Theme Issue Article

new media & society
2014, Vol. 16(7) 1051–1067

DOI: 10.1177/1461444814543995
nms.sagepub.com

Networked privacy: How teenagers negotiate context in social media

Alice E Marwick
Fordham University, USA

danah boyd
Microsoft Research, USA

Abstract

While much attention is given to young people's online privacy practices on sites like Facebook, current theories of privacy fail to account for the ways in which social media alter practices of information-sharing and visibility. Traditional models of privacy are individualistic, but the realities of privacy reflect the location of individuals in contexts and networks. The affordances of social technologies, which enable people to share information about others, further preclude individual control over privacy. Despite this, social media technologies primarily follow technical models of privacy that presume individual information control. We argue that the dynamics of sites like Facebook have forced teens to alter their conceptions of privacy to account for the networked nature of social media. Drawing on their practices and experiences, we offer a model of networked privacy to explain how privacy is achieved in networked publics.

Keywords

Context collapse, Facebook, privacy, social media, social network sites, teenagers

Introduction

> Waffles: Every teenager wants privacy. Every single last one of them, whether they tell you or not, wants privacy … Just because teenagers use internet sites to connect to other people doesn't mean they don't care about their privacy. We don't tell everybody every single thing

Corresponding author:
Alice E Marwick, Department of Communication and Media Studies, Fordham University, New York, NY 10458, USA.
Email: amarwick@gmail.com

> about our lives. We tell them general information—names, places, what we like to do—but that's general knowledge. That's not something you like to keep private—"Oh, I play games. I better not tell anybody about that." … So to go ahead and say that teenagers don't like privacy is pretty ignorant and inconsiderate honestly, I believe, on the adult's part.

The myth that teenagers do not care about privacy persists, despite evidence that suggests little variation between adults and young people (Hoofnagle et al., 2010; Madden et al., 2013). Almost all American teenagers (95%) are Internet users, and 85% use social media (Lenhart et al., 2011). Parents, journalists, and entrepreneurs often use teens' deep engagement with and willingness to share information on social media as "proof" that they eschew privacy. However, as "Waffles"—a White 17-year-old from North Carolina—explains, online participation does not necessarily indicate that today's teens reject privacy as a value (Livingstone, 2008). Instead, teenagers attempt to simultaneously participate in the networked publics that are foundational to their peer groups while maintaining a degree of privacy. Simply put, they are trying to be *in* public without always *being* public. Their frequent sharing of digital content does not suggest that they share indiscriminately, nor does it mean that what they do share is intended for wide audiences.

New technologies, from closed-circuit television cameras to large databases, have long complicated privacy practices (Solove, 2004). Such technologies shift the information landscape in ways that call into question cultural assumptions and social norms about sharing, visibility, and the very essence of privacy. By helping create "networked publics"—spaces constructed through networked technologies and imagined communities that emerge as a result of the intersection of people, technology, and practice (boyd, 2014)—social media has given people new tools to see and be seen, forcing participants to reassess their personal privacy desires in a highly networked society where sharing is a central component of participation. Although models of data sharing are typically understood through the lens of individual rights and controls, the networked nature of social media means that individuals' experiences with their data are consistently imbricated with others. Given that social media content has the potential to be distributed to enormous online audiences, there is a tendency to argue that the only way to maintain privacy is not to share in the first place. Youth do not approach privacy this way. Instead, they develop innovative mechanisms for achieving privacy in response to the technical architectures and social dynamics that underpin networked publics.

In this article, we interrogate the notion that "teenagers don't care about privacy" by arguing that engagement with social media has shifted conceptions of privacy from an individualistic frame to one that is networked. While social scientists have long argued that privacy is contextual (Altman, 1977; Palen and Dourish, 2003), the individualistic approach promulgated by legal frames and technological implementations has dominated public discourse. Social media-enabled practices require people to contend with the limitations of individual control and address how to actively navigate context when boundaries cannot be taken for granted. We draw on examples from a large-scale ethnographic study of American teenagers to explore what we refer to as *networked privacy*. This article examines both how youth manage privacy in networked publics and how networked data challenges predominant conceptualizations of privacy. We argue that the realities of privacy practice in networked publics reveal the intrinsically contextual

nature of privacy. As a result, legal and technical understandings of online privacy should shift to incorporate networked contexts.

Literature review: Individual and contextual privacy models

Most American legal models of privacy are centered around the individual (Cohen, 2012; Regan, 1995). Privacy law follows a model of liberal selfhood in which privacy is an individual right, and privacy harms are measured by their impact on the individual. For instance, the "reasonable expectation" test established in *Katz vs. US* determines whether or not something violates privacy if the person involved had a personal expectation to be let alone from government intrusion (Wilkins, 1987). The "right to privacy" has been applied widely, including cases involving contraception, health records, and educational records.

