The Politics of Privacy Theories: Moving from Norms to Vulnerabilities

Nora McDonald
University of Maryland, Baltimore County
nkm@umbc.edu

Andrea Forte
Drexel University
aforte@drexel.edu

ABSTRACT
Privacy and surveillance are central features of public discourse around use of computing systems. As the systems we design and study are increasingly used and regulated as potential instruments of surveillance, HCI researchers—even those whose focus is not privacy—find themselves needing to understand privacy in their work. Concepts like contextual integrity and boundary regulation have become touchstones for thinking about privacy in HCI. In this paper, we draw on HCI and privacy literature to understand the limitations of commonly used theories and examine their assumptions, politics, strengths, and weaknesses. We use a case study from the HCI literature to illustrate conceptual gaps in existing frameworks where privacy requirements can fall through. Finally, we advocate *vulnerability* as a core concept for privacy theorizing and examine how feminist, queer-Marxist, and intersectional thinking may augment our existing repertoire of privacy theories to create a more inclusive scholarship and design practice.

Author Keywords
Privacy theory, feminist intersectional theory, queer theory

CSS Concepts
• **Human-Centered Computing** → HCI design and evaluation methods; HCI theory, concepts, and models

INTRODUCTION
Whether or not they are intended to serve as instruments of surveillance, many systems studied and designed by HCI researchers are used to track people's behaviors, location, activities, emotions, health, interests, and other personal characteristics. These systems situate HCI work in the thick of discussions about surveillance and privacy. Moreover, while targeted advertising, election interference, and surveillance permeate discussions about privacy, concerns like racism, sexism, and anti-immigrant, anti-LGBTQ sentiment simultaneously drive discussions about inclusivity and equity. How do common privacy theories shape design and research practice, particularly where inclusivity and equity are concerned? Understanding the answer to this question can help grow responsible scholarship in HCI.

Privacy is a concern that affects all people, online and off, although the nature of privacy concerns vary depending on the person and the context. This variability has made privacy a rich area of empirical and philosophical innovation. In HCI and related design disciplines, designing systems for technology users who are constantly changing contexts—moving from one group or one platform to another, platforms that are themselves constantly updating their policies and privacy settings— has been an enduring and much beloved problem [23, 77]. This familiarity and appreciation for the problem of context has made Helen Nissenbaum's concept of privacy as *contextual integrity* a natural fit for HCI researchers looking to understand how to investigate and respect privacy concerns of technology users [81].

In this paper, we review privacy theories with special attention to the privacy paradox, boundary regulation, and contextual integrity—not only in its historic role as a response to privacy theories that inadequately addressed the problem of context but also as a theory that itself has limits and requires augmentation. Specifically, we consider the limitations of norms as an analytic tool, provide a case study of how and when the unique privacy concerns of vulnerable populations can slip through norm-based analyses of privacy requirements. We define *vulnerable* populations as those whose members are not only more likely to be susceptible to privacy violations, but whose safety and wellbeing are disproportionately affected by such violations. These vulnerabilities are often conceptualized as identity characteristics, for example living in poverty or within a child welfare system [7, 96], immigrants [41, 66], activists, journalists [101], those with HIV [106], LGBTQ [12, 39, 54, 93], survivors of domestic abuse or intimate partner violence or surveillance (IPV or IPS) [22, 35, 74], the very young [6, 108] and very old [48], those using assistive technologies and those who suffer discrimination because of their race, gender or sex, and class.

We join Pierce et al. [88] in advocating for vulnerability as a core concept for understanding risk, but we further suggest that intersectional feminist and queer Marxist theory provide important guidance in considering not only features of identity and context, but economic and political systems of oppression that converge unequally on different individuals.

CHI '20, April 25–30, 2020, Honolulu, HI, USA

ACM 978-1-4503-6708-0/20/04…$15.00
https://doi.org/10.1145/3313831.3376167

PRIVACY THEORIES

HCI scholars have imported and adapted many concepts from overlapping literatures to inform privacy-related research and design efforts. In the next sections we walk through enduring privacy theory canons and discuss their strengths and shortcomings. HCI privacy work is grounded in the understanding that privacy is simultaneously, "individually subjective and socially situated," as Ackerman and Mainwaring observed [1]; nevertheless, to understand the body of privacy theories that inform HCI research, we organize them into two broad categories: those focused on the individual and those focused on social features.

Theories Focused on the Individual

Boundary Regulation

Social psychologist Irwin Altman conceives of privacy as a dialectical process for controlling privacy boundaries [4]. Building on Altman's theory, Palen and Dourish [86] helpfully update boundary regulation for the internet, positioning it as a framework that involves disclosure (privacy vs. publicity); identity (features of identity vs. different audiences); and temporality (past/present/future self are in tension). These areas of control evolve as technologies and social practices change. For instance, one might not have worried about what they posted on Facebook in the past until the company designed a search feature that allowed users to find and retrieve old posts. Palen and Dourish use the example of posting manuscripts as PDFs, not Word documents, which raises future barriers to editing the document. Palen and Dourish's disclosure, identity, and temporality boundaries are a helpful way of advancing Altman's way of thinking about boundaries because they highlight the need to depart from traditional views about what is necessary to maintain boundaries on the internet, and the need for new solutions to regulate access to the self.

Social media researchers have explored the idea that privacy frees people to segregate and tailor identity performances through regulating access to personal information. The types of strategies that people employ include pseudonymity and creation of multiple profiles to manage group contexts [97]. Even as context collapses and the proliferation of online spaces complicates boundary work, Marwick argues that tending social boundaries is part of everyday networked practice [69]. Nevertheless, Vitak et al. find that collapsing contexts and imagined audiences (those they are actively considering as well as potential viewers such as a future employer) further complicate privacy management strategies [103]. Yet doing so requires a great deal of effort on the part of the user. Consider the strategies identified by Stutzman and Hartzog—practical obscurity (obscuring profile through modification of privacy settings, pseudonymity, technical separation) and transparent separation (maintaining multiple profiles without obscuring identity) [97]. These strategies are not easily achieved in modern networked environments. The concept of boundary control lays a critical foundation for understanding how people regulate identity clues, yet it tends to emphasize identity exploration, manipulation/creation, and self-presentation over risk of violation.

Westin's Individualism and the Privacy Paradox

Alan Westin grouped privacy into four states: solitude, intimacy, reserve, and anonymity [107]. *Solitude* describes the state of being free from observation by others. Most privacy theories are concerned with intimacy and reserve because those are spheres in which access to information is traditionally guarded or managed in personal relationships. *Intimacy* encompasses the conditions that we share with family, close friends and work cliques. *Reserve* is "the creation of a psychological barrier against unwanted intrusion, which occurs when the individual's need to limit communication about himself is protected by the willing discretion of those surrounding him." *Anonymity* "occurs when the individual is in public spaces or performing public acts but still seeks, and finds, freedom from identification and surveillance." Its character and significance have taken on new meaning on the internet, a world that allows for more varied forms of remote participation and equally varied and penetrating forms of surveillance.

Westin first raised the specter of uncertainty of the individuals' desire for privacy (of a privacy paradox) by segmenting individuals into pragmatists, fundamentalists, and unconcerned. He argued that, in any situation, there are always individuals who are apparently not concerned about their privacy but because the groupings are fluid, the composition of that unconcerned group will vary according to the context [47]. At the same time, he argued for individual-driven determination about what data is shared about them, which would become the bases for notice and consent laws [16].

Privacy focused on "Community": Contextual or Distributed Privacy

As privacy researchers in HCI and other fields have embraced more collective notions of privacy, attention has shifted to the idea that boundaries are regulated as part of a group or communitarian process [59]. A central example of this move toward understanding privacy as dynamic, shared beliefs is contextual integrity, a framework introduced by Nissenbaum, which acknowledges that while "privacy norms vary across and within social groups," they are "systematically related to characteristics of the background social situation" [81]. This framework posits that expectations for privacy are tied to the norms and data flows of a given context, and that appropriate information flows are those that align with shared information norms of a given context. Information norms, a concept critical to contextual integrity, govern the flow of information from one party in accordance with community principles of appropriateness and distribution or information flows, establishing what content may be shared with which parties, and by whom [80].

The advantages of replacing individual concerns with "community" norms is that it prompts investigation of shared expectations and becomes a practical way to talk about

expectations of privacy and how they are articulated and agreed upon. For instance, we know (or intuit) that while its acceptable for a doctor to ask about your medical history, it's not necessarily acceptable for the reverse [80].

Social Norms

Social norms play a central role in community-focused approaches to theorizing privacy. Social norms refer to the values and behaviors that groups recognize as being shared or expected. Norm articulation is the retranslation of these norms into policy and design. An example of norm articulation would be placing a barrier on a bathroom stall to suggest that people expect not to be seen when doing certain things in the bathroom. In Japan, these norms are taken a step further to suggest that people should not be heard either, as the toilets often play music in public stalls. We might place carrels in libraries to shield others from our screen or a book we're reading, or curtains in voting booths to prevent anyone from observing our vote. Interestingly, some get out the vote campaigns are trying to bring this technically public data out of obscurity [95] with apps that transform social norms around voting by, for example, alerting others that friends haven't voted in previous elections. In each of these contexts, these barriers mean slightly different things and draw from different sets of concerns and values.

The concept of a norm is helpful because it prompts researchers to define shared features of groups that members themselves may not think about or even perceive. Norms usefully delineate what views and values (or at very least, expectations) must be shared in order for people to want to participate in a group. They can also provide useful guidance in designing systems, policies, and laws that are more likely to serve a given community. In the context of online privacy, where context collapse means that audiences converge in sometimes unforeseen ways, thinking about divergent norms is particularly useful for designers.

Lampinen et al. introduces the idea of group co-presence, when many groups are simultaneously present on one network, to explain how boundary regulation works when multiple norms threaten to intersect [60]. This occurs, in part, because online interactions are unlike the physical world where time and space help us partition separate and discordant aspects of our lives. Interestingly, one of the ways that people manage group co-presence is by dividing the platform into separate spaces and selection of appropriate communication channels, partitioning off spaces and by extension, norms and values [61]. In fact, this management of group co-presence may have its roots in less recent ways of framing privacy, emerging from law and philosophy, as "a balancing of normative and individual interests" [64], where benefits to the group are weighed against benefits to the individual. Participation in social network sites is often conceptualized as a tradeoff between the aspirations of personal privacy and the benefits of participation—although Wisniewski argues that those whose privacy needs are met are more engaged in such sites, demonstrating that "tradeoff" is not the only model [109].

CRITIQUE OF PRIVACY THEORIES

In this section, we explain how using norms as yardsticks for design and policy, while useful, also privileges certain members of groups over others. The implicit assumption that norms are shared by and represent the interests of all members of a group is problematic for privacy theorizing in particular, where it can render some people's privacy concerns less visible than others.

Norms. What are they good for?

Norms transfer agency to the collective, but realistically, not all parties are equally engaged in the process of establishing norms. If systems are developed to support norms that are unrepresentative of their users, one would expect to find resistance and circumvention of certain features among populations who have been less well represented. Indeed, much research looks at how users, particularly teens and others who have little power and privilege circumvent norms embedded in design of social networks [14, 70, 72]. Norms are useful shorthand for how people expect to navigate relationships, situations, and spaces but, as we will illustrate using a case study of open collaboration projects, it is often the most privileged individuals who are able to participate in norm setting and articulation.

Sarah Igo's *The Known Citizen* provides useful context for the history of privacy discourse and justification for examining privacy outside of normative perspectives that complicate, if not, obfuscate important issues around privacy in relationship to power [50]. Like Igo, we challenge the idea that privacy is a uniform shared value. Marwick and Boyd similarly highlight how power can be used to normalize privacy violations:

> "The stark reality is that achieving privacy is especially difficult for those who are marginalized in other areas of life. Parents argue that they have the right to surveil their children 'for safety reasons.' Activists who challenge repressive regimes are regularly monitored by state actors. And poor people find themselves forced to provide information in return for basic services" [73].

Privacy Literacy

Literacy is an example of a normative approach to defining a socially desirable set of skills and behaviors. When people's practices or skills don't align with norms or place them at a disadvantage, one explanation is that it's because they are not literate in the set of expected practices. The remedy for literacy gaps is usually some form of educational intervention. In some cases, this framing may be accurate and effective; however, it may also confuse lack of literacy with intentional, alternate behaviors or a lack of power to act otherwise. What seems to be a lack of literacy may at times be a lack of agency. For example, the use of banking sites on insecure public kiosks or public wifi may suggest that educating people about risks can be helpful; however, those

who are dependent on public resources might have few choices about where to do their banking conveniently.

In the latter case, the concept of privacy literacy can be considered either ineffective as a safeguard or beside the point, insofar as it shifts responsibility for privacy to people who cannot possibly be expected to fend for themselves given their lack of control over the systems they inhabit. As a frame, privacy literacy places the burden of privacy protection on the individual. As we will discuss, we argue that problems with the framing of "literacy" stem from its origins in establishing educational norms that fail to consider the structural inequalities and idiosyncratic experiences that shape people's wide-ranging behaviors and needs. Privacy literacy is at best insufficient in protecting low income populations from the difficulties they face safeguarding their privacy [67].

'Victim Blaming'

Research with marginalized youth supports the idea that privacy literacy is insufficient to explain privacy-related behaviors. Marwick et al. find that marginalized social and economic positions amplify risks online, and contribute to avoidance of social media and self-censorship [71]. However, they use the parallel finding that marginalized youth experience structural racism in the form of policing and physical surveillance to recast the victim-blaming narrative around privacy. The study portrays youth as well aware of the connection between Facebook posts and online and offline consequences (e.g., being doxed, bullied, or fired) and therefore prone to self-censor or disengage altogether. Marwick et al. further explain how these same young adults are exposed to police surveillance and brutality from which there is no escape through disengagement or taking individual responsibility. This framing helps to circumvent the "victim-blaming narrative of some media literacy efforts" that have traditionally placed responsibility on individuals to secure their privacy [71]. The idea that some individuals are not concerned about their privacy, or that people's behavior contradicts their stated concerns (what is referred to as the "privacy paradox" [3, 9, 68, 78, 82, 84, 100, 107]), leads to a kind of "victim blaming"— i.e., when those who have no control over harm that befalls them (in this case, from surveillance) are told that they are responsible for safeguarding themselves (e.g., their privacy).

Marwick et al. challenge the notion that young people's behavior exemplifies a privacy paradox; they show how young people are often beholden to privacy infrastructures that are similar to systems of oppression, arguing for "framing online privacy violations as inevitable and widespread" and young people's responses as rational [71].

The so-called privacy paradox—that people say they care about privacy but act as though they do not—has been supported with findings that individuals do not manage their privacy settings on social media [40], that they underestimate their profile visibility [10], and that stated privacy concerns are a weak predictor of behavior [2]. Some cite lack of awareness, peer pressure and trust in the network to explain the misalignment between stated privacy concerns and privacy management [2]. This frame does not account for the possibility that people simply feel powerless to maintain their privacy and the potential consequence that they may resort to measures outside of explicit boundary regulation such as blocking [110]. The privacy paradox arises from powerlessness, not necessarily an enactment of indifference or contradiction. This disempowerment, engendered by the awareness that privacy violations are ineluctable, spawns what may appear to observers as apathy among teens [45]. It can, in fact, be a sense of futility masquerading as apathy. Research depicts users as both able to control certain types of information while also feeling helpless to control other types of information. Woodruff et al. demonstrate where the organizing principles that once inspired the privacy paradox (Westin's Privacy Segmentation Index, which grouped individuals based on their privacy attitudes and behaviors) do not hold up when the consequences of privacy violations are considered [112]. Other literature demonstrates that people's experiences shape the stringency of their privacy practices [53].

Notice and consent regimes, with their presumed alignment between intent and behavior, also lay bare the privacy paradox. Drawing on Foucault, Hull argues that such privacy self-management regimes are grounded in neoliberal thinking that suggests "subjectivity and ethical behavior are matters primarily of individual risk management coupled with individual responsibility for poorly-managed risks" [49]. Others argue that notice and consent is grounded in the assumption that because privacy laws, tools and regulatory bodies exist, users must control their privacy [76]. Gurses and Hobokon situate privacy as hard to address due to the misalignment of software development practices with regulations that presume a static production process [42].

Others have argued that normative constraints perpetuated by surveillance capitalism may prove insurmountable [36, 113] and that pervasive surveillance disproportionately harms vulnerable and low-income people just for taking part in society—from online consumerism [62, 79], to social network sites [67], to the workplace [92], to social services [15, 27, 67]. The management of identity knowledge is always limited by the scope of tools that system designers make available. For low-income communities, surveillance can lead to avoidance of financial and social institutions for whom the risks of privacy breaches are greater because they lack secure technologies and resources for combating privacy violations like identity theft [67].

Vulnerable Identities

For marginalized or stigmatized individuals in particular, information visibility can carry risk on social networks [71, 87, 89, 102] such that users may attempt to conceal some or all aspects of their identity [5] or simply not engage altogether [24]. Research suggests that people sometimes circumvent risk by performing their privacy in public [14] or

censoring [89]. Mary Gray explores how Queer youth use social platforms as a space to articulate and negotiate counter-norms but observes that Queer youth are also subject to censorship when they perceive threats. Even in these boundary publics, where many people have mastered the art of being private in public, harassment emerges [69]. In the panoptic environment of social networks, individuals are prone to self-censorship, suggesting that behaviors may have shifted to accommodate surveillance infrastructures. Marwick describes social surveillance as the state of heightened and proactive awareness of the activities of others and contextualization of our own surveillance [69].

There will always be tensions in the design of systems, but designs that take into account vulnerable identities may eventually foster more democratic systems that have greater and more equal value for all participants. Those who by design or accident are currently excluded from online platforms because of unmet privacy requirements not only could have more freedom to choose their level of participation; they may also bring perspectives from which all participants could benefit.

As discussed, research as well as public discourse has often labeled individuals who don't appear to do anything to preserve their privacy as either not knowing any better (i.e., failing to appreciate their risks and the consequences of those risks) or not caring. In contrast, other research, including HCI, has demonstrated how people manage the presence of multiple groups by cloaking or censoring their behavior (e.g., [14, 59]). Despite the success of individuals to manage overlapping networks or groups, the entanglement of group norms with individual responsibility may place undue burden on vulnerable participants whose challenges are structural and system-based and not necessarily amenable to challenges from individuals or even groups.

Real World Implications

Individualistic theories of privacy assume that the internet is a democratized space where people are free to negotiate privacy within the normative boundaries set by various platform service providers. The problem is that, as Palen and Dourish noted, one must give up identity information simply to participate in the internet, and there are no conventional (or physical) partitions behind which to conceal oneself. Individualistic theories of privacy self-regulation and paradox take for granted the idea that humans have agency over their privacy online. When privacy is not executed well (or as intended) this perspective places blame on the victim, rather than considering whether structural inequalities could account for lack of alignment between privacy goals and actions [71]. This perspective pits the individual against multiple, sometimes competing norms. The idea that it is up to individuals to maintain their own self-interest (i.e., privacy) is a traditionally privileged, neoliberal stance. In their studies of interpersonal privacy strategies, Lampinen et al. note that individuals not only make frequent assumptions about what to share with others and what not to, they take for granted that others share the same values, or can be trusted, and are often missing the right tools to negotiate privacy precepts [59, 61]. Notably, social network sites don't provide space or tools for explicit negotiation required to formalize norms, so people make assumptions and don't necessarily know what's appropriate, particularly when it comes to sharing information about others [59].

Scholars worried about shifting social norms around privacy often point to the privacy paradox. We believe that the privacy paradox actually suggests peoples' use of technology reflects their response to values and norms embedded in the system design and not necessarily their own values. Further, we suggest that this is especially true of technology users who have vulnerabilities and/or whose needs and requirements are marginalized. As a frame, privacy literacy places the burden on the individual and blames them when they don't seem to care enough about their privacy to take dramatic steps to protect it.

The real world implication of using social norms as a yardstick by which to measure privacy concerns is that it mismeasures the concerns of individuals whose concerns are *not* the norm. Attention to social norms leads scholars to consider the dominant values of users. For example, sharing real names with social networks is a norm, but for some (minority, low income individuals, in particular) this can result in threats like opportunity loss that results in censorship [89] or abstinence [104]. Alice Goffman asserts that individuals abstain from, for example, reporting crimes or attending the birth of their children to avoid technological surveillance [38]. Mistrust of social media and the internet more generally among low income individuals is theme identified by Vitak et al [104].

When we assume that individuals are victims because of their skillset (and not because of structures of discrimination affecting vulnerable populations, e.g., ensuring they are more often targets because they have devices with less security [26] or are dependent on public internet and resources), we presume that the internet is a skill and not an extension of our flawed society and networked life.

AN EXAMPLE: PRIVACY NORMS IN OPEN COLLABORATION PROJECTS

Here we use a case from the HCI literature to demonstrate how norms can shape the design of systems in ways that leave some people out because their privacy concerns are not the dominant ones. Open collaboration projects like open source software, Wikipedia, citizen science, or openStreetMap are often studied in HCI and adjacent literatures because they provide extensive public datasets of online interactions.

Twin studies published at CHI and CSCW investigated a. the concerns of people who identify a having privacy concerns when contributing to open collaboration projects [28] and b. the privacy concerns perceived by the organizations that provide infrastructure for open collaboration projects [75].

Together, these studies highlight the gaps between the privacy concerns felt by people participating in an online project and the concerns perceived by those who provide the tools that people use.

Specifically, people who identified as having privacy concerns were worried about things like harassment, threats, reputation loss and often took measures to either hide their identity or avoid what they viewed as risky participation. For example, Forte et. al interviewed a medical student who simply stopped adding information to Wikipedia about women's health because she didn't want the pushback [28]. In another case, a software developer took pains to hide his location when posting online because he had written open source software that he believed some people objected to on political grounds. Still another person feared that she would attract unwelcome attention in her home country of Iran and asked "braver" non-Iranian friends to post for her if it was on a topic that could be construed as political.

In contrast, in interviews, McDonald et al. found that open collaboration service providers viewed privacy protection measures like anonymous posting largely as a way to ensure low barriers for newcomers to start contributing [75]. The kinds of concerns described by privacy-seeking contributors were not central features of how service providers viewed anonymous contributors. Moreover, in a subsequent analysis of public mailing list records from the English Wikipedia community, McDonald et al. confirmed that the perspectives of vulnerable privacy seekers seldom surfaced in discussions of how Wikipedia should handle anonymity. The paper concludes that people with privacy concerns are by definition alienated from the spaces where norms are established through discussion and participation. Their privacy concerns render them less able to participate in the community and therefore unavailable to contribute to the very discussions that might allow them to raise their privacy concerns and help define community norms.

The case of open collaboration highlights a real-world example of dominant voices and norms overshadowing the privacy concerns of less powerful people. When researchers and designers look to understand norms in a community, they may find that the norms align with the interests of those who are most free to participate. Structural barriers and inequalities dampen certain voices, rendering them "counter normative." Without taking intentional steps to identify less powerful or marginalized people in a community, social norms leave us with an impoverished view of privacy concerns.

POLITICS OF PRIVACY THEORIES

In this section, we consider the political theories to which the dominant privacy frames are moored as a way of framing shifting political tides (characterized by socialist and more inclusive politics on the one hand and populist, isolationist movements on the other) and how they might align with a new analytical approach to studies of privacy.

The transition in privacy theories from concepts of public and private spheres managed by user-centric boundary control to a more diffuse and porous sphere managed by shared community norms is an important advance in scholarly thinking about the ethics of privacy across a broad range of networked spaces. Nissenbaum, for instance, provides an analytical update to individualist theories, such as Altman's, which didn't account for the permeability of boundaries [86].

Contextual integrity draws on the thinking of Michael Walzer, whose argument in *Spheres of Justice*, explores distribution of goods (e.g., public education, healthcare) in relationship to the context of these goods [105]. This highly contextualized notion of pluralistic justice (sometimes referred to as "communitarianism," a term which is applied but which Walzer himself did not use) translates well to contextual integrity, where contexts dictate privacy expectations and thus distribution or flow of data. Contextual integrity builds on parallels between Walzer's concept of spheres that organize around public goods to describe the norms of a given context around which communities organize and design principles for information flows that are generally successful and ethical.

Walzer's theory assumes distribution of goods are local and culturally dependent and thus takes into account only people with legitimate access to those spheres or platforms. The same could be said for information flows that only take into account the "unique set of norms of justice" [80]. This has unsettling implications for those who are concerned with privacy for vulnerable populations who require privacy protections that render them "second class citizens" online [75] and offline because they are often from populations that suffer inequalities and which may not have the same privacy rights of privileged individuals [15].

Walzer asserts that the traditions and culture of a given community (requiring local understanding) is what determines the meaning of goods, and that those communities are defined by "admission and exclusion" and by their *shared values*. Scholars have applied this notion and concluded in studies of online environments that privacy has not been violated if the members of the community perceive that only certain types of people (essentially those without privacy concerns) can join [13]. Distributed spheres and contextual integrity seek consensus but are permissive of inequality because justice is defined by the community, which inoculates it from redress by "outsiders" who are seeking more privacy and by definition can't get in.

Walzer's theory rests on the dominant view of justice held by a community—that is, it lacks flexibility with regard to those who reside outside the boundaries of membership, or for that matter, the legal rights of a community (e.g., immigrants). Nissenbaum similarly assumes that a specific context dictates the appropriate flows of information based on widely held norms of distribution within that context. But when adopted in HCI, this leaves room for the design of

platforms where only privileged members can participate because they don't experience risk factors that exceed the normative threshold. In some cases, membership may equate to racial, economic, or gender privilege, such as being white, or middle class, or male.

Feminist political philosopher, Susan Moller Okin argues that Walzer (and other communitarian) theories that "appeal to 'our traditions' and the 'shared understandings' approach are incapable of dealing with the problem of the effects of *social domination* on beliefs and understandings" [83]. Okin takes up Walzer's counter-argument that competing ideologies can reach some resolution and that "the possibility of chance in general rest on the flourishing of dissent":

> "The weaknesses of both these lines of defense of a theory of justice built on the interpretation of shared meanings are readily exposed when we raise the issue of the justice or injustice of gender. The problem with the first counterargument—the reliance on dissent—is that the closer a social system is to a caste system, in which social meanings overlap, cohere, and are integrated and hierarchical, the less likely it will be that the dissenting ideas appear or develop. The more thoroughgoing the dominance, and the more pervasive its ideology across the various spheres, the less chance there is that the whole prevailing system will be questioned or resisted. By arguing that such a system meets 'internal standards of justice' if it is really accepted by its members, Walzer admits the paradox that the more likely a system is to be able to enshrine ideology of the ruling group and hence to meet his "shared understandings" criterion of justice, the more unjust it will be by his other criterion, since dominance will be all-pervasive within it." (Page 64) [83].

Indeed, it is simply impossible when dissent is coming from marginalized and sometimes indivisible actors for change to flourish. Walzer's model assumes collectives share the same values.

Other critics of Walzer have argued for interpretations that downplay pluralism (which Walzer equates with competing ideologies that presumable resolve) and advocate for justice that traverses boundaries of political communities—Trappenburg calls this "mitigated pluralism" [99]. They oppose the view that a sphere (or a context) can or should "uphold their internal moral logic" and maintain distinctions between spheres of justice. This an important criticism for those who would argue that sphere-specificity is permissive of inequality.

Underlying Walzer and Nissenbaum's work is a commitment to ethics and self-determination within a "protected space" [85]. But what constitutes a "protected space" or a sphere or a context? The internet is, perhaps, infinitely extensible and code (as well as data flows and unseen surveillance) complicates notions of space, sphere or context. Further, platforms and technologies themselves restrict access and features to those who refuse to "opt in" to various privacy policies that dictate what and how they can use information [113]. In our example of research of open collaboration platforms, users who chose to go anonymous may be limited in what features they can access and their ability to participate, for instance, in chat spaces [75].

Territories and Networked/IoT Life

Some argue that territories and the laws that govern them are also becoming increasingly abstract and deny members of the community say in how information flows. Smart city technologies are one example of how sensor technologies are bypassing laws to dictate how space is used and what gets built, replacing politics with computation [57]. One such firm that Zuboff details in her book, *Surveillance Capitalism*, weaves together data flows from public and privacy assets like ride-sharing services and public transit with the goal of providing municipalities with better parking data that translates to more city revenue [113]. The same companies are collaborating with urban planners to decide what to build and where, taking decisions about housing and urban geography out of the hands of constituents and leaving it up to algorithms and markets.

This severing of technology with local identity and interests is something that Latour takes up in his mediation on politics in the Anthropocene embrace crisis of environment and social justice as inextricable [63]. He sees the fight being over the politics of territory and a borderless world. Latour considers a future that leaves the most vulnerable in a sort of constant state of diaspora, a state from which he gleans a way forward through a "radical terrestrial." For Latour, the future is a nomadic and permeant context where the most vulnerable, clamoring for resources, will require fluid and permeable boundaries. In a context where immigration is the norm, what are our norms and what context or material production could possibly contain them or reflect them? He portrays a context that is in flux, which motivates my turn toward identity theories that move across borders and regulated boundaries and defy physical notions of privacy.

EXPANDING THEORETICAL HORIZONS

In this section, we look at how feminist, queer and intersectional perspectives deal with identity, and we argue that they offer a potential salve against the tendency towards normative identity-politics that appear to reproduce inequalities online.

Feminist struggles have long been concerned with privacy based on concerns that any form of repression can be violative of individual boundaries [37, 91]. The State's incursion into the home is the object of critique for Marxist feminists [33] as well as legal scholars [15], who argue that conditions of class, gender, and race inequality lead to violence, and that our approaches to welfare and criminalization, for example, undermines the privacy and civil rights of those they attempt to serve. Recent Marxist-feminist work has grappled with the way capitalism imposes norms that regulate sexual identities once considered

counter-normative, making them feel welcome, but only within a monitored sphere [33]. We see this echoed in the way that social networks address hate speech, enlisting the community to defend (implied weaker) others against attack. This kind of socially constructed peace-keeping (at minimum) set the terms by which identities are protected by those who don't necessarily occupy them, if not how those identities are expressed.

Intersectional theory expands the marginalized perspective represented by feminist theories [46] to account for the impact of having simultaneous identities that may compound oppression in relationship to systems of discrimination.

Kimberlé Crenshaw [21] "coined" the term [18, 20, 43] as a black feminist critique of antidiscrimination doctrine and feminist theory [43]. Although intersectionality as social critique was popularized by Crenshaw, numerous others provided critical insight into its use as an analytical framework (e.g., [18, 19]) and have also pointed out its roots in critical black feminist thought dating back to the 18th century [90]. The HCI community has recently begun to recognize intersectional thinking as a powerful means to recognize and redress when inequities and injustices are recreated or entrenched in the design of computing systems [31, 58, 90, 98, 111].

Queer theory situates the individual as shaped by power, drawing heavily on Foucauldian frameworks. Queer theory interrogates discipline and power from the perspective of the radical, intersectional individual and emphasizes lived experience. Queer-Marxist queer theorist, Holly Lewis, argues that experience is critical to shaping a radical identity but cautions that material comforts can easily erase or take the place of the experience of discrimination [65]. These are lessons that serve privacy theorizing as well. It is easy for individuals to accept the helpfulness of technology and forget past (and perhaps continuing) transgressions. Notably, Lewis argues that intersectionality, while an important corrective to privileged feminism, ignores the way in which racism and sexism are routed within a "material matrix" and that class should not be viewed as an "*additional vector"* but rather, "*is* the metric of social injustice" [65].

Queer theory is grounded heavily in Foucauldian notions of power-knowledge, which posit that norms (or the elimination of difference) are a way for the state to impose social control [30]. Foucault argued that discipline is established through imposition of norms via surveillance (or the semblance of it) [29]. Drawing on the conceptualization of the panopticon, the mere visibility of a surveillance apparatus is intended to reinforce norms, regardless of whether there is someone actually watching.

Ultimately, Lewis argues that queer communitarianism—shared norms around being queer—may signal acceptance, but also requires that vulnerable groups occupy sanctioned safe spaces in which they are identified and accepted but also excluded; that is, they do not have power. For Lewis communitarianism evokes "boundaries and exclusions," not activism. Interestingly, Lewis does not believe that norms need to be overcome so much as exposed for their power and political relations, with emphasis on economic/exploitative and political vectors of oppression. Those who are forced to compromise their privacy are far more likely to be marginalized and subject to discriminatory power relations because of their identity and class [73]. Queer theories and notably queer-Marxist theory interrogate norms and how they operate for vulnerable identities through late stage capitalism. We therefore urge researchers to consider both the political and economic/exploitative vectors proposed by Lewis and the structures of inequality proposed by Crenshaw in addition to identities and discourse that shapes norms and behaviors. These frameworks are most powerful when taken together, precisely because they don't just consider identities, structures, or discourses alone. We see no circumstances where race, gender and class (as well as other culturally situated vulnerabilities) are not dictating the terms (and challenges) of privacy in an economy and political society where power is the cite of information extraction and control.

Integrating the Two: Intersectionality and Queer-Marxism

As HCI and adjacent research communities move towards greater inclusion of feminist intersectional approaches [11, 32, 58, 90, 94, 98, 111], we propose updating our conceptual and pragmatic approaches to studying privacy to integrate intersectional and queer-Marxist theories.

Intersectional theory considers the "marginal" user whose context (e.g., roles, information, relationships, etc.) represent an alternative to the dominant norms [8] and to develop privacy frameworks that account for everyone. Queer-Marxist theory moves beyond framing inequality as vectors of political economies, but insofar as it invokes material struggles, it is relevant for vulnerable communities who often seek lower barriers on those terms. Alongside intersectionality, queer-Marxist theory offers a critical lens through which to examine identity and class as neither reactionary nor revolutionary and not in opposition to norms so much as how they operate.

Perhaps similar to Latour, queer-Marxist theory, according to Lewis, is committed to a kind of post-communitarian epoch where transnational activism would upend contextual norms. Lewis argues the materialist queer theory lens optimizes gender-based politics with its focus on profiling and exclusion. We need theories that will look at how a flood of affordable devices inadequate to protect even the savviest users are making the vulnerable more vulnerable. We need theory built on an appreciation for the way social relations make it difficult for someone to trust or access information about what services are safer, and an understanding that these relationships are, themselves, shaped by modes of production, which dictates income and accessibility of these technologies. We need to render visible the challenges that users face in relationship to their status in society, which is

not equal. There is a problem with simply looking at privacy shortfalls of undeserved communities; rather, we must look at what creates those conditions. Otherwise, we are just engaging in victim blaming [71].

"PRIVACY VULNERABILITIES" AS A CORRECTIVE MEASURE

Pragmatically, incorporating intersectional and queer theory in HCI research practice requires a shift in perspective. We propose *privacy vulnerability* as a lens through which to understand the risks faced by vulnerable individuals.

Recall that service providers' perceptions of open collaboration contributors shapes the privacy protections they provide, but that their perception leaves out a significant population who are vulnerable to privacy violations because of their gender, race, sexual orientation or interests [28, 75]. These individuals can't negotiate corrective strategies because people with vulnerabilities may opt-out or self-censor, which has the effect of making them and their concerns invisible. By purposely identifying and articulating vulnerability, researchers and designers have an opportunity to give voice to these concerns and ultimately create most inclusive and equitable designs.

These theories offer a way to investigate the concerns of vulnerable contributors that takes into account a defining context for their identities—the power structures that oppress them through identity-based norms and capitalism. To apply an intersectional, queer-Marxist lens forces researchers and technologists to consider the structures of discrimination within and without organizations that produce technologies *and* the conditions of capitalism that assume certain identity risks as the norm. For example, to recognize that both vectors make it hard or impossible for certain individuals to participate (or suffer unacceptable risks when they do) means that well-meaning service providers of open collaboration platforms must take into account identity-based vulnerabilities, they must consider the way their identities relate to structures of oppression in and outside their walls as well as the norms of privacy that capitalism dictates. We argue that these considerations extend beyond the case of open collaboration; for example, are the privacy norms and expectations of Play Store Apps an acceptable risk for an IPV victim, for a child who doesn't want to be monitored [34]? Moreover, how does being poor and surviving IPV, which means you are further exposed to information vulnerabilities, further complicate this privacy narrative?

Contextual integrity, while it provides a useful framework for thinking about privacy expectations as situated sociotechnical norms, relies on open discourse around competing values (or realities) to expose tensions around norms. If not all perspectives are present (or, as is often the case, they are not empowered) these tensions never surface. Contextual integrity assumes that in a given context the impacts of privacy violations will be experienced equally. However, we know that for instance, use of home video surveillance and public and private available data are used by police to target and deport immigrants. Although not the only company to sell its facial recognition technology (e.g., IBM, Microsoft, etc.) Amazon has also teamed up with the US Immigration and Customs Enforcement (ICE) agency to facilitate deportation by integrating existing databases of public and private data [44]. Recognizing the potential for these systems to do harm to marginalized communities in the US and the potential for further abuse underscores the urgency of the problem [51, 55].

Queer-Marxist theory argues class and capitalism are a unifying challenge for many who cannot afford to give up identity information but are nevertheless forced to by virtue of their economic conditions and the norms around those conditions. By adopting this lens, HCI researchers are well positioned to understand identity-based vulnerabilities in the context of political economies and norms that are pervasive and that help sustain structures of inequality. Considering the needs of the most vulnerable members of a community who may be marginalized by the very norms that dictate acceptable information flows, provides an important corrective measure for privacy researchers.

IMPLICATIONS FOR HCI

If we don't take corrective steps to consider vulnerable populations when designing for privacy, we run the risk of creating a future HCI that exacerbates or at best perpetuates existing inequalities. We borrow from Ekbia and Nardi, who argue for adopting a political economy perspective in HCI [25], to argue that privacy theories should be questioned by HCI scholars to evaluate whether and how these theories perpetuate or (implicitly) endorse or reify certain politics. We should not shy away from politics in our "conceptual apparatus" [25]; and we should also continue to examine what those politics are (even when we thought they were "good"). For instance, under capitalism, there are incentives for companies to obscure privacy policies and decide who gets to participate [49].

The critique we have raised suggests a range of remedies. An extreme response might be a complete revaluation of privacy-related concepts and frameworks. A more pragmatic response involves augmenting existing frameworks; for example, contextual integrity and other privacy analyses frequently rely on qualitative investigations of a population to understand important features like norms of information flow within a given context. Because it is a methodological necessity to sample from a population in order to understand privacy expectations and needs, by introducing vulnerability as a core feature of how we think about privacy, we can improve the diversity of sampling and avoid relying on the most central, safest, or easily accessed members of a given group.

CONCLUSIONS

We are witnessing the migration of vulnerable privacy concerns into the mainstream suggesting precisely this point that privileged privacy that serves one end is used to exploit a whole class of individual. For instance, the simple

technology used to stalk IPV victims is the very same technology used by parents to track their children [17]. These are technologies that have mainstream legitimate use and thus are slowly becoming the norm.

Identity and political discourse may be critical to how service providers design for privacy and how users conceive of privacy. This is a departure from individualism as well as normative frames, both of which we have shown to be entangled in ways that reinforce heteronormative, privileged identity discourse and notions of territory. Predicting information flows based on expectations is problematic—in large part because companies collect our data and we have no voice in how much and to whom it is given. The privacy violations affecting vulnerable identities are surfacing the problematic nature of our relationship to privacy design and technologies that are unregulated or *part of services* to the extent that they make attacks possible by people with no technical abilities, or who simply use those technologies and services. The convergence of social, economic, and identity-based disadvantages exacerbates harms by advertisers and governments. Facebook algorithms predict, for example, gender, ethnicity, and sexual orientation, based on user liking and friending behavior [52, 56]. Loan and job algorithms "learn" to identify women and minorities using otherwise obscure identity proxies like shopping habits or keywords. Moreover, our expectations have been constantly put to the test by continuous data breaches and the understanding that we are always sharing our data with technology companies and institutions.

Individualism assumes that people have equal voice in articulating their privacy and defending it when we know that not to be the case. Normative approaches tend to overlook especially the fact that vulnerable individuals do not have a voice in what is agreed upon to be appropriate levels of privacy. Intersectional identity frames how people behave in the context of social structures, and how those structures stifle expression and free movement.

When looking at norm-based theories, it is important to consider the political theories, cultures, classes, and systems to which they are moored. Norm-based theories of privacy draw on collectivism. But what are we to make of norms produced in cultures where the politics (or political goals) are dramatically different? We need to acknowledge that there are competing norms—in some cases to achieve the same ends—and only some norms are articulated in the system. This is because norm-based theories are grounded in shared understanding of only those with legitimate access to these platforms. Contexts reflect a world of privilege in design and discourse, and thus require identity- and political-based approaches. Intersectional frames bring together identities and structures of power and queer-Marxism a "material matrix" and politics of identity; together, we argue, they are best-equipped to deal with this privacy landscape.

Positionality

Both authors are privacy researchers with a critical orientation to this space. To adopt and practice intersectionality or critical identity theory, one has to come to terms with their own positionality. As white women scholars who are neither black nor queer, we acknowledge that our role in pointing out where our privacy theories are potentially hegemonic and oppressive, while perhaps helpful, is also problematic. For instance, we take care to credit our ideas to the scholars on whom our work is built, to translate our ideas to concrete suggestions, and to be wary of how our own efforts to contribute may perpetuate the very problems we are seeking to expose and solve: erasure or marginalization, complexity of lived experiences, and the role of norms and power in subjugating vulnerable people.

ACKNOWLEDGEMENTS

This work was supported in part by the National Science Foundation grant CNS-1703736. Thank you to Jina Huh-Yoo for valuable feedback on early drafts of this paper.

REFERENCES

[1] Ackerman, M.S. and Mainwaring, S.D. 2005. Privacy issues and human-computer interaction. *Computer*. 27, 5 (2005), 19–26.

[2] Acquisti, A. and Gross, R. 2006. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. *PETS* (2006), 36–58.

[3] Acquisti, A. and Grossklags, J. 2004. Privacy attitudes and privacy behavior: Losses, gains, and hyperbolic discounting. *The economics of information security*. Kluwer Academic Publishers. 1–15.

[4] Altman, I. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Brooks/Cole.

[5] Andalibi, N., Haimson, O.L., De Choudhury, M. and Forte, A. 2016. Understanding Social Media Disclosures of Sexual Abuse Through the Lenses of Support Seeking and Anonymity. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2016), 3906–3918.

[6] Anjum, B. 2018. An Interview with Pamela Wisniewski: Making the Online World Safer for Our Youth. *Ubiquity*. 2018, December (Dec. 2018), 2:1–2:6. DOI:https://doi.org/10.1145/3301323.

[7] Badillo-Urquiola, K., Page, X. and Wisniewski, P. 2019. Risk vs. Restriction: The Tension between Providing a Sense of Normalcy and Keeping Foster Teens Safe Online. *The ACM CHI Conference on Human Factors in Computing Systems* (2019).

[8] Bardzell, S. 2010. Feminist HCI: Taking Stock and Outlining an Agenda for Design. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2010), 1301–1310.

[9] Barnes, S.B. 2006. A privacy paradox: Social networking in the United States. *First Monday*. 11, 9 (Sep. 2006).

[10] Bernstein, M.S., Bakshy, E., Burke, M. and Karrer, B. 2013. Quantifying the Invisible Audience in Social Networks. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2013), 21–30.

[11] Blackwell, L., Dimond, J., Schoenebeck, S. and Lampe, C. 2017. Classification and Its Consequences for Online Harassment: Design Insights from HeartMob. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW (Dec. 2017), 24:1–24:19.

[12] Blackwell, L., Hardy, J., Ammari, T., Veinot, T., Lampe, C. and Schoenebeck, S. 2016. LGBT Parents and Social Media: Advocacy, Privacy, and Disclosure During Shifting Social Movements. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2016), 610–622.

[13] Bowser, A., Shilton, K., Preece, J. and Warrick, E. 2017. Accounting for Privacy in Citizen Science: Ethical Research in a Context of Openness. *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (New York, NY, USA, 2017), 2124–2136.

[14] boyd, danah 2014. *It's Complicated: The Social Lives of Networked Teens*. Yale University Press.

[15] Bridges, K.M. 2017. *The Poverty of Privacy Rights*. Stanford Law Books.

[16] Cate, F.H. 2010. The Limits of Notice and Choice. *IEEE Security Privacy*. 8, 2 (Mar. 2010), 59–62. DOI:https://doi.org/10.1109/MSP.2010.84.

[17] Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., Levy, K., Dell, N., McCoy, D. and Ristenpart, T. 2018. The Spyware Used in Intimate Partner Violence. *2018 IEEE Symposium on Security and Privacy (SP)* (May 2018), 441–458.

[18] Collins, P.H. 2019. *Intersectionality as Critical Social Theory*. Duke University Press Books.

[19] Collins, P.H. 2015. Intersectionality's Definitional Dilemmas. *Annual Review of Sociology*. 41, 1 (2015), 1–20.

[20] Collins, P.H. and Bilge, S. 2016. *Intersectionality*. Polity.

[21] Crenshaw, K. 1989. Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine. *University of Chicago Legal Forum*. 1989, 1 (1989).

[22] Domestic Abuse Survivors Go "Underground" With the Tor Network: 2014. *http://www.adweek.com/digital/domestic-abuse-survivors-go-underground-tor-network/*. Accessed: 2017-08-31.

[23] Dourish, P. 2001. Seeking a Foundation for Context-Aware Computing. *Human–Computer Interaction*. 16, 2–4 (Dec. 2001), 229–241.

[24] Dym, B. and Fiesler, C. 2018. Vulnerable and Online: Fandom's Case for Stronger Privacy Norms and Tools. *Companion of the 2018 ACM Conference on Computer Supported Cooperative Work and Social Computing* (New York, NY, USA, 2018), 329–332.

[25] Ekbia, H. and Nardi, B. 2016. Social Inequality and HCI: The View from Political Economy. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2016), 4997–5002.

[26] Encryption Is a Luxury: 2016. *https://www.theatlantic.com/technology/archive/2016/03/the-digital-security-divide/475590/*. Accessed: 2019-08-12.

[27] Eubanks, V. 2018. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press.

[28] Forte, A., Andalibi, N. and Greenstadt, R. 2017. Privacy, Anonymity, and Perceived Risk in Open Collaboration: A Study of Tor Users and Wikipedians. *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (New York, NY, USA, 2017), 1800–1811.

[29] Foucault, M. 1977. *Discipline & Punish: The Birth of the Prison*. Vintage Books.

[30] Foucault, M. 1976. *The History of Sexuality, Vol. 1: An Introduction*. Vintage.

[31] Fox, S., Menking, A., Steinhardt, S., Hoffmann, A.L. and Bardzell, S. 2017. Imagining Intersectional Futures: Feminist Approaches in CSCW. *Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (New York, NY, USA, 2017), 387–393.

[32] Fox, S., Menking, A., Steinhardt, S., Hoffmann, A.L. and Bardzell, S. 2017. Imagining Intersectional Futures: Feminist Approaches in CSCW. *Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (New York, NY, USA, 2017), 387–393.

[33] Fraser, N., Bhattacharya, T. and Arruzza, C. 2019. *Feminism for the 99%*. Verso.

[34] Fratantonio, Y., Qian, C., Chung, S.P. and Lee, W. 2017. Cloak and Dagger: From Two Permissions to Complete Control of the UI Feedback Loop. *2017 IEEE Symposium on Security and Privacy (SP)* (May 2017), 1041–1057.

[35] Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T. and Dell, N. 2018. A Stalker's Paradise: How Intimate Partner Abusers Exploit Technology. (2018), 1–13.

[36] Gandy, O.H. 2017. Surveillance and the Formation of Public Policy. *Surveillance & Society Biennial Conference* (2017).

[37] Gavison, R. 1992. Feminism and the Public/Private Distinction. *Stanford Law Review*. 45, 1 (1992), 1–45. DOI:https://doi.org/10.2307/1228984.

[38] Goffman, A. 2014. *On the Run: Fugitive Life in an American City*. University of Chicago Press.

[39] Gray, M.L. 2009. *Out in the Country: Youth, Media, and Queer Visibility in Rural America*. NYU Press.

[40] Gross, R. and Acquisti, A. 2005. Information Revelation and Privacy in Online Social Networks. *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society* (New York, NY, USA, 2005), 71–80.

[41] Guberek, T., McDonald, A., Simioni, S., Mhaidli, A.H., Toyama, K. and Schaub, F. 2018. Keeping a Low Profile?: Technology, Risk and Privacy Among Undocumented Immigrants. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2018), 114:1–114:15.

[42] Gurses, S. and Hoboken, J. van 2016. Privacy after the Agile Turn. (Aug. 2016).

[43] Hancock, A.-M. 2016. *Intersectionality: An Intellectual History*. Oxford University Press.

[44] Hao, K. 2018. Amazon is the invisible backbone behind ICE's immigration crackdown. *MIT Technology Review*.

[45] Hargittai, E. and Marwick, A. 2016. "What can I really do?" Explaining the privacy paradox with onine apathy. *International Journal of Communication*. 10, (2016), 3737–3757.

[46] Hartsock, N.C. 1983. The Feminist Standpoint: Developing the Ground for a Specifically Feminist Historical Materialism. *Discovering Reality*. Reidel Publishing Company. 283–310.

[47] Hoofnagle, C. and Urban, J. 2014. Alan Westin's Privacy Homo Economicus. *Wake Forest Law Review*. (Jun. 2014), 261.

[48] Hornung, D., Müller, C., Shklovski, I., Jakobi, T. and Wulf, V. 2017. Navigating Relationships and Boundaries: Concerns Around ICT-uptake for Elderly People. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2017), 7057–7069.

[49] Hull, G. 2015. Successful Failure: What Foucault Can Teach Us About Privacy Self-Management in a World of Facebook and Big Data. *Ethics and Information Technology*. 17, 2 (2015), 89–101.

[50] Igo, S.E. 2018. *The Known Citizen: A History of Privacy in Modern America*. Harvard University Press.

[51] Is China's social credit system as Orwellian as it sounds? *https://www.technologyreview.com/f/613027/chinas-social-credit-system-isnt-as-orwellian-as-it-sounds/*. Accessed: 2019-07-31.

[52] Jernigan, C. and Mistree, B.F.T. 2009. Gaydar: Facebook friendships expose sexual orientation. *First Monday*. 14, 10 (Sep. 2009). DOI:https://doi.org/10.5210/fm.v14i10.2611.

[53] Kang, R., Brown, S. and Kiesler, S. 2013. Why Do People Seek Anonymity on the Internet?: Informing Policy and Design. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2013), 2657–2666.

[54] 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*. 0, 0 (2019).

[55] Kobie, N. 2019. The complicated truth about China's social credit system. *Wired UK*.

[56] Kosinski, M., Stillwell, D. and Graepel, T. 2013. Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*. 110, 15 (Apr. 2013), 5802–5805. DOI:https://doi.org/10.1073/pnas.1218772110.

[57] Kulwin, N. 2019. Shoshana Zuboff Talks Surveillance Capitalism's Threat to Democracy. *New York Magazine*.

[58] Kumar, N. and Karusala, N. 2019. Intersectional Computing. *Interactions*. 26, 2 (Feb. 2019), 50–54.

[59] Lampinen, A., Lehtinen, V., Lehmuskallio, A. and Tamminen, S. 2011. We're in It Together: Interpersonal Management of Disclosure in Social Network Services. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2011), 3217–3226.

[60] Lampinen, A., Tamminen, S. and Oulasvirta, A. 2009. All My People Right Here, Right Now: Management of Group Co-presence on a Social Networking Site. *Proceedings of the ACM 2009 International Conference on Supporting Group Work* (New York, NY, USA, 2009), 281–290.

[61] Lampinen, A., Tamminen, S. and Oulasvirta, A. 2009. All My People Right Here, Right Now: Management of Group Co-presence on a Social Networking Site. *Proceedings of the ACM 2009 International Conference on Supporting Group Work* (New York, NY, USA, 2009), 281–290.

[62] Lanier, J. 2014. *Who Owns the Future?*. Simon & Schuster.

[63] Latour, B. 2018. *Down to Earth: Politics in the New Climatic Regime*. Polity.

[64] Laufer, R.S. and Wolfe, M. 1977. Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues*. 33, 3 (Jul. 1977), 22–42.

[65] Lewis, H. 2016. *The Politics of Everybody: Feminism, Queer Theory and Marxism at the Intersection*. Zed Books.

[66] Madden, M. 2017. *Privacy, Security, and Digital Inequality*.

[67] Madden, M., Gilman, M., Levy, K. and Marwick, A. 2017. Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans. *Washington University Law Review*. 95, 1 (Jan. 2017), 053–125.

[68] Madejski, M., Johnson, M. and Bellovin, S.M. 2012. A study of privacy settings errors in an online social network. *2012 IEEE International Conference on Pervasive Computing and Communications Workshops* (Mar. 2012), 340–345.

[69] Marwick, A. 2012. The Public Domain: Surveillance in Everyday Life. *Surveillance & Society*. 9, 4 (Jun. 2012), 378–393.

[70] Marwick, A. and boyd, danah 2010. I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, and the Imagined Audience. *New Media & Society*. (2010).

[71] Marwick, A., Fontaine, C. and boyd, danah 2017. "Nobody Sees It, Nobody Gets Mad": Social Media, Privacy, and Personal Responsibility Among Low-SES Youth. *Social Media + Society*. 3, 2 (Apr. 2017).

[72] Marwick, A.E. and boyd, danah 2014. Networked privacy: How teenagers negotiate context in social media. *New Media & Society*. 16, 7 (Nov. 2014), 1051–1067.

[73] Marwick, A.E. and Boyd, D. 2018. Privacy at the Margins| Understanding Privacy at the Margins—Introduction. *International Journal of Communication*. 12, 0 (Mar. 2018), 9.

[74] Matthews, T., O'Leary, K., Turner, A., Sleeper, M., Woelfer, J.P., Shelton, M., Manthorne, C., Churchill, E.F. and Consolvo, S. 2017. Stories from Survivors: Privacy & Security Practices when Coping with Intimate Partner Abuse. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2017), 2189–2201.

[75] McDonald, N., Mako Hill, B., Greenstadt, R. and Forte, A. 2019. Privacy, Anonymity, and Perceived Risk in Open Collaboration: A Study of Service Providers. *CHI* (New York, NY, USA, 2019).

[76] Mulligan, D. and King, J. 2011. Bridging the Gap between Privacy and Design. *University of Pennsylvania Journal of Constitutional Law*. 14, (Jan. 2011), 989.

[77] Nardi, B.A. 1996. Studying context: A comparison of activity theory, situated action models, and distributed cognition. *Context and consciousness: Activity theory and human–computer interaction*. The MIT Press. 69–102.

[78] Netter, M., Riesner, M., Weber, M. and Pernul, G. 2013. Privacy Settings in Online Social Networks -- Preferences, Perception, and Reality. *Proceedings of the Hawaii international Conference on System Sciences HICSS'13* (2013), 3219–3228.

[79] 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 (2014).

[80] Nissenbaum, H. 2004. Privacy as Contextual Integrity. *Washington Law Review*. 79, 1 (2004), 101–139.

[81] Nissenbaum, H. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

[82] Norberg, P.A., Horne, D.R. and Horne, D.A. 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*. 41, 1 (Jun. 2007), 100–126.

[83] Okin, S.M. 1989. *Justice, gender, and the family*. Basic Books.

[84] Onuma, M., Kimura, A. and Mukawa, N. 2013. Exploring Social Cognition Related to Privacy Settings in SNS Usage. *Proceedings of the 2013 International Conference on Signal-Image Technology & Internet-Based Systems* (Washington, DC, USA, 2013), 1077–1082.

[85] Orend, B. 2001. Walzer's General Theory of Justice. *Social Theory and Practice*. 27, 2 (2001), 207–229.

[86] Palen, L. and Dourish, P. 2003. Unpacking "Privacy" for a Networked World. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2003), 129–136.

[87] Pearce, K.E., Vitakm, J. and Barta, K. 2018. Socially Mediated Visibility: Friendship and Dissent in Authoritarian Azerbaijan. *International journal of communication (Online)*. (Mar. 2018), 1310-.

[88] Pierce, J., Fox, S., Merrill, N. and Wong, R. 2018. Differential Vulnerabilities and a Diversity of Tactics: What Toolkits Teach Us About Cybersecurity. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW (Nov. 2018), 139:1–139:24. DOI:https://doi.org/10.1145/3274408.

[89] Pitcan, M., Marwick, A.E. and Boyd, D. 2018. Performing a Vanilla Self: Respectability Politics, Social Class, and the Digital World. *Journal of Computer-Mediated Communication*. 23, 3 (May 2018), 163–179. DOI:https://doi.org/10.1093/jcmc/zmy008.

[90] Rankin, Y.A. and Thomas, J.O. 2019. Straighten Up and Fly Right: Rethinking Intersectionality in HCI Research. *Interactions*. 26, 6 (Oct. 2019), 64–68.

[91] Richardson, J. 2014. Spinoza, Feminism and Privacy: Exploring an Immanent Ethics of Privacy. *Feminist Legal Studies; Dordrecht*. 22, 3 (Dec. 2014), 225–241.

[92] Rosenblat, A., Kneese, T. and boyd, danah 2014. WorkplaceSurveillance. *Data & Society Working Paper*. (2014), 19.

[93] Scheuerman, M.K., Branham, S.M. and Hamidi, F. 2018. Safe Spaces and Safe Places: Unpacking Technology-Mediated Experiences of Safety and Harm with Transgender People. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW (Nov. 2018), 155:1–155:27.

[94] Schlesinger, A., Edwards, W.K. and Grinter, R.E. 2017. Intersectional HCI: Engaging Identity Through Gender, Race, and Class. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2017), 5412–5427.

[95] Selinger, E. and Hartzog, W. 2014. *Obscurity and Privacy*. Technical Report #ID 2439866. Social Science Research Network.

[96] Sleeper, M., Matthews, T., O'Leary, K., Turner, A., Woelfer, J.P., Shelton, M., Oplinger, A., Schou, A. and Consolvo, S. 2019. Tough Times at Transitional Homeless Shelters: Considering the Impact of Financial Insecurity on Digital Security and Privacy. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2019), 89:1–89:12.

[97] Stutzman, F. and Hartzog, W. 2012. Boundary Regulation in Social Media. *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work* (New York, NY, USA, 2012), 769–778.

[98] Thomas, J.O., Joseph, N., Williams, A., Crum, C. and Burge, J. 2018. Speaking Truth to Power: Exploring the Intersectional Experiences of Black Women in Computing. *2018 Research on Equity and Sustained Participation in Engineering, Computing, and Technology (RESPECT)* (Feb. 2018), 1–8.

[99] Trappenburg, M. 2000. In Defence of Pure Pluralism: Two Readings of Walzer's Spheres of Justice. *Journal of Political Philosophy*. 8, 3 (2000), 343–362. DOI:https://doi.org/10.1111/1467-9760.00106.

[100] Tufekci, Z. 2007. Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology & Society*. 28, 1 (2007), 20–36.

[101] Tufekci, Z. 2017. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. Yale University Press.

[102] Tufekci, Z. 2017. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. Yale University Press.

[103] Vitak, J., Blasiola, S., Patil, S. and Litt, E. 2015. Balancing Audience and Privacy Tensions on Social Network Sites: Strategies of Highly Engaged Users. *International Journal of Communication*. 9, 0 (May 2015), 20.

[104] 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. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW (Nov. 2018), 176:1–176:25.

[105] Walzer, M. 1984. *Spheres Of Justice: A Defense Of Pluralism And Equality*. Basic Books.

[106] 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. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW (Nov. 2018), 181:1–181:22.

[107] Westin, A.F. 1967. *Privacy and Freedom*. Atheneum.

[108] Wisniewski, P., Ghosh, A.K., Xu, H., Rosson, M.B. and Carroll, J.M. 2017. Parental Control vs. Teen Self-Regulation: Is There a Middle Ground for Mobile Online Safety? *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (New York, NY, USA, 2017), 51–69.

[109] Wisniewski, P., Islam, A.K.M.N., Knijnenburg, B.P. and Patil, S. 2015. Give Social Network Users the Privacy They Want. *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (New York, NY, USA, 2015), 1427–1441.

[110] Wisniewski, P., Lipford, H. and Wilson, D. 2012. Fighting for My Space: Coping Mechanisms for Sns Boundary Regulation. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2012), 609–618.

[111] Wisniewski, P.J., Kumar, N., Bassem, C., Clinch, S., Dray, S.M., Fitzpatrick, G., Lampe, C., Muller, M. and Peters, A.N. 2018. Intersectionality As a Lens to Promote Equity and Inclusivity Within SIGCHI. *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2018).

[112] Woodruff, A., Pihur, V., Consolvo, S., Schmidt, L., Brandimarte, L. and Acquisti, A. 2014. Would a Privacy Fundamentalist Sell Their DNA for $1000... If Nothing Bad Happened As a Result? The Westin Categories, Behavioral Intentions, and Consequences. *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security* (Berkeley, CA, USA, 2014), 1–18.

[113] Zuboff, S. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.