (like those introduced by Westin [94]) should not be reevaluated as stemming from vulnerabilities (particularly, socioeconomic vulnerabilities) which leads them to "misunderstand the scope of data collection and falsely believe that relevant privacy rights are enshrined in privacy policies and guaranteed by law" [95]. We hypothesize, however, that these vulnerabilities are not so much about literacies as sense of agency and overwhelming exposure to less expensive and, by extension, vulnerable technologies, scams, predatory marketing, and exploitative sites [2]. We readily give up identity information when applying for jobs and social services or simply picking up drugs at the pharmacy. As low-income, marginalized Americans, many of these activities may be more likely to take place over less secure WiFi and devices, the consequences of which are enhanced risk of privacy violations or avoidance of financial and social institutions altogether [41].

To usefully augment these theories, designers and researchers must consciously consider the experiences of those whose privacy concerns may not be captured by the prevailing "norms." Media scholar Mike Yao talks about how the invention of printing technology made it easy to disperse private information and how, later, electronic devices increased efficiency and speed of information sharing [81]. Each of these innovations required a remapping of human boundaries and a reconceptualization of personal privacy. Until now, privacy has been broadly situated as tool of withdrawal from the public eye. Yet, Yao argues, online privacy is not a normative or legal concept, but a personal, socio-technical strategy. Up until now, shifts in privacy have assumed a shift in boundaries (which could be intellectual and abstract or physical), but no such terrain exists on the Internet. The lack of legal safeguards and also the permeable, ever-changing barriers of the Internet present challenges for demarcating spheres according to old precepts having to do with physical spaces and abstractions and almost always assume boundaries to exist and be identifiable. To define a legal or technical terrain of privacy, Yao argues, would be "relatively easy," but the problem is that there is no cultural consensus, even in the United States, the constitution does not unambiguously guarantee the right to privacy.

15.5 Better Frameworks for Vulnerable Populations

Section Highlights

- **Feminist theories and queer Marxist theories** offer a useful lens through which to consider marginalized perspectives.
- **Intersectionality helps us understand marginalized identities and the ways in which they overlap to compound unique vulnerabilities in relation to systems of oppression.** It is understanding these unique relationships that, we argue, will open up designers to new ways of thinking about privacy needs for vulnerable populations.
- **Recent scholarship is increasingly drawing on feminist intersectional lenses to tackle design problems.**

In the prior section, we talked about how thinking in terms of social norms can fail to illuminate inequalities embedded in design and privacy policy. In this section, we explain how theories that specifically take up identity are critical additions to our understanding of privacy. Feminist intersectional theory is an important lens through which to consider privacy design because it focuses on identity and structures of power—the intersection of different identities and their experience of institutions that we described in Sect. 15.3. Often those experiences coincide with conditions brought on by social norms of discrimination, and these scenarios may be challenging for designers and technologists to understand and grapple with. If designers and technologists cannot imagine vulnerable users and do not seek them out during requirements gathering, then they will be left out of design and policy. We argue that designers of systems should think in terms of marginalized identities to shape (or, at very least, inform) research and decision-making.

Feminism has long been concerned with privacy [96, 97], starting with an interest in the States' role in the family and violence within the home. Recent Marxist feminist work has observed that capitalism imposes norms on counter-normative sexual identities, making them feel welcome only within a monitored sphere [98]. We see this echoed in the way that, for instance, social networks have increasingly spoken out against hate speech and bullying by portraying the victim as powerless to defend themselves while at the same time calling on the community to defend (weaker) others against attack. This kind of sanctioned, socially constructed peace-keeping does not prompt better privacy or identity protections or tools; rather it asks the community to help regulate and reform those who would openly ridicule someone. Put another way, by focusing only on monitoring, this approach side-steps design and policy-making that might protect these users at the outset.

Though feminist theories (especially those combined with queer or Marxist thought) are helpful in revealing these design tensions, intersectional theory expands the single-issue, marginalized perspective represented by feminist theories [99] to account for simultaneous identities that may not simply be additive but multiplicative in relation to systems of discrimination. Kimberle Crenshaw is credited with first introducing intersectional theory as a black feminist critique of antidiscrimination doctrine and feminist theory [100]. Crenshaw describes the social hierarchies of inequality (of the vulnerable) by describing individuals who stand on each other's shoulders, feet stacked in a deep basement. In this metaphor, Crenshaw asks us to imagine "a basement which contains all people who are disadvantaged on the basis of race, sex, class, sexual preference, age and/or physical ability. These people are stacked—feet standing on shoulders—with those on the bottom being disadvantaged by the full array of factors, up to the very top, where the heads of all those disadvantaged by a singular factor brush up against the ceiling. Their ceiling is actually the floor above which only those who are *not* disadvantaged in any way reside" [100]. This metaphor renders intersectionality as consideration for the multiplicity of vulnerabilities within the context of structures of inequality.

It is important to remember that how we investigate people's privacy concerns should take into account the defining context for intersectional identities. Taking an intersectional lens requires that we appreciate the way in which the deck can be stacked against individuals down to the basement floor and that it gets *uniquely* worse the further down you go. We propose that intersectional frameworks are often needed to address the complex layering of vulnerabilities and their consequences—for instance, the implications of being a black trans woman as opposed to just black [101]—in order to fully comprehend the nature and magnitude of risk and identify ways to mitigate risk through improved design [12].

Identity vulnerabilities and their historical relationship to policy-making are something to consider when contemplating the stakes involved with user identity information. An intersectional perspective allows us to see how multiple vulnerabilities can create heightened risks and also how policies have historically not been calibrated to address these risks—that is, exposing deeply embedded structural inequalities. In a way, it seems simple: only design that is grounded in lived political and social experience can serve the real-world needs and privacy threats faced by individuals. It is important to note that both feminist and intersectional inquiries (especially) are equipped with a critical lens that is focused on social change, power and economic structures, and empowerment and may disavow concepts that seem to perpetuate injustices the research is looking to overcome [102]. For example, feminist researchers seeking to challenge hegemonic categories of available knowledge and to privilege marginal perspectives have permission to discard traditional frameworks [103, 104]. The researchers' goal is thus to work through experience and perception and privilege the users' perspective.

Shaowen Bardzell introduces feminist design criteria that are committed to "agency, fulfillment, identity and the self, equity, empowerment, diversity, and social justice" [105]. Bardzell identifies a number of studies that integrated gender perspectives in the study of design and highlighted opportunities to draw on feminism in design research. In particular, Bardzell argues that homes are often dominated by gender norms and that "feminist approaches can bring clarity to the way that subjectivity and experience with technology are gendered" [105]. She argues further that feminism could support inquiries into practical technology requirements while also avoiding pitfalls that propagate marginalization of women or any other group. Feminism does this through critique of dominant epistemologies, elevation of those on the margins, critical stance toward local norms, and the user identity as being prescribed by gender and other dominant norms.

Intersectional frames (maybe by contrast) invite new analytical approaches in their quest to challenge the systems that reproduce inequality [102]. Yet Schlesinger et al. find that as of 2016, identity-focused research tends only to look at one facet of identity [106] as opposed to considering where overlaps create additional vectors of vulnerabilities *and how.* What we learn from intersectional scholar Patricia Collins is that what counts as intersectionality is far from settled [102].

Recent scholarship has drawn on intersectional theories to support new ways of thinking about research and design. Blackwell et al. [107] argued for the relevance of feminist intersectional theory in thinking about HeartMob, a platform where victims of harassment can describe their experience by submitting a harassment case and then request help from volunteers. Finding that users might perceive themselves as "outsiders" because their experiences do not fit within typical categories, they contend that to fully address online harassment, platforms must consider the needs of marginalized users into the design (e.g., classification systems) and moderation policies of platforms.

15.6 Actionable Guidelines

Section Highlights

- **Designers should consider, at minimum, what kind of identity policy is reasonable for their services and what kind of vulnerable communities are part of their requirements gathering and design phases.**
- **Additionally, designers might consider how these identities might be harmed by their services and what obvious technical solutions might mitigate these harms.** Also, are there channels for experiences to be voiced? Are there opportunities to incorporate those voices into design—even after product launch?
- **Are there ways that identities intersect to create added and more complex burdens?** What are the burdens and risks and how can they be addressed?

So how can intersectional design thinking be accomplished? We see a few places to start. First, we recommend that designers actively develop personas of vulnerable users with associated key information flows and risks. Personas are a description of a fictional person that are a composite of attributes of a user segment either based on assumptions or data [108]. At minimum, we encourage designers to build personas to guide design.

We have also discussed in Sect. 15.2 the way in which technologies tend to exacerbate existing (offline) inequalities that harm vulnerable users in disproportionate ways. At minimum, we suggest designers consider the following:

- What kind of identity policy is reasonable and required for the services you offer? What are the trade-offs between anonymity, pseudonymity, and real names for users of your system?
- What vulnerable communities are you including in your requirements gathering and design explorations (e.g., minorities, LGBTQ, etc.)?

In Sect. 15.3, we talk about specific vulnerabilities and intersections and invite service providers and designers to consider how the harms potentially outweigh the benefits of "real-name" policies, when user pseudonyms connected to user histories would suffice. More broadly, we ask that designers and policy makers consider the trade-offs whenever they introduce solutions for one vulnerable population that may harm or overlook another. One way to do this may be to keep vulnerable communities engaged in the process in a way that creates a potential channel for outreach as problems arise. Further, we encourage those seeking to design systems for diverse communities to go a step further and consider the following when designing their research:

- What communities are included among your end users and who are most vulnerable? How might these vulnerable users potentially be harmed by data (e.g., "real name") policies and what are the trade-offs and possible workarounds?
- Whose voices are you hearing and whose voices are getting left out of policy and norm articulation process? Are you considering obvious technical solutions that serve your bottom line (knowing about, customizing for, creating history of, while empowering) … your user?
- How does your design process and outreach create comfortable opportunities for divergent opinions and experiences to be voiced? … When you incorporate these voices, are you giving them ample opportunity to follow design scenarios to their logical conclusion?

We have described the importance of considering the array of end users and, in particular, asking what voices have, in the past, been left out of technology and policy decisions, what the means for current design norms, and what (minimally disruptive) technical solutions might solve the problem. An important and critical step to overcoming this challenge is having designers consider or talk with users who are vulnerable and thus face privacy challenges. Another easy and obvious place to start would be to involve those with vulnerable demographics in the design process, both hiring them as designers and interviewing them as potential users. We advocate for caution, however, as this risks what queer theorist Holly Lewis describes as "tokenism" whereby "minor changes within the composition of the group … short-circuit the possibility of" changing the way the group interacts or solves problems (p. 68 [89]).

In Sects. 15.4 and 15.5, we talk about the inadequacy of existing frameworks and the importance of considering how identity and structures of discrimination can compound vulnerabilities. While the above questions are aimed at a more intersectional approach to design thinking, we recommend that designers and technologists also consider the following:

- What are some of the ways the identities that intersect create added burdens for users of your system? For example, it may be common practice to ensure that women are represented in design processes, but are there specific concerns from women of color, trans women, women who are living in poverty, who have survived domestic abuse, or all of the above?
- What risks does your technology introduce for people with intersectional identities?

15.6.1 A Thought Experiment

Section Highlights

- **Our thought experiment about a ride-sharing service highlights the way in which identity raises the stakes for those using services** and about the information flows that services may take for granted, especially when what works for one individual potentially harms another.
- **Intersectionality allows designers to think about facets of identity in relation to risks** created by local norms and institutions.

To help designers think through some of these questions, we developed a thought experiment using a hypothetical ride-sharing service. We chose this example because this is a technology that is not only becoming mainstream and ubiquitous, the use of location-based and identity information that has become central to these services presents obvious and not so obvious (as we will see) privacy challenges.

> **Ride sharing scenario:** Consider that you are designing a ride-share service app with a carpool feature. What information would you collect and display about users? Would you share their name with other riders? Their destination? Their Spotify playlist? All of these pieces of identity information are available on ride-sharing app, and the first two are readily shared. None of these are pieces of information that were part of the standard hailing cab services of yore, yet they have become the norm. Contextual norms dictate that we give up or confirm our name to our driver through their window, or as soon as we get in the car—much like how we used to tell a cab service where we were going at those two junctures. This is how, without a hailing signal or a yellow-checkered cab, we make sure we do not pick up the wrong person or step into the wrong vehicle. Yet when you share a ride, who has access to this information spreads and norm-based theories cannot sufficiently interrogate these seemingly benign incursions—or these shift-shaping norms.

We have been conditioned to think that our legal identities somehow make our interactions more authentic. Is there any social value in requiring real names for use of a ride-share service? When hailing a cab, was it customary to give one's name to the driver? Authentication could be separated from name identity information. What are the trade-offs of such an approach?

Further complicating this assessment is the recent murder of a student by a person posing as a Uber driver that spawned the hashtag campaign #WhatsMyName [109]. The idea behind this campaign is to encourage ride-sharing users to immediately asked drivers, “What’s my name?” Although this does not specify other riders, it does swing the pendulum in the other direction where the use of name identity information is essential for safety. These types of trade-offs introduced by this incident must be part of the ongoing design and policy-making process.

Identity and experience play a huge role in driving privacy strategies [110] and in ways that are potentially at odds. For some, giving your name might be a matter of life or death; for others, the opposite might be true [111]. What is important is that we gather these perspectives and be aware of the implications for the kinds of nuanced control people need over their identity knowledge [112] even if that means that one solution for a certain group might be in opposition to another.

Consider a rider who is not just female but who has multiple vulnerabilities. How does that raise the stakes for ensuring that end user identity links were sufficiently anonymous? For example, in addition to obscuring name information, should this ride-share company provide a set of tools for riders to get picked up and dropped off near but not at their destination? The normative frame is that riders want the convenience of door-to-door service and are annoyed when they are not picked up and dropped off at the exact address. Ride-share companies do offer pick-ups and drop-offs to nearby locations, but this is for the incentive to save time and money; it is not an advertised safety feature. The designers likely did not anticipate that offering nearby location pick-up and drop-off service could potentially be a safer alternative; rather, they thought of it as a cost savings. Intersectionality allows us to think about facets of identity in relationship to risks created by local norms and institutions.

15.6.2 Reimagining Privacy for Inclusivity

Section Highlights

- **We argue for design of systems that not only provide ways to report harm but strive *not* to enable it.**
- **Intersectional identities introduce unique avenues for harm and thus require unique solutions.** The ride-sharing thought experiment usefully describes a situation where mitigating harm for one group enhances it for another and solving one problem potentially benefits a whole category of vulnerable users. These nuances present privacy design challenges, but they are surmountable.
- **We are all at risk of being the privacy “underclass”** [113]. But the privacy needs of vulnerable populations are nevertheless highly nuanced and require careful, individual attention to ensure they are addressed.
- **It is hard to know what challenges one will uncover until they use the system. We suggest designers start, however, by asking:** What are some examples of vulnerable people who may be interested in using your product, and how can you

engage them in systems design from requirements gathering to implementation and testing? How can you leave open channels for vulnerable individuals to voice their concerns as they arise?

There is ample opportunity for designers to reimagine spaces [114]. Some have suggested that designers better understand bad actors as a way of mitigating abuse and that cisgender, privileged individuals stick up for their vulnerable counterparts. In fact, addressing the abuse post hoc cannot be the only answer. We must design systems that strive to *not* enable harm (and certainly not amplify it). This requires that we radically rethink representation on social media as well as forms of participation that support different kinds of anonymity and ephemerality [30].

What the ride-sharing example illustrates is that sometimes the solution for one group is not appropriate for another. It is important that platform designers consider what tools users need to have to make sure they can make informed decisions that support their privacy goals and adequately protect them against privacy threats with research, design, and policy.

If certain classes of contributors are being excluded, or if their concerns are superseded by the concerns of a less vulnerable class of contributor, then the experiences of people with vulnerable or marginalized identities may be systematically excluded from the development of community norms and effectively rendered "invisible" on the Internet. As we come to terms with the darker implications of "surveillance capitalism" [113, 115], we might imagine that threats are also more opaque and harder to define as simply a bully, a perpetrator of hate, or an abusive domestic partner. If Shoshana Zuboff is, in fact, correct that all "users" are all the underclass (the property of tech companies), then fighting for the privacy of the most vulnerable becomes urgent for all [113]. This sets off a new "axis of inequality" which, Zuboff argues, puts at risk not just the overtly vulnerable but those not formally perceived as such. The privacy needs of vulnerable populations are nevertheless highly nuanced and require careful, individual attention to ensure they are addressed.

Privacy is the ultimate negative right. It is the right *not to* be exposed to public scrutiny, to *limit* incursions of the state or attempts of others to know what an individual is doing. There is no easy syllogism between privacy and democracy or freedom; that makes it challenging to understanding privacy. There is no universal definition of privacy. Privacy is culturally and individually defined and therefore not universally valued; nor are violations and consequences of those violations perceived or experienced by all individuals in the same way. In a society where access to technology and information requires all of us to relinquish some privacy, we must understand that the terms and conditions of that loss are inherently unequal and the consequences especially grave for some. Technology gatekeepers need to play a critical role in extending protections to those most vulnerable, guided by an empathetic and well-informed perspective on what protections are required.

There are simple steps that technologists can take to begin hearing vulnerable voices and including them in design and research. We suggest that designers ask themselves the questions we have outlined, considering broadly the way that certain design trade-offs can harm vulnerable users and also thinking more specifically about what communities are impacted by the design of specific technologies. For instance, what are some examples of vulnerable people who may be interested in using your product, and how can you engage them in systems design from requirements gathering to implementation and testing? Moreover, it is essential that designers leave open channels for vulnerable individuals to voice their concerns as they arise. It is hard to know what challenges one will uncover until they use the system. In addition to involving target vulnerable groups in prototyping and testing, they should be targeted sources of feedback for new products as they enter the market—and existing ones.

Acknowledgments This work was supported in part by the National Science Foundation grant CNS-1703736.

References

1. Madden, M. 2017. *Privacy, Security, and Digital Inequality*.
2. Madden, M., M. Gilman, K. Levy, and A. Marwick. 2017. Privacy, poverty, and big data: a matrix of vulnerabilities for poor Americans. *Washington University Law Review* 95 (1): 053–125.
3. Domestic Abuse Survivors Go "Underground" With the Tor Network. 2014. http://www.adweek.com/digital/domestic-abuse-survivors-go-underground-tor-network/. Accessed 31 Aug 2017.
4. Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T. and Dell, N. 2018. A Stalker's paradise: how intimate partner abusers exploit technology. pp 1–13.
5. Matthews, T., K. O'Leary, A. Turner, M. Sleeper, J.P. Woelfer, M. Shelton, C. Manthorne, E.F. Churchill, and S. Consolvo. 2017. Stories from survivors: Privacy & Security Practices when coping with intimate partner abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2189–2201. New York, NY: CHI.
6. Guberek, T., A. McDonald, S. Simioni, A.H. Mhaidli, K. Toyama, and F. Schaub. 2018. Keeping a low profile? Technology, risk and privacy among undocumented immigrants. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 114:1–114:15. New York, NY: CHI.
7. Tufekci, Z. 2017. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. New Haven: Yale University Press.
8. Warner, M., Gutmann, A., Sasse, M.A., and Blandford, A. 2018. Privacy unraveling around explicit HIV status disclosure fields in the online Geosocial hookup app Grindr. *Proceedings ACM Human-Computing Interact* 2, CSCW (Nov. 2018), 181:1–181:22. https://doi.org/10.1145/3274450.
9. Blackwell, L., J. Hardy, T. Ammari, T. Veinot, C. Lampe, and S. Schoenebeck. 2016. LGBT parents and social media: Advocacy, privacy, and disclosure during shifting social movements. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 610–622. New York, NY: CHI.
10. Gray, M.L. 2009. *Out in the Country: Youth, Media, and Queer Visibility in Rural America*. New York: NYU Press.
11. Kitzie, V. 2019. "That looks like me or something i can do": Affordances and constraints in the online identity work of US LGBTQ+ millennials. *Journal of the Association for Information Science and Technology*. https://doi.org/10.1002/asi.24217.

12. Scheuerman, M.K., S.M. Branham, and F. Hamidi. 2018. Safe spaces and safe places: Unpacking technology-mediated experiences of safety and harm with transgender people. *Proceedings ACM Human-Computing Interact.* 2, CSCW (Nov. 2018), 155:1–155:27. https://doi.org/10.1145/3274424.
13. Anjum, B. 2018, December. An interview with Pamela Wisniewski: Making the online world safer for our youth. *Ubiquity* 2018: 2:1–2:6. https://doi.org/10.1145/3301323.
14. Wisniewski, P., A.K. Ghosh, H. Xu, M.B. Rosson, and J.M. Carroll. 2017. Parental control vs. teen self-regulation: Is there a middle ground for Mobile online safety? In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, 51–69. New York, NY: ACM.
15. Hornung, D., C. Müller, I. Shklovski, T. Jakobi, and V. Wulf. 2017. Navigating relationships and boundaries: Concerns around ICT-uptake for elderly people. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing System*, 7057–7069. New York, NY: CHI.
16. Bridges, K.M. 2017. *The Poverty of Privacy Rights*. Stanford, CA: Stanford Law Books.
17. Eubanks, V. 2018. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: St. Martin's Press.
18. Ferguson, A.G. 2017. *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: NYU Press.
19. Noble, S.U. 2018. *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: NYU Press.
20. Andalibi, N., O.L. Haimson, M. De Choudhury, and A. Forte. 2016. Understanding social media disclosures of sexual abuse through the lenses of support seeking and anonymity. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 3906–3918. New York, NY: CHI.
21. Joinson, A. 2001, March. Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. *European Journal of Social Psychology* 31 (2): 177–192. https://doi.org/10.1002/ejsp.36.
22. Ma, X., J. Hancock, and M. Naaman. 2016. Anonymity, intimacy and self-disclosure in social media. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 3857–3869. New York, NY: CHI.
23. McKenna, K. and Bargh, J. 1998. Coming out in the age of the internet: Identity demarginalization through virtual group participation Journal of Personality and Social Psychology 75 (3): 681–694.
24. Pavalanathan, U., and M. De Choudhury. 2015. Identity management and mental health discourse in social media. In *Proceedings of the 24th International Conference on World Wide Web*, New York, NY, 315–321.
25. Schrading, N., Alm, C.O., Ptucha, R., and Homan, C.M. 2015. An analysis of domestic abuse discourse on Reddit. *Conference on Empirical Methods in Natural Language Processing*.
26. Ellison, N., L. Blackwell, C. Lampe, and P. Trieu. 2016, November. "The question exists, but you Don't exist with it": Strategic anonymity in the social lives of adolescents. *Social Media + Society* 2 (4): 2056305116670673. https://doi.org/10.1177/2056305116670673.
27. Pennebaker, J.W., and C.K. Chung. 2007. Expressive writing, emotional upheavals, and health. In *Foundations of Health Psychology*, 263–284. New York: Oxford University Press.
28. Pennebaker, J.W., J.K. Kiecolt-Glaser, and R. Glaser. 1988. Disclosure of traumas and immune function: health implications for psychotherapy. *Journal of Consulting and Clinical Psychology* 56 (2): 239–245.
29. Smyth, J.M. 1998. Written emotional expression: Effect sizes, outcome, types, and moderating variables. *Journal of Consulting and Clinical Psychology.* 66 (1998): 174–184.
30. Xu, B., P. Chang, C.L. Welker, N.N. Bazarova, and D. Cosley. 2016. Automatic archiving versus default deletion: What snapchat tells us about ephemerality in design. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, 1662–1675. New York, NY: ACM.
31. Sharing to the power of 2012. *The Economist*.

32. Facebook is playing games with your privacy and there's nothing you can do about it. https://www.forbes.com/sites/thomasbrewster/2016/06/29/facebook-location-tracking-friend-games/. Accessed 18 Apr 2019.
33. German court says Facebook's real name policy is illegal. 2018. https://www.theverge.com/2018/2/12/17005746/facebook-real-name-policy-illegal-german-court-rules. Accessed 18 Apr 2019.
34. Pitcan, M., A.E. Marwick, and D. Boyd. 2018, May. Performing a vanilla self: Respectability politics, social class, and the digital world. *Journal of Computer-Mediated Communication* 23 (3): 163–179. https://doi.org/10.1093/jcmc/zmy008.
35. Forte, A., N. Andalibi, and R. Greenstadt. 2017. Privacy, anonymity, and perceived risk in open collaboration: A study of Tor users and Wikipedians. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, 1800–1811. New York, NY: ACM.
36. Rios, VM. 2011. *Punished: Policing the Lives of Black and Latino Boys (New Perspectives in Crime, Deviance, and Law) – Kindle Edition by Victor M. Rios. Politics & Social Sciences Kindle eBooks* @Amazon.com. New York: NYU Press.
37. Ames, M.G., J. Go, J.J. Kaye, and M. Spasojevic. 2011. Understanding technology choices and values through social class. In *Proceedings of the ACM 2011 Conference on Computer Supported Cooperative Work*, 55–64. New York, NY: ACM.
38. Yardi, S., and A. Bruckman. 2012. Income, race, and class: Exploring socioeconomic differences in family technology use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 3041–3050. New York, NY: SIGCHI.
39. Ames, M.G., and J. Burrell. 2017. "Connected learning" and the equity agenda: A microsociology of Minecraft play. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, 446–457. New York, NY: ACM.
40. Richardson, R., Schultz, J., and Crawford, K. 2019. Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. *New York University Law Review Online*.
41. Lanier, J. 2014. *Who Owns the Future?* New York: Simon & Schuster.
42. Newman, N. 2014. The costs of lost privacy: Consumer harm and rising economic inequality in the age of Google. *William Mitchell Law Review* 40: 2.
43. Mann, G., and C. O'Neil. 2016. *Hiring Algorithms Are not Neutral*. Brighton: Harvard Business Review.
44. Guendelsberger, E. 2019. *On the Clock: What Low-Wage Work Did to Me and How It Drives America Insane*. New York, NY: Little, Brown and Company
45. Rosenblat, A., T. Kneese, and D. Boyd. 2014. Workplace Surveillance. Data & Society Working Paper, p. 19.
46. Le Dantec, C.A., and W.K. Edwards. 2008. The view from the trenches: Organization, power, and Technology at two Nonprofit Homeless Outreach Centers. In *Proceedings of the 2008 ACM Conference on Computer Supported Cooperative Work*, 589–598. New York, NY: ACM.
47. Le Dantec, C.A., R.G. Farrell, J.E. Christensen, M. Bailey, J.B. Ellis, W.A. Kellogg, and W.K. Edwards. 2011. Publics in practice: Ubiquitous computing at a shelter for homeless mothers. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1687–1696. New York, NY: SIGCHI.
48. Menking, A., and I. Erickson. 2015. The heart work of Wikipedia: Gendered, emotional labor in the World's largest online encyclopedia. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 207–210. New York, NY: ACM.
49. Changing Your Gender on Facebook is Easy. https://www.lifewire.com/edit-gender-identity-status-on-facebook-2654421. Accessed 02 Aug 2019.
50. Introducing More Genders on Tinder. 2016. https://blog.gotinder.com/genders/. Accessed 02 Aug 2019.
51. Lesbian, Gay. Bisexual and transgender persons & socioeconomic status. https://www.apa.org/pi/ses/resources/publications/lgbt. Accessed 29 July 2019.

52. Growing up LGBT in America: View and share statistics. http://www.hrc.org/youth-report/view-and-share-statistics/. Accessed 27 Feb 2019.
53. Blackwell, L., J. Hardy, T. Ammari, T. Veinot, C. Lampe, and S. Schoenebeck. 2016. LGBT parents and social media: Advocacy, privacy, and disclosure during shifting social movements. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 610–622. New York, NY: CHI.
54. Duguay, S. 2016, June. "He has a way gayer Facebook than I do": Investigating sexual identity disclosure and context collapse on a social networking site. *New Media & Society* 18 (6): 891–907. https://doi.org/10.1177/1461444814549930.
55. Dym, B., and C. Fiesler. 2018. Vulnerable and online: Fandom's case for stronger privacy norms and tools. In *Companion of the 2018 ACM Conference on Computer Supported Cooperative Work and Social Computing*, 329–332. New York, NY: ACM.
56. NCADV | National Coalition Against Domestic Violence. https://ncadv.org/statistics. Accessed 18 Apr 2019.
57. NCADV | National Coalition Against Domestic Violence: https://ncadv.org/blog/posts/domestic-violence-and-the-lgbtq-community. Accessed 29 July 2019.
58. Crenshaw, K. 1991. Mapping the margins: Intersectionality, identity politics, and violence against women of color. *Stanford Law Review* 43 (6): 1241–1299. https://doi.org/10.2307/1229039.
59. Google Buzz Privacy Update. 2010. https://www.eff.org/deeplinks/2010/02/google-buzz-privacy-update. Accessed 25 Apr 2019.
60. Google Buzz privacy issues have real life implications. *TechCrunch*.
61. Marwick, A., C. Fontaine, and Danah Boyd. 2017, April. "Nobody sees it, nobody gets mad": Social media, privacy, and personal responsibility among low-SES youth. *Social Media + Society* 3: 2. https://doi.org/10.1177/2056305117710455.
62. Conti, G., and Sobiesk, E. 2007. An honest man has nothing to fear: User perceptions on web-based information disclosure. In *Proceedings of the 3rd Symposium on Usable Privacy and Security* (New York, NY, USA, 2007), 112–121.
63. Solove, D.J. 2013. *Nothing to Hide: The False Tradeoff Between Privacy and Security*. London: Yale University Press.
64. Israni, A., S. Erete, and C.L. Smith. 2017. Snitches, trolls, and social norms: Unpacking perceptions of social media use for crime prevention. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, 1193–1209. New York, NY: ACM.
65. Being African American & LGBTQ: An Introduction. https://www.hrc.org/resources/being-african-american-lgbtq-an-introduction/. Accessed 25 Apr 2019.
66. Morton, M.H., A. Dworsky, and G.M. Samuels. 2017. Missed opportunities: Youth homelessness in America. In *National Estimates*. Chicago, IL: Chapin Hall at the University of Chicago.
67. Hargittai, E. 2005. Survey measures of web-oriented digital literacy. *Social Science Computer Review* 23 (3): 371–379.
68. Hargittai, E., and E. Litt. 2013, May. New strategies for employment? Internet skills and online privacy practices during people's job search. *IEEE Security Privacy* 11 (3): 38–45. https://doi.org/10.1109/MSP.2013.64.
69. Park, Y.J. 2011. Digital literacy and privacy behavior online. *Communication Research* 40 (2): 215–236. https://doi.org/10.1177/0093650211418338.
70. Kang, R., Dabbish, L., Fruchter, N. and Kiesler, S. 2015. "My data just Goes everywhere:" user mental models of the internet and Implications for privacy and security. In *Eleventh Symposium on Usable Privacy and Security SOUPS'15* (Ottawa, 2015), 35–52.
71. Vitak, J., Liao, Y., Subramaniam, M. and Kumar, P. 2018. "I knew it was too Good to be true": The challenges economically disadvantaged internet users face in assessing trustworthiness, avoiding scams, and developing self-efficacy online. In *Proceedings ACM Human-Computing Interact* 2, CSCW (Nov. 2018), 176:1–176:25. https://doi.org/10.1145/3274445.
72. Altman, I. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory*. Brooks/Cole: Crowding.

73. Palen, L., and P. Dourish. 2003. Unpacking “privacy” for a networked world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 129–136. New York, NY: SIGCHI.
74. Marwick, A. 2012, June. The public domain: surveillance in everyday life. *Surveillance & Society* 9 (4): 378–393.
75. Ahern, S., Eckles, D., Good, N.S., King, S., Naaman, M., and Nair, R. 2007. Over-exposed? Privacy patterns and considerations in online and Mobile photo sharing. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* 357–366. New York, NY: SIGCHI.
76. Besmer, A., and H. Richter Lipford. 2010. Moving beyond Untagging: Photo privacy in a tagged world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1563–1572. New York, NY: SIGCHI.
77. Marwick, A., and Danah Boyd. 2010. I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society.* 113 (1): 114–133.
78. Stutzman, F., and W. Hartzog. 2012. Boundary regulation in social media. In *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work*, 769–778. New York, NY: ACM.
79. Stutzman, F., and J. Kramer-Duffield. 2010. Friends only: Examining a privacy-enhancing behavior in Facebook. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1553–1562. New York, NY: SIGCHI.
80. Vitak, J., S. Blasiola, S. Patil, and E. Litt. 2015, May. Balancing audience and privacy tensions on social network sites: Strategies of highly engaged users. *International Journal of Communication* 9: 20.
81. Yao, M.Z. 2011. Self-protection of online privacy: A behavioral approach. In *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*, ed. S. Trepte and L. Reinecke, 111–125. Berlin: Springer-Verlag.
82. Lampinen, A. 2015. Networked Privacy Beyond the Individual: Four Perspectives to “Sharing.” In *Proceedings of the Fifth Decennial Aarhus Conference on Critical Alternatives*, 25–28.
83. Lampinen, A., V. Lehtinen, A. Lehmuskallio, and S. Tamminen. 2011. We’re in it together: Interpersonal management of disclosure in social network services. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 3217–3226. New York, NY: SIGCHI.
84. Lampinen, A., S. Tamminen, and A. Oulasvirta. 2009. All my people right Here, right now: Management of Group co-presence on a social networking site. In *Proceedings of the ACM 2009 International Conference on Supporting Group Work*, 281–290. New York, NY: ACM.
85. Nissenbaum, H. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford Law Books.
86. Wisniewski, P., A.K.M.N. Islam, B.P. Knijnenburg, and S. Patil. 2015. Give social network users the privacy they want. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, 1427–1441. New York, NY: ACM.
87. Baumer, E., P. Adams, V.D. Khovanskaya, T.C. Liao, M.E. Smith, V. Schwanda Sosik, and K. Williams. 2013. Limiting, leaving, and (re)lapsing: An exploration of Facebook non-use practices and experiences. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 3257–3266. New York, NY: SIGCHI.
88. Rainie, L., A. Smith, and M. Duggan. 2013. *Coming and Going on Facebook | Pew Research Center*. Washington, DC: Pew Research Center.
89. Lewis, H. 2016. *The Politics of Everybody: Feminism, Queer Theory and Marxism at the Intersection*. London: Zed Books.
90. Duggan, M. 2017. *Online Harassment 2017*. Washington, DC: Pew Research Center.
91. Hamidi, F., M.K. Scheuerman, and S.M. Branham. 2018. Gender recognition or gender reductionism? The social Implications of embedded gender recognition systems. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 8:1–8:13. New York, NY: CHI.

92. 2017. *Discrimination in America: Experiences and Views of LGBTQ Americans*. National Public Radio, the Robert Wood Johnson Foundation, and Harvard T.H. Chan School of Public Health.
93. McDonald, N., B. Mako Hill, R. Greenstadt, and A. Forte. 2019. Privacy, anonymity, and perceived risk in open collaboration: A study of service providers. In *CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019)*. New York, NY: CHI.
94. Hoofnagle, C., and Urban, J. (2014, June). Alan Westin's privacy Homo Economicus. *Wake Forest Law Review* 49: 261.
95. Urban, J.M. and Hoofnagle, C.J. 2014. The privacy pragmatic as privacy vulnerable. Technical report #ID 2514381. Social Science Research Network.
96. Gavison, R. 1992. Feminism and the public/private distinction. *Stanford Law Review* 45 (1): 1–45. https://doi.org/10.2307/1228984.
97. Richardson, J. (2014, December). Spinoza, feminism and privacy: Exploring an immanent ethics of privacy. *Feminist Legal Studies; Dordrecht, 22*(3):225–241. http://dx.doi.org.ezproxy2.library.drexel.edu/10.1007/s10691-014-9271-3.
98. Fraser, N., Bhattacharya, T. and Arruzza, C. 2019. Feminism for the 99%. Verso.
99. Hartsock, N.C. 1983. The feminist standpoint: Developing the ground for a specifically feminist historical materialism. In *Discovering Reality*, 283–310. Boston, MA: Reidel Publishing Company.
100. Crenshaw, K. 1989. Demarginalizing the intersection of race and sex: A black feminist critique of antidiscrimination doctrine. *University of Chicago Legal Forum* 1989 (1): 139–167.
101. The Report of the 2015 U.S. Trangender Survey: 2016. http://www.ustranssurvey.org/. Accessed 21 Apr 2019.
102. Collins, P.H. 2015. Intersectionality's definitional dilemmas. *Annual Review of Sociology* 41 (1): 1–20.
103. Bardzell, S. 2010. Feminist HCI: Taking stock and outlining an agenda for design. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1301–1310. New York, NY: SIGCHI.
104. Bellini, R., A. Strohmayer, E. Alabdulqader, A.A. Ahmed, K. Spiel, S. Bardzell, and M. Balaam. 2018. Feminist HCI: Taking stock, moving forward, and engaging community. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, SIG02:1–SIG02:4. New York, NY: CHI.
105. Bardzell, S. 2010. Feminist HCI: Taking stock and outlining an agenda for design. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1301–1310. New York, NY: SIGCHI.
106. Schlesinger, A., W.K. Edwards, and R.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*, 5412–5427. New York, NY: CHI.
107. Blackwell, L., Dimond, J., Schoenebeck, S. and Lampe, C. 2017. Classification and its consequences for online harassment: Design insights from HeartMob. *Proceedings of the ACM on Human Computer Interaction.* 1, CSCW (Dec. 2017), 24:1–24:19 https://doi.org/10.1145/3134659.
108. Personas. https://www.interaction-design.org/literature/book/the-encyclopedia-of-human-computer-interaction-2nd-ed. Accessed 26 July 2019.
109. Salam, M. 2019. #WhatsMyName stresses safety for Uber riders. *The New York Times*.
110. Kang, R., S. Brown, and S. Kiesler. 2013. Why do people seek anonymity on the internet?: Informing policy and design. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2657–2666. New York, NY: SIGCHI.
111. Chang, E. 2019. Opinion | what women know about the internet. *The New York Times*.
112. Marx, G.T. 1999. What's in a name? Some reflections on the sociology of anonymity. *The Information Society* 15 (2): 99–112.
113. Zuboff, S. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.

114. Dourish, P. 2006. Re-space-ing place: “Place” and “space” ten years on. *Proceedings of the 2006 20th Anniversary Conference on Computer Supported Cooperative Work* (New York, NY, USA, 2006), 299–308.
115. Gandy, O.H. 2017. Surveillance and the formation of public policy. In *Surveillance & Society Biennial Conference 2017*.