This legal model of individual privacy has been extended into the technical context through the concept of "personally identifiable information" (PII). This includes "any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records" (McCallister et al., 2010). Computer scientists have shown that the very concept of "personally identifiable information" is, at best, murky (Sweeney, 2000), as people can be identified even from supposedly anonymized datasets from which PII has been removed (Ohm, 2010). When AOL released anonymized search logs to researchers, reporters manually identified individual users using the contents of web searches (Barbaro and Zeller, 2006). Sophisticated "re-identification" algorithms make this even simpler; as Narayanan and Shmatikov (2010) write, "The versatility and power of re-identification algorithms imply that terms such as 'personally identifiable' and 'quasi-identifier' simply have no technical meaning" (p. 26). Despite the technical problems with PII, in many federal and state statutes, PII is protected while non-PII is not (Schwartz and Solove, 2011).

PII follows a somewhat cybernetic model of communication, in which information like a social security number is a discrete entity moving from actor to actor. This model is often replicated in popular technologies. Most social media sites adhere to "access-control list" models, in which users determine who can get access to certain information. Some, like Facebook and LiveJournal, let users create groups and restrict access to individual pieces of content. For instance, on Facebook, Sophia may have a "colleagues" group and a "family" group; she might share wedding photos with the latter, but not with the former. Sites like Twitter and Instagram approach access-control at the account level. Accounts are public or private; there is either total access or none.

Despite technical models of personal control over discrete bits of information, critical scholarship shows that privacy is intrinsically contextual. Legal theorist Julie Cohen (2012) argues that current legal models of privacy are based on "simplistic models of individual behavior" while "human societies are constituted by webs of cultural and material connections" (pp. 4–5). Anthropologists and sociologists maintain that privacy is a social construct that reflects the values and norms of individuals within cultures, meaning that the ways in which people conceptualize, locate, and practice privacy varies

tremendously (Nippert-Eng, 2010). Altman's (1977) meta-analysis of ethnographic accounts of privacy found that while privacy is a culturally universal process, it manifests quite differently among different cultures. In other words, the ways that people *practice* privacy, including "verbal, non-verbal, environmental, and cultural mechanisms," are highly culturally specific and contextual (p. 82).

Following Altman, Palen and Dourish (2003) conceptualize privacy as a boundary regulation process. They write that "privacy is not about setting rules and enforcing them; rather, it is the continual management of boundaries between different spheres of action and degrees of disclosure within those spheres" (p. 3). Privacy is thus practiced by people in a wide variety of ways, depending on "local physical environment, audience, social status, task or objective, motivation and intention, [and] information technologies in use." This concept of privacy implies a series of strategies that individuals can deploy depending on how appropriate they are to a specific circumstance. Because people vary the way they communicate with others based on context and audience (Goffman, 1959), technologies that make it difficult to understand or regulate boundaries often make managing privacy more difficult. When social technologies cause a collision of information norms—or "context collapse"—people experience them as privacy violations (Marwick and boyd, 2011; Vitak et al., 2012).

Contextual integrity is key to privacy. Helen Nissenbaum (2010) explains that the norms that govern "the flow of personal information in a given context" (p. 127) are dependent on the type of information being shared; the social roles of the sender, subject, and recipient; and how information is transmitted. Someone might be very comfortable disclosing his HIV status to his doctor due to the formal and legal information norms that surround the doctor's office. If the doctor then tells her wife over dinner, it is not the information that has changed, but the context and the audience. The information flows from a context with one set of information norms (the office) to another (the private home), and the individual perceives a privacy violation. While Nissenbaum's model attempts to insert context and collectivity into rights-based models of privacy, acknowledging the reality of information dissemination without consent, it also presumes that the individual in the doctor's office is fully cognizant of the social context in which disclosure takes place. Although the flow of information to another context is where the privacy violation is experienced, individuals' disclosures depend upon their skills to read a social situation and their perception of context. This can be challenging in computer-mediated environments.

While privacy is often conceptualized as restricting access to information, participating in social media requires people to share. To exist online, people must type themselves into being (Sundén, 2003). Individuals contribute text, photos, and other content, and "like," "favorite," and comment on other people's content to both recognize and engage with others. The act of sharing, an intrinsic—albeit dubious (John, 2013)—component of social media—is central to participation. Because sharing in social media often means contributing content to a persistent and widely accessible ecosystem, it is often mistakenly assumed to be an act of publicity ungoverned by conceptions of privacy. Just as people seek out privacy in public spaces, however, they take steps to achieve privacy in networked publics, even when simply participating in such environments requires sharing.

Method

This article draws from 166 semi-structured interviews with teenagers and participant observation conducted across 17 US states as part of an ongoing ethnographic project regarding teen social media practices (boyd, in press; Marwick and boyd, 2014). The first wave of interviews (n = 106) was conducted in 14 states during 2006–2009 and focused on general technology practices. The second wave (n = 60) was conducted in 2010–2011 in five states and emphasized privacy.

We worked with community organizations to recruit diverse teenagers. Of our interview subjects, 94 were female and 72 were male. In all, 86 identified as White; 39 as Black, African-American, or biracial Black/White; 22 as Hispanic, Chicano, Latino, or biracial Hispanic/White; 13 as Asian, Indian, or Pakistani; 3 as Native American; and 3 as Middle Eastern or Egyptian. Our participants' ranged in age from 13 to 19 (*mean* = 16). A total of 45 teens had at least one parent with a graduate or professional degree, 50 had at least one parent with a Bachelor of Arts (BA) or some college, and the parents of 35 had a high school diploma or less; 36 reported that they didn't know their parents' education level. While this is not a generalizable sample, it reflects a variety of experiences and backgrounds. All names and identifying information have been changed to protect the identities of our participants.

Before each interview, participants (or their parents) signed a consent form. They filled out a questionnaire, including open-ended questions about demography, household makeup, technology usage, and media consumption. Interviews ranged from 60 minutes to 2 hours. Participants were compensated for their time: US$ 30 during the first wave and US$ 40 during the second wave.

We used a semi-structured interview method to ask about a range of topics, including general questions like "What makes someone a friend?" in addition to technology-specific questions like "When is it better to use technology than to talk face-to-face?" The second wave also included questions about privacy, sharing, and publicity. We followed an ethnographic approach to interviewing, listening to how teenagers explained and conceptualized their lives rather than interrogating the accuracy of their statements. We focused on cultural meaning-making, language use, description, and experience (Spradley, 1979). We asked participants to clarify with concrete examples, and took screenshots of their social media profiles. Interviews were digitally recorded and transcribed by a transcription company; a research assistant double-checked the transcripts for accuracy.

Observing and participating in the communities where we interviewed teenagers allowed us to situate interviews within a broader context. We attended school football games, went to religious services at megachurches, and ate fast food alongside teens.

Our theory of networked privacy was formulated throughout data collection and analysis through both thematic and inductive analysis (Thomas, 2006). Reading through the transcripts, both authors identified themes related to privacy (e.g. participants' tactics), emerging patterns, and concepts. Interview data were coded according to an emergent coding schema using Atlas.ti. The second author (danah) wrote ethnographic memos of specific incidents that demonstrated particular aspects of networked privacy. As our understanding of networked privacy deepened, the first author (Alice) returned to the

corpus and coded for related concepts. Due to the iterative nature of coding and analysis, coding was ongoing.

During the writing process, our understanding of networked privacy developed based on findings that problematized our original theories. We presented earlier versions of this article at academic conferences and revised our theories based on feedback. Our theory of networked privacy was thus formulated throughout interviewing, data analysis, and writing, rather than in advance.

Findings: Achieving privacy

The privacy landscape navigated by teenagers looks quite different from that conceptualized by many lawyers, privacy theorists, or activists. Networked publics, especially social media, challenge how people connect and share information in many ways. The dynamics of sites like Facebook make privacy difficult to achieve; privacy settings are complicated and confusing, and rarely provide meaningful protection. Personal interactions are often visible regardless of whether teenagers themselves posted the information (boyd, 2014). Parents look over teens' shoulders at home. Friends tag them in embarrassing photos. Exes post angry rants, inappropriate photos, or worse. Even grandmothers think nothing of sharing old baby photos.

To manage an environment where information is easily reproduced and broadcast, we find that many teenagers conceptualize privacy as an ability to control their situation, including their environment, how they are perceived, and the information that they share. This is more difficult than it may seem. Many adults chastise youth for disregarding privacy, while simultaneously undermining the agency of teenagers. Parents invade their children's privacy by searching rooms and scrutinizing phones, while sharing information on Facebook in ways that challenge teenage attempts to maintain privacy (Shmueli and Blecher-Prigat, 2010). Since American society generally views teenagers as vulnerable (Nelson, 2010), many adults feel that they have the right to surveil teenagers under the guise of protection (Ruck et al., 2008). For their part, most youth are less disturbed by abstract invasions of privacy by government agencies and corporations than the very real and ever-present experience of trying to negotiate privacy in light of nosy parents, teachers, siblings, and peers (Tufekci, 2008). To achieve privacy, teenagers use technologies in novel ways and implement a variety of strategies and tactics in an attempt to regain control over what information is consumed by whom and how that information is interpreted, even when control is not technically possible within a given system.

Determining context

It is challenging to manage discrete social worlds simultaneously, particularly when the norms and values of these worlds differ. The resulting "context collapse," in which seemingly disparate audiences co-exist, often creates a sense of lost privacy. Hunter, a 14-year-old Black youth from inner-city Washington, DC, is frustrated when friends or family members fail to recognize that their beliefs and norms are not universally held:

> When I'm talking to my friends on Facebook or I put up a status, something I hate is when people who I'm not addressing in my statuses comment on my statuses. In [my old school],

> people always used to call me nerdy and that I was the least black black person that they've ever met, some people say that, and I said on Facebook, "Should I take offense to the fact that somebody put the ringtone 'White and Nerdy' [a satirical song by Weird Al Yankovic] for me?" and it was a joke. I guess we were talking about it in school, and [my sister] comes out of nowhere, "Aw, baby bro," and I'm like, no, don't say that, I wasn't talking to you.

Hunter is friends with his sister on Facebook, but feels that she should understand that not all Facebook conversations are intended for her. When danah asked him how someone should know what is appropriate for commentary, Hunter responded by saying,

> I guess that is a point. Sometimes it probably is hard, but I think it's just the certain way that you talk. I will talk to my sister a different way than I'll talk to my friends at school … I mean, I think you can figure out that I'm not talking to you if I'm talking about a certain teacher.

Hunter recognizes that linguistic and social cues indicate whether or not a status update is directed toward a particular audience.

In an effort to reclaim a sense of control over the social situations presented on Facebook—and, thus, gain a sense of privacy—Hunter tries to use Facebook's privacy settings to segment his audience. When he wants to talk about video games, he posts different messages for his cousins and his classmates. Hunter's cousins like first person shooter games, and mock his interest in the old-fashioned Pokémon and Legend of Zelda games popular among his peers at school. To avoid being embarrassed in front of his school friends, he blocks his cousins from seeing these posts. While Hunter does not want to exclude them from his life, he cannot imagine another way to manage the different norms and values present in his network other than de-friending his cousins or deleting comments, both of which are socially costly.

By manually filtering content suitable for his cousins and school friends, Hunter's experience highlights how challenging it can be to meaningfully control information flow in a networked public where content is typically accessible and persistent. He succeeds primarily because he is the sole bridge between the two networks. Had his school friends also been friends with his cousins, it would be much more difficult for Hunter to separate family and school contexts because responses from friends would be visible to his cousins.

While teens can control what they post on their profiles by using different privacy settings, they have far less control over what friends post about them or how their friends' practices shape how they're seen. Ramón, a 17-year-old of Puerto Rican descent, is a talented North Carolina soccer player aspiring to get a college athletic scholarship. He regularly befriended university soccer coaches on Facebook to show that he was a thoughtful, compassionate, all American athlete. His White classmate and friend Matthew approached Facebook differently, often using the site to share crass and juvenile humor with friends that was not intended for adult eyes. Matthew did not friend anyone outside his peer group, but set his privacy settings so friends-of-friends could see his posts. He assumed his friends treated Facebook similarly; he was horrified to realize that Ramón was friends with college representatives. It hadn't dawned on Matthew that adults might see the joking comments he posted on Ramón's pictures.

Matthew failed to understand the context in which he was posting, and thus misunderstood the potential audience for his remarks. Although he intended to share his jokes only

with a limited audience, they traveled outside his envisioned boundary, exposing both him and Ramón in unanticipated ways. Ramón is affected not only by his own content, but how those around him socially co-construct Facebook. Meanwhile, Matthew cannot realistically keep track of how each of his friends manages their privacy settings. This means that in a networked environment, neither teen can assert control over the context. To accurately define the social situation, they must understand how others have shaped the context and operate accordingly. This is not practically possible.

Privacy-protecting tactics and strategies

While the teenagers we spoke to conceptualized privacy in a variety of ways (boyd and Marwick, 2011), many engaged in creative tactics to regulate who could access the information they shared online. A common approach is to ignore the technical features of social media altogether and instead, focus on encoding the content itself in order to limit the audience. This can take different forms, depending on the visibility of the encoding practices.

Carmen, a 17-year-old Latina from Massachusetts, uses Facebook to talk to friends and family. She loves her mother's involvement in her life, but feels that her mother has a tendency to jump in inappropriately and overreact unnecessarily online. Carmen gets frustrated when her mother comments on her Facebook posts "Because then it scares everyone away. Everyone kind of disappears after the mom post … And it's just uncool having your mom all over your wall, that's just lame." When Carmen and her boyfriend broke up, she wanted sympathy and support from her friends. Her inclination was to post sappy song lyrics that reflected her sad state of mind, but she was afraid that her mother would overreact; it had happened before. Knowing that her Argentinean mother would not recognize references to 1970s British comedy, Carmen decided to post lyrics from a movie that she had recently watched with her geeky friends. When her mom saw the update, "Always look on the bright side of life," she commented that it was great to see Carmen doing so well. Her friends, recognizing the lyric came from the Monty Python film *Life of Brian* where the main character is being crucified, immediately texted her.

By hiding content in plain sight, Carmen engaged in a practice that we call "social steganography." *Steganography* is a Greek word that means "covered writing"; to cryptographers and spies, it is a method of hiding information that conceals the very existence of a message (Johnson and Jajodia, 1998). Invisible ink, for example, was used to write private messages on a mundane letter that could be read by anyone; only those who knew to "read between the lines" could access its true meaning. Similarly, the meaning behind Carmen's post was only visible to those who knew where to look and how to interpret what they saw. Other people may have seen the post in a stream of updates, but didn't recognize the cultural reference or understand the relevance to Carmen's life. They may have read it literally or ignored it; not all Facebook updates are scrutinized. By encoding her message, Carmen was able to simultaneously prepare for her mother's gaze and post a meaningful message to a narrow, desired audience. Rather than trying to restrict access to content, Carmen was able to achieve privacy by limiting access to meaning.

Social steganography is not the only form of encoding that we saw. Often, teens choose to render posts inaccessible in a performative manner. This is frequently related

to what American teenagers call "drama," which we define as "performative, interpersonal conflict that takes place in front of an active, engaged audience, often on social media" (Marwick and boyd, 2014). In North Carolina, danah was scrolling through Facebook with 17-year-old Serena when she stumbled on a status update written by Kristy. "I'm sick and tired of all of this" was "Liked" by more than 30 people. Unable to interpret the post, she asked Serena for an explanation. Apparently, Kristy was fighting with another girl, Cathy, about a boy. Cathy had written "She's such a bitch" on her Facebook wall, which was liked by a number of her friends. Kristy posted this message in response, and her friends took her side by "Liking" the update. Serena was a bystander in this argument, but she knew how to interpret each message, danah, as an outsider, did not. Cathy and Kristy are performing for others to see, but they are also limiting the meaning to those who are in the know. In doing so, they can exclude people who are not part of the cycle of gossip at school, namely parents, teachers, and peers outside their immediate social sphere.

Teens are acutely aware that their peers use pronouns and obscure references to say negative things about others without clearly stating that this is what is taking place. Camille, a White 17-year-old from North Carolina explained,

> If you're talking about somebody on Facebook, they can see it … not directly talking about somebody, but talking about them without using their names, and then, they'll start talking about them without using their name, and it's obviously they know they're making fun of each other.

When Alice asked how this worked, Camille said,

> Like everybody will use a quote that somebody said, and then they'll be like, that's so stupid or something, who is she, and then another person will say it, and then they'll, like, respond to something else, and kind of making fun of them indirectly, fighting.

The practice of purposefully encoding messages that contain drama has become so common on social media that some teens refer to this practice as "subtweeting." A subtweet does not name names, but is clearly calling out or criticizing a specific individual; some might characterize subtweets as "passive aggressive." Subtweeting creates plausible deniability, since the subtweeter can always claim the tweet was about someone else if confronted. In other instances, the subtweet may reveal aspects of drama without revealing the whole story. One teenage boy posted on Twitter "Ok so you blocked me.. But why LOL." While the boy may be curious—laugh out loud (LOL) notwithstanding— there is no @ reply or username mentioned, obscuring the incident from curious onlookers. Sometimes, subtweets are obvious insults; another boy tweeted, "Why do u post pictures on instagram of urself in the morning when u look so ratchet. #subtweet." The insult is magnified by the #subtweet tag which makes it explicit.

While social steganography and other methods to limit access to meaning are common teenage strategies, other tactics, especially those that involve creatively manipulating the technical affordances of social media, are less common. Consider the esoteric techniques used by 18-year-old Mikalah and 17-year-old Shamika, two Black inner-city teens in Washington, DC, who are wary of others.

Mikalah wanted to limit adults' access to her Facebook content. As a ward of the state, government agencies regularly used technology to monitor her, or asked her about her online activities. Frustrated by their surveillance and pressure, she tried to delete her Facebook account. Instead, Facebook suggested that she deactivate her account, so she could recover the content whenever she wished. She saw a unique opportunity to limit what people could see about her, and so deactivated her account. Every evening, she logged on to Facebook and reactivated her account. When she was done for the day, she deactivated it again. She assumed—reasonably—that adults would not look at her Facebook profile at night when she was chatting with friends. During the day, when she was offline, it appeared that she didn't have a Facebook page at all, since her account was deactivated. In effect, she created an invisibility cloak for her Facebook, allowing her to believe that she controlled the social situation by making Facebook a real-time service.

Shamika was more concerned with her peers, who frequently dredged up past comments and status updates to start "drama" in the present. To gain control over the context in which her remarks were interpreted, she chose to delete all comments and messages she received after she read them, and deleted all the comments and updates that she left on others' pages a day or two after she posted them. By keeping Facebook clean, she was able to focus others' attention on the present rather than dealing with the persistent nature of normative Facebook practices. While she acknowledged that anyone could manually record older content by taking a screenshot, she stressed that this would be a clear violation of what she thought was appropriate. Her decision to eliminate content was her way of maintaining control.

Mikalah and Shamika's efforts to use Facebook's technical affordances to control their social situations are atypical, but exemplify extreme measures youth can take to achieve privacy by using technology in unexpected ways. As teens attempt to negotiate peers, friends, and family simultaneously on sites like Facebook, they appropriate technical affordances and develop different tactics and strategies to segment audiences, restrict flows of information, and limit who can interpret what to the best of their ability. This does not prevent people from posting messages about them, or others from misinterpreting what they see, but their ingenuity allows some degree of control in an otherwise destabilizing social context.

The power of trust

The teenagers we spoke with recognized that their online social contexts were networked, and often chose to conceal or obscure information as a result. Taylor, a 15-year-old White from Massachusetts, is often frustrated by her friends' tendency to pester her about what's happening in her life when she's quiet. While she understands that they get "in her business" because they care, she still finds their curiosity annoying. To ward off her friends' attention, Taylor shares the "lite version" of her life on Facebook. She posts updates about mundane activities instead of offering emotionally vulnerable content.

When young people do share with friends, they place significant emphasis on what may be done with their information. Consistently, what emerges is the importance of trust and respect. Meixing loves to share, and she loves Facebook. The Tennessee-based 17-year-old of Chinese descent has blocked strangers from accessing her Facebook, but sees herself as an open book to those in her inner circle. She tells loved ones what's

happening in her life, but also gives her most trusted friends access to intimate digital materials:

> I mean I do care about privacy, but if I found someone that I could trust then my first instinct would be to share stuff with that person. For example, I think, like my last boyfriend and I we were really close and then we had each other's passwords to Facebook and to emails and stuff. And so if I would get something that I didn't know about then he would notify me and look over my stuff.

For Meixing, making herself vulnerable to another is a form of intimacy: "It made me feel more connected and less lonely. Because I feel like Facebook sometimes is kind of like a lonely sport … But if someone else knows your password and stuff it just feels better."

The idea that Meixing could care about privacy while still sharing her password may seem paradoxical. But this practice is quite common among teens, many of whom had grown up sharing their passwords with their parents (Lenhart et al., 2011). Parents ask children for their passwords based on advice from online safety experts. Some parents make password sharing a rule, while others use the language of "trust" to frame password sharing as a mechanism of protection. From this, many youths have concluded that to trust means to share. And to share means to trust.

In a networked setting, teens cannot depend on single-handedly controlling how their information is distributed. What their peers share about them, and what they do with the information they receive cannot be regulated technically, but must be negotiated socially. Teens may naively share with a significant other only to be spurned after a nasty breakup, or they may trust their parents to only login to their accounts in an emergency. But no technical solution can provide complete reassurance. Instead, teenagers often rely on interpersonal relationship management to negotiate who shares what about them, who does what with their information, and how their reputations are treated. As countless teenagers have learned, assuming trust is by no means foolproof, but no technical solution to networked data offers a better path forward.

Examining the history of eavesdropping, John L. Locke (2010) explains that people only share personal information when they are confident that it cannot hurt them. One way to do this is through mutual information-sharing, which tends to build trust, "while, paradoxically, making trust less necessary, since each party possesses the tools to hurt the other" (Locke, 2010: 102). Trust and intimacy create reciprocity, which, less charitably, might be viewed as a sort of mutually assured destruction. Similarly, teenagers create trust by revealing information, which in turn may prevent their intimates from revealing that information to others and thus breaking trust. Nissenbaum (2010) describes such contexts as "spheres of trust," she writes, "the parent chooses not to read the child's journal, even though he knows where the journal is kept, as this would not only violate a principle of transmission but would undermine the bonds of trust" (pp. 240–241).

Discussion: The complexity of privacy

The legal and technical emphasis on individual conceptions of privacy has prompted the creation of laws and technologies that do not reflect the nuanced ways in which people

seek to share and maintain privacy. The clunky "access-control list" and "personally identifiable information" models do not cover the instances in which a user's desired approach to information flow may be violated by her network or by a system's technical architecture. If a Facebook user is tagged in a picture or mentioned in a status update, it will appear on her timeline. Even if she is not tagged, Facebook's "tag suggestion" feature may suggest her name to others, based on tagging patterns and facial recognition algorithms (Butcher, 2013). If a Twitter account is private, friends with public accounts who @reply to tweets or retweet messages may reveal the topic of an otherwise protected conversation. Mobile location apps like Foursquare make it possible for friends to "check in" a user at a physical location without prior permission, while LiveJournal makes the time stamp of the last journal entry public, revealing to filtered-out users that posts existed that they cannot see.

Social media privacy controls imply that individuals should be held responsible for how they manage their privacy settings regardless of how well they understand those settings or how frequently those settings change. Facebook's privacy settings, for example, have changed significantly over the last decade (Stutzman et al., 2013), and many users are not confident that they can configure their settings to obtain a desired level of privacy (boyd and Hargittai, 2010). Even when people do configure their settings correctly, information can still slip through the cracks. When Taylor McCormick, a student at the University of Texas, joined the campus's Queer Chorus Facebook group, his participation was broadcast to everyone in his network, effectively outing him to his parents. While Taylor had configured his privacy settings to exclude his parents from seeing much of what he posted, groups have separate privacy settings which trump that of the individual user (Fowler, 2012).

When users choose to share content, or fail to keep content private, companies often reserve the right to share that data with third parties. Others may mine, store, or republish that content elsewhere under the guise that it was public and, therefore, permissible, regardless of the desires of the relevant parties. In a networked world, technical mechanisms often drive normative sensibilities. Businesses, governments, educators, law enforcement, and other actors use these technical affordances to justify decisions to examine, use, and spread anything that is visible. The onus is placed on the individual to understand and adjust their settings and practices accordingly. Failure to do so is interpreted as apathy vis-à-vis privacy, giving rise to the popular idea that because teenagers share information online, they "don't care" about privacy.

Networked privacy

In order to better understand how privacy is achieved in networked publics, we need a model of privacy that is *networked*. Privacy in social media cannot be entirely maintained and established by individuals, as it is not wholly dependent on individual choices or control over data. This networked context is determined through a combination of audience, technical mechanisms, and social norms. Because contexts shift and overlap over time, privacy is an ongoing, active practice. How people achieve privacy depends not solely on their ability to navigate technology, but requires them to fully understand the context in which they are operating, influence others' behaviors, shape who can

interpret what information, and possess the knowledge and skills necessary to directly affect how information flows and is interpreted within that context. In other words, they must have *agency*. Networked publics complicate privacy precisely because they alter social situations in such ways that having power, knowledge, and skills cannot be taken for granted.

Networked privacy invokes the constellation of audience dynamics, social norms, and technical functionality that affect the processes of information disclosure, concealment, obscurity, and interpretation within a networked public. If we understand privacy to be about the management of boundaries, networked privacy is the ongoing negotiation of contexts in a networked ecosystem in which contexts regularly blur and collapse. Networked privacy cannot be achieved simply by providing or denying information; it requires meaningful control over the networked contexts in which the information flows. In other words, achieving privacy requires that people have an understanding of and influence in shaping the context in which information is being interpreted. This can be done by co-constructing the architecture of the systems, or it can be done by embedding meaning and context into the content itself.

Ultimately, attempts to navigate privacy through social media reveal the underlying interactional dynamics of privacy practices, demonstrating that the individualistic model of privacy does not accurately map to human behavior. People live in social contexts; their acts within networked publics implicate each other. Recognizing that privacy is networked suggests that privacy might best be maintained through shared social norms over information-sharing.

Furthermore, conceptualizing privacy as networked highlights the difficulty involved in defining or even understanding social contexts, as they are co-constructed by all present and shaped by the affordances of the social technology in play.

To illustrate these shifts, consider the results when Alice asked her students to violate an unspoken online social norm. Some chose to comment on older photos of their friends. Interacting with older photos can be a taboo among college students, who, after all, have embarrassing middle school pictures in their Facebook albums. Although these photos were "public," in that they were visible to all Facebook friends, the act of commenting re-broadcast them to the network. In other words, the act of commenting became an act of publicizing. The pushback from peers was intense; some students were defriended, others were gossiped about, while still others received text messages or phone calls asking them to stop. The complex information norms of Facebook were not about whether the photos were public or private, but whether or not they were publicized. The fact that this dynamic is experienced as a privacy violation is indicative of how context and norms are entwined with networked privacy.

Conclusion

Legal and technical instantiations of online privacy assume that individuals can and should manage privacy. Networked privacy offers a different model for understanding privacy practices in a networked era. Networked privacy also challenges the access-control list model, which suggests that privacy can be managed by determining who can see a particular piece of information. In the networked privacy model, it is assumed that information

will pass through the network and that privacy can easily be violated by any individual connected to the user. The only guarantee against such things may be shared social norms and social ties. Even if a user makes a picture available to only three friends, these friends can easily disseminate it further. Whether or not they do so is not predicated upon their access to the picture, but their shared social norms and ties to the picture-provider.

Furthermore, networked privacy complicates Nissenbaum's theory of contextual integrity. Contextual integrity assumes that an individual can easily understand the context in which information is originally provided, that contexts are stable and separable, and that privacy violations only occur once information slips to a different context with differing information norms. Networked privacy goes further to suggest that information norms and contexts are co-constructed by participants and frequently shifting. There are differing skill levels to understanding context, and context slips and changes according to fluctuating social norms and technological affordances. Moreover, contexts are not bounded and information norms are not fixed. Instead, situations are co-constructed by all participants. Contextual integrity assumes the context is a given, whereas networked privacy takes into account that individuals may interpret context differently, that contexts may be destabilized or collapse, or that other people may have control over the context in ways that are beyond the purview of the individual (e.g. surveillance, information leakage, or data-mining).

A theory of networked privacy suggests that we must re-conceptualize the harms of privacy. Rather than thinking about privacy harms in terms of individuals or groups—classes of people—we need to frame privacy in terms of networks, or the relationships between people. Social media highlights that information is intrinsically intertwined; photographs contain multiple subjects, messages have senders and recipients, and people share information that implicates others. These complexities cannot be resolved through property models that rely on joint rights. Instead, viable models need to respect that networks of people are connected to information shared in a socially networked world. In a world where networked privacy is common, both legal and technical regimes around information privacy must adapt to better reflect the reality of networked social information.

A networked model of privacy contradicts many of the paternalistic discourses about young people that exist today. When privacy models are individual and technology-focused, the onus is placed on teens, their guardians, or the technology itself to control the flow of data. If a teenager makes digital content available, there is an assumption that privacy no longer matters. Concerned adults encourage teenagers to lock down access for protection. When they do not, they are assumed to be naïve, irresponsible, or engaging in risky behaviors.

Networked publics make it difficult for teens to effectively control information flow. The privacy practices and strategies that teenagers engage in do not necessarily "solve" the problem of privacy, but they do reveal how the technical affordances of networked publics are insufficient to protect privacy. Networked publics create serious and significant conflicts for what youth are trying to achieve in disclosing or withdrawing both information and meaning. Their strategies and tactics reveal one way of managing this conundrum, while also highlighting the importance of re-conceptualizing privacy in a networked era.

Acknowledgements

The authors would like to thank the attendees of the 2011 Privacy Law Scholars Conference, the 2012 Association of Internet Researchers annual meeting, and the Oxford Internet Institute's A Decade in Internet Time symposium; members of the Social Media Collective at Microsoft Research and the Privacy Research Group at NYU Law; Heather Casteel; and the anonymous reviewers for their helpful feedback and advice.

Funding

This project was funded by Microsoft Research and the John D. and Catherine T. MacArthur Foundation. Its findings are solely the responsibility of the authors and do not necessarily represent the views of either funder.

References

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

Barbaro M and Zeller T Jr (2006) A face is exposed for AOL searcher no. 4417749. *The New York Times*, 9 August. Available at: http://www.nytimes.com/2006/08/09/technology/ 09aol.html

boyd d (2014) *It's Complicated: The Social Lives of Networked Teens*. New Haven, CT: Yale University Press.

boyd d and Hargittai E (2010) Facebook privacy settings: who cares? *First Monday* 15(8): 2.

boyd d and Marwick A (2011) Social privacy in networked publics: teens' attitudes, practices, and strategies. *Paper presented at the Oxford Internet Institute Decade in Internet Time Symposium*, Oxford, 22 September.

boyd d (in press) Making sense of teen life: strategies for capturing ethnographic data in a networked era. In: Hargittai E and Sandvig C (eds) *Digital Research Confidential: The Secrets of Studying Behavior Online*. Cambridge, MA: The MIT Press.

Butcher M (2013) Facebook turns photo tag suggestions back on in the US: will users like it this time? *TechCrunch*, 1 February. Available at: http://techcrunch.com/2013/02/01/facebook-turns-photo-tag-suggestions-back-on-in-the-us-will-users-like-it-this-time/ (accessed 24 July 2013).

Cohen JE (2012) *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. New Haven, CT: Yale University Press.

Fowler GA (2012) When the most personal secrets get outed on Facebook. *The Wall Street Journal*, 13 October. Available at: http://online.wsj.com/news/articles/SB10000872396390444165804578008740578200224

Goffman E (1959) *The Presentation of Self in Everyday Life*. New York: Doubleday.

Hoofnagle CJ, King J, Li S, et al. (2010) *How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policies?* Berkeley, CA: University of California, Berkeley. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864

John NA (2013) Sharing and Web 2.0: the emergence of a keyword. *New Media & Society* 15(2): 167–182.

Johnson NF and Jajodia S (1998) Exploring steganography: seeing the unseen. *Computer* 31(2): 26–34.

Lenhart A, Madden M, Smith A, et al. (2011) *Teens, Kindness and Cruelty on Social Network Sites*. Washington, DC: Pew Internet & American Life Project. Available at: http://pewinternet.org/Reports/2011/Teens-and-social-media.aspx

Livingstone S (2008) Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society* 10(3): 393–411.

Locke JL (2010) *Eavesdropping: An Intimate History*. New York: Oxford University Press.

McCallister E, Grance T and Scarfone KA (2010) *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (Computer Security, Special Publication). Washington, DC: National Institute of Standards and Technology. Available at: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf (accessed 26 March 2014).

Madden M, Lenhart A, Cortesi S, et al. (2013) *Teens, Social Media, and Privacy*. Washington, DC: Pew Internet & American Life Project. Available at: http://pewinternet.org/Reports/2013/Teens-Social-Media-And-Privacy/Summary-of-Findings.aspx (accessed 11 July 2013).

Marwick A and boyd d (2011) I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society* 13(1): 114–133.

Marwick A and boyd d (2014) 'It's Just Drama': teen perspectives on conflict and aggression in a networked era. *Journal of Youth Studies*. Epub ahead of print 4 April. DOI: