International Journal of Communication 12(2018), 1157–1165 1932–8036/20180005

Understanding Privacy at the Margins

Introduction

ALICE E. MARWICK[1]
University of North Carolina at Chapel Hill
Data & Society, USA

DANAH BOYD
Microsoft Research
Data & Society, USA

Although privacy and surveillance affect different populations in disparate ways, they are often treated as monolithic concepts by journalists, privacy advocates, and researchers. Achieving privacy is especially difficult for those who are marginalized in other areas of life. This special section interrogates what privacy looks like at the margins, investigating a broad spectrum of issues, methodologies, and contexts. Many make an intervention into mainstream theories of privacy and surveillance, showing how examining the experiences of individuals outside the normative White, American, middle-class subject often complicates assumptions about how privacy operates. Others examine the mundane and the banal to analyze how power relations play out in everyday life. By incorporating research outside the canon of privacy research, and by advocating for projects that discuss more diverse conceptualizations of "the user" or the subject, we can envision a future for privacy scholarship that incorporates a wider set of harms and needs and encompasses the concerns of a larger base of citizens.

Keywords: privacy, socioeconomic status, marginalization, networked privacy

Alice E. Marwick: amarwick@unc.edu
danah boyd: danah@datasociety.net
Date submitted: 2018–02–05

[1] Our recent work on privacy at the margins was made possible by a grant from the Digital Trust Foundation. We have had the great fortune of being surrounded by a cohort of scholars who are working hard to increase the diversity of concerns represented by privacy scholarship. Many of them served as referees and advisors for this special section and we are deeply grateful for them. We also want to thank attendees of the first Data & Society workshop where scholars workshopped different papers related to privacy at the margins, including two represented in this special section. Thank you also to Brittany Keppel for helping us organize this project.

Privilege and Privacy

The word *privilege* is etymologically linked to the Latin concept of *privilegium*, which comprises two roots meaning *private* and *law*. In effect, the notion of privilege is the idea of a particular law or policy that benefits or harms an individual. The concept of "privacy" is predicated on the idea that a private individual deserves to be "let alone" from being observed or disturbed by others (Warren & Brandeis, 1890). Yet, in practice, the ability to achieve privacy often requires the privilege to make choices and create structures that make such freedoms possible.

Together, we have interviewed and observed countless teens and young adults as they struggle to achieve privacy in a networked age. Many people choose to participate in social media, carry cell phones, and engage in other online activities knowing full well that their data are being collected, their actions are being monitored, and their online experiences are being algorithmically generated and personalized. Journalists and technology leaders often use everyday people's engagement with social technologies as "proof" that people do not care about privacy. Yet, we have consistently found that people care deeply about privacy and develop innovative strategies to achieve privacy while participating in the systems that allow them to access information, socialize with friends, and interact with contemporary entertainment platforms (boyd, 2014; boyd & Marwick, 2011; Marwick & boyd, 2014; Marwick, Fontaine, & boyd, 2017). For many people, privacy is not simply the ability to restrict access to information, but the ability to strategically control a social situation by influencing what information is available to others, how this information is interpreted, and how it will spread. Needless to say, networked technology complicates these dynamics, to the point where most people find themselves constantly negotiating between disclosure, concealment, and connection.

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. Meanwhile, privacy is increasingly important as data-hungry algorithmic systems are introduced into every part of society, gobbling up data about people and their practices to feed decision-making systems in sectors as varied as criminal justice, advertising, transportation, and news delivery. The privilege to "opt out" of these data-oriented systems is increasingly unattainable.

How data are collected is important, as it illuminates many contemporary tensions around privacy and privilege. The tech industry often frames its products as a give-and-take between people willingly sharing personal information in exchange for benefits. Although there are plenty of people who approach specific services with a mind-set that they are intentionally choosing to do so—for instance, providing an e-mail address in exchange for a coupon—a great deal of information is not collected from truly informed and consenting individuals. (Often, people do not even know that their data are being collected.) On the other end of the spectrum, there are countless situations in which individuals are required to provide data as a condition of employment, to receive social services, or to avoid financial ruin or imprisonment. For instance, in the United States, employers regularly require credit reports for low-wage positions such as telemarketing, retail, and home health care, despite the fact that credit records have little or no bearing

on a person's job performance (Traub, 2013). Those who are coerced into providing data are far more likely to be at the margins than those who choose to provide data. Most people's experiences do not reflect either extreme. Instead, our data enter into the digital stream as a byproduct of our participation in contemporary life. We live in a data-by-circumstance world, and so we simply hold our breath, hoping that the companies we trust with our data will not undermine us.

As data-based systems become increasingly ubiquitous, and companies that people entrust frequently fail to protect personal data, the lines between choice, circumstance, and coercion grow increasingly blurry. Instead, what becomes most important is that how much privilege individuals have significantly affects their ability to weather the storm presented by a data breach or data abuse. Privacy scholarship has significantly increased alongside the rise of data-driven technologies, with legal scholars and humanists working with social scientists and computer scientists to interrogate what privacy means, how people experience privacy, and what technical and legal structures are needed to protect privacy. Yet, by and large, most of this work has treated people universally, under the assumption that all people experience privacy equally. Given our work with young people marginalized by a wide variety of circumstances, we question that assumption.

Where Is the Margin?

Privacy law and privacy technology are significantly intertwined. At the same time, most work in this area is distinctly Western and predominantly American and European. Yet, as Irving Altman (1977) showed in his analysis of anthropological studies, expectations of privacy differ from culture to culture. But this is rarely taken into account in privacy scholarship. Partly this is because most privacy scholarship comes from the law and computer science, each of which has its own reasons for presuming a universal subjectivity. Partly this is because U.S. companies create many problematic and worrisome technologies. Western laws typically define mechanisms of data protection, which are formalized and instantiated into code by technology companies. But primarily, this is because—like much academic work—privacy scholarship is overwhelmingly written in English and biased toward the United States, which is far from a universal context (e.g., although citizens of many countries have a right to free speech, the way that Internet companies such as Reddit and Twitter understand and implement it is very much linked to neoliberal Silicon Valley ideologies, with complex ramifications). Ultimately, although privacy and surveillance affect different populations in disparate ways, they are often treated as monolithic concepts by journalists, privacy advocates, and researchers.

Not only does privacy differ across broad national and linguistic cultural differences, but it also differs within communities depending tremendously on context, subject position, and the dynamics of any given interaction. In short, the role of power is ever present. Whole classes of people who have been systematically and structurally marginalized (e.g., LGBTQ communities, people of color, immigrants, low-income communities, people with disabilities, youth and elders, and those from religious minorities, to name but a few) experience privacy differently from those who hold some semblance of privilege within a given society. Consider Khiara M. Bridges' (2017) argument in *The Poverty of Privacy Rights*. In it, she provides the example of a pregnant woman, "Erica," seeking public assistance. In the process of obtaining benefits, Erica is interviewed by a social worker, who is required to ask a series of questions about her

romantic relationships, history with drugs and alcohol, and experiences with domestic violence and sexual assault. The supposed reason for such intrusive questioning is to protect Erica's child. However, the questions do not focus on Erica's preparedness for motherhood or her plans for feeding or clothing her child. Instead, Bridges argues, they presume that Erica is a particular kind of person, a morally suspect individual, and that she is poor because of this. As Virginia Eubanks (2018) details in *Automating Inequality*, such data are increasingly fed into automated systems that make decisions about social services with enormous impacts, but little opacity or process for appeal. These systems amplify the inequalities and disempowerment that poor people face and make privacy violations such as Erica's virtually impossible to avoid.

Individuals' relationship to privacy can also change significantly depending on their context and the social dynamics at play. When people are ill and at risk of losing health insurance, the way they think about and value their health data changes radically compared with when they are healthy. Women who are facing the abuse of a stalker find themselves in a fundamentally different position from those without such a threat. All too often, technology simply mirrors and magnifies these problems, increasing the pain felt by the target of a stalker or the likelihood that the health data of a sick person will end up limiting access to health care. Needless to say, those who are multiply marginalized face even more intense treatment.

Although the contemporary conversation about privacy is intimately intertwined with digital technologies, the concerns and realities of people's privacy experience are not solely about the digital domain. Physical space and the built environment deeply affect how people experience and understand privacy. For example, in a recent study, we interviewed low-income young people in the New York City area about their privacy experiences. Having grown up under stop-and-frisk, our participants, most of whom were Black or Brown, often experienced privacy violations most viscerally through police surveillance (Marwick et al., 2017). When talking to teenagers many years ago, we often heard stories about parents or siblings searching dressers or backpacks (boyd, 2014; boyd & Marwick, 2011). Yet, when people are asked about privacy, they often default to conversations about online privacy. Given that scholars no longer consider the online and offline separate realms (Baym, 2010), privacy must be considered through a rich tapestry of objects, interactions, and processes that span the digital and the analog, the face-to-face, and the virtual.

The Special Section

The purpose of this special section is to interrogate what privacy looks like at the margins. The articles collected in this special section cover a broad spectrum of issues, methodologies, and contexts. Many make an intervention into mainstream theories of privacy and surveillance, showing how examining the experiences of individuals outside the often-studied White, American, middle-class subject often complicates our assumptions about how privacy operates. Others examine the mundane and the banal to analyze how power relations play out in everyday life. By incorporating research outside the canon of privacy research, and by advocating for projects that discuss more diverse conceptualizations of "the user" or the subject, we can envision a future for privacy scholarship that incorporates a wider set of harms and needs and encompasses the concerns of a larger base of citizens.

Karen Levy and Solon Barocas's "Refractive Surveillance: Monitoring Customers to Manage Workers" develops a new framework of surveillance, *refractive surveillance*, that incorporates the social dimensions of privacy, recent critiques of the dyadic model of surveillance, and social and economic justice. This framework is explicated through an examination of various customer-monitoring technologies deployed in low-wage retail work. New developments such as sensors and cameras, designed to make up for the relative lack of customer data collected in brick-and-mortar stores when compared with online shopping, deeply impact retail workers. Levy and Barocas demonstrate how data collection from customers affords greater surveillance of workers, making schedules less stable and predictable, intensifying tracking and evaluation, facilitating automation, and contributing to deskilling. Refractive surveillance suggests that information collected about one group can deeply impact another, a useful finding in the age of big data and networked privacy.

In "Not the Normal Trans Story: Negotiating Trans Narratives While Crowdfunding at the Margins," Niki Fritz and Amy Gonzales interview trans people who have used crowdfunding sites to raise money for top surgery. Crowdfunding sites often prompt users to share personal information to create affective ties between audience and subject (in practice, to encourage people to donate money), but trans bodies and identities are often stigmatized and understood in simple or binary terms rather than as fluid or complex. Fritz and Gonzales draw from privacy calculus theory, which frames online information provision as a trade-off for economic or social benefits. Although trans individuals are often at risk when disclosing personal information, Fritz and Gonzales's participants had to do so to create affective ties with audiences. They found that, because trans people often negotiate complicated privacy concerns in daily life, online and offline privacy concerns were intimately intertwined. Some of their participants found it empowering to tell their narratives in their own words, and many positively experienced gains in social support. Thus, both the perceived risks and the actual support were greater than expected.

Larissa Hjorth, Sarah Pink, and Heather Horst's article "Being at Home With Privacy: Privacy and Mundane Intimacy Through Same-Sex Locative Media Practices" draws on ethnographic research in Melbourne, Australia, to examine how locative technologies contribute to intimacy work in the lives of two Australian female same-sex couples. Focused on the daily rhythms of the couples, the authors define privacy as a process key to the boundary work necessary to create and maintain affective closeness, especially salient to women, who often bear the burden of emotional labor. For the authors' participants, locative technologies were tied to safety and mitigation of risk, but also were deeply imbricated in intimacy. For example, one participant used her account to book Uber rides for her partner, which enabled her to track the car moving and ensure that her partner arrived at her destination and was safe. In other cases, participants chose to take selfies, post about their relationship, or "check in" to create and maintain intimate ties. The constant trade-off between disclosure and privacy, both of which could maintain or threaten intimacy, is characterized by the authors as *careful surveillance*, which illustrates "the way we monitor and watch our intimates as cohabitants subject to our care. Yet, it also deliberately implies that surveillance should be a careful practice, one that we consider very carefully in terms of its impact on others" (Hjorth, Pink, & Horst, this Special Section). Like Levy and Barocas's article, Hjorth and colleagues push back against a simple dyadic concept of surveillance by building on findings from work by Lauren Berlant (2011), Melissa Gregg (2013), and others who have theorized the relationship between publicity, privacy, and affect.

Taking a much more expansive approach, "The Poverty of Privacy: Understanding Privacy Trade-Offs From Identity Infrastructure Users in India" by Janaki Srinivasan, Savita Bailur, Emrys Schoemaker, and Sarita Seshagiri reflects findings from a large-scale qualitative study of how low-income Indians experience Aadhaar, India's enormous biometric national identification system. Drawing from 150 interviews in three Indian states, the study asks how low-income users, who are often forced to participate in intrusive bureaucratic systems to receive benefits from the state, negotiate the new digital forms of identity infrastructures. The participants articulate a variety of relationships with the state and use various creative, culturally specific strategies to maintain their privacy and security in the face of state requirements. For instance, one female participant resisted having her photograph taken for her ration card (her privacy norms included wearing a veil and restricting relationships with men), which she circumvented by having her picture and fingerprints taken by women and using her husband and son's mobile number instead of her own. Many participants used a privacy calculus approach to decide whether to disclose information, weighing both the perceived benefits and the justification for data. They considered privacy to be relative, rather than simply present or absent, important, or unimportant. Such a nuanced approach to privacy attitudes interrogates how participants came to the choices they made vis-à-vis disclosure or concealment, rather than attempting to measure a nebulous privacy concern.

Taking a similar ethnographic approach to privacy, but in a completely different context, is "Technology in Rural Appalachia: Cultural Strategies of Resistance and Navigation," by Sherry Hamby, Elizabeth Taylor, Allison Smith, Kimberly Mitchell, and Lisa Jones. The authors examine privacy attitudes and practices in Appalachia, a poor, rural part of the United States with a very distinct culture. Appalachian people are often stereotyped as drunk, lazy, and "backwards," and are understudied and frequently misunderstood. By using a sociocultural approach, the authors examine how the core Appalachian values of privacy, kinship networks, self-reliance, and humility affect Appalachian people's relationships with digital technologies. Many participants were reluctant technology adopters, and used self-deprecating humor to justify and frame their interactions with technologies. Others expressed concerns that technology would erode the self-reliance so important to the area. As in the Aadhaar study, the participants used a variety of very creative privacy-protective strategies that were entirely specific to the cultural context; one man impressed a focus group when he described posing as an FBI agent to scare away telephone scam artists. Hamby et al. find that their participants drew from Appalachian discursive resources to resist the encroachment of digital materialism writ large, posing a counternarrative to the idea of technology as intrinsically beneficial and progressive. Thus, they reasserted their agency in a way congruent with their cultural contexts.

Focusing on a more urban context, Xiaoqian Li, Wenhong Chen, and Joseph Straubhaar's "Concerns, Skills, and Activities: Multilayered Privacy Issues in Disadvantaged Urban Communities" is a quantitative examination of the privacy experiences of public housing residents in a major U.S. city. Unlike broader nonusers of the Internet, those in this study—who were disproportionately likely to not be online—included privacy and safety as one of their top reasons for opting out. Multiply marginalized individuals had lower levels of digital privacy-protecting skills, but those with higher levels of skills participated in privacy-compromising digital activities more often. Because digital inclusion is often seen as an inherently beneficial goal, the complicated interplay between privacy and participation is often

overlooked. Yet, this study highlights how privacy concerns inhibit participation while privacy-protecting skills interact with Internet access quality to buffer those who do participate from risky behaviors that might affect their outcomes in significant ways.

In "Privacy Versus Relatedness: Managing Device Use in Australia's Remote Aboriginal Communities," Ellie Rennie, Indigo Holcombe-James, and Tyson Yunkaporta describe another way in which privacy concerns can result in digital exclusion. While mobile phones are disrupting a variety of norms and practices around the world, the social unrest and interpersonal conflict that are emerging in Aboriginal Australia pit Western values against native paradigms. Technologies are designed to focus on individual access and control. This is both undone by and the undoing of norms within the Aboriginal context. Not only do Aboriginal peoples share mobile devices instead of treating them as the property of individuals, but their approach to privacy recognizes communal interests more centrally than Western society. In a culture in which the social is rooted in relatedness rather than conceptions of individual selves interacting, practices of negotiating individual profiles and personal privacy setting make little sense. By upending the individualistic-centric ideas of privacy, this article highlights how privacy as it is instantiated by technology often extends the colonial work of Western powers while appearing to be working on behalf of individuals.

Katy Pearce, Jessica Vitak, and Kristen Barta's "Socially Mediated Visibility: Friendship and Dissent in Authoritarian Azerbaijan" approaches the question of privacy in a context in which those with marginalized political views often struggle to strategically navigate visibility while sharing political views through social media. Drawing on a series of interviews, this article examines the strategies that young Azerbaijani dissidents take to communicate with peers, find like-minded people and receive support, and inform and advocate, while managing the risks of exposure and abuse. The analysis done in this article helps complicate broader assumptions about the implicitly presumed benefits of increased visibility for activists and those seeking to build community. Although many of the dissidents Pearce interviewed were willing to tolerate cruelty and social alienation in return for the benefits they gained by participating in political communities, this article also reveals how technology's empowerment comes with serious costs for those at the margins.

Also challenging common assumptions, "Settler Governance and Privacy: Canada's Indian Residential School Settlement Agreement and the Mediation of State-Based Violence" by Lara Fullenwieder and Adam Molnar examines how the Canadian reconciliation process around the violent and assimilative history of residential schools pits divergent views about privacy against one another. Contrasted against the views of some community members and the goals of self-determination, the liberal privacy approach fostered by the 2007 Indian Residential School Settlement Agreement can also be seen as an expansion of colonialism, reproducing the harms that the reconciliation process is intended to remedy. Rather than empowering Aboriginal people by allowing them to define privacy in their own terms, privacy can exist as an instrument of settler colonialism, governing the rights and freedoms of Indigenous peoples whose stories and records were shared in good faith as part of the reconciliation process. Because self-determination is a central tenet of First Nation people, the dominating Western logic of privacy may not always support Indigenous cultural values and traditions, but serves as a way to make the reconciliation process operate under distinctly Western values.

References

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues*, *33*(3), 66–84.

Baym, N. K. (2010). *Personal connections in the digital age*. Malden, MA: Polity Press.

Berlant, L. G. (2011). *Cruel optimism*. Durham, NC: Duke University Press.

boyd, d. (2014). *It's complicated: The social lives of networked teens*. New Haven, CT: Yale University Press.

boyd, d., & Marwick, A. (2011, September). *Social privacy in networked publics: Teens' attitudes, practices, and strategies*. Presented at A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, Oxford, UK. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128

Bridges, K. M. (2017). *The poverty of privacy rights*. Palo Alto, CA: Stanford University Press.

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. New York, NY: St. Martin's Press.

Fritz, N., & Gonzales, A. (2018). Not the normal trans story: Negotiating trans narratives while crowdfunding at the margins. *International Journal of Communication, 14,* this Special Section.

Fullenwieder, L., & Molnar, A. (2018). Settler governance and privacy: Canada's Indian Residential School Settlement Agreement and the mediation of state-based violence. *International Journal of Communication, 14,* this Special Section.

Gregg, M. (2013). *Work's intimacy*. Malden, MA: Polity Press.

Hamby, S., Taylor, E., Smith, A., Mitchell, K., & Jones, L. (2018). Technology in rural Appalachia: Cultural strategies of resistance and navigation. *International Journal of Communication, 14,* this Special Section.

Hjorth, L., Pink, S., & Horst, H. A. (2018). Being at home with privacy: Privacy and mundane intimacy through same-sex locative media practices. *International Journal of Communication, 14,* this Special Section.

Levy, K., & Barocas, S. (2018). Refractive surveillance: Monitoring customers to manage workers. *International Journal of Communication, 14,* this Special Section.

Li, X., Chen, W., & Straubhaar, J. D. (2018). Concerns, skills, and activities: Multilayered privacy issues in disadvantaged urban communities. *International Journal of Communication, 14,* this Special Section.

Marwick, A., & boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*(7), 1051–1067.

Marwick, A., Fontaine, C., & boyd, d. (2017). "Nobody sees it, nobody gets mad": Social media, privacy, and personal responsibility among low-SES youth. *Social Media & Society, 3*(2). doi:10.1177/2056305117710455

Pearce, K. A., Vitak, J., & Barta, K. (2018). Socially mediated visibility: Friendship and dissent in authoritarian Azerbaijan. *International Journal of Communication, 14,* this Special Section.

Rennie, E., Holcombe-James, I., & Yunkaporta, T. (2018). Privacy versus relatedness: Managing device use in Australia's remote Aboriginal communities. *International Journal of Communication, 14,* this Special Section.

Srinivasan, J., Bailur, S., Schoemaker, E., & Seshagiri, S. (2018). The poverty of privacy: Understanding privacy trade-offs from identity infrastructure users in India. *International Journal of Communication, 14,* this Special Section.

Traub, A. (2013). *Discredited: How employment credit checks keep qualified workers out of a job*. New York, NY: Demos. Retrieved from http://www.demos.org/discredited-how-employment-credit-checks-keep-qualified-workers-out-job

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193–220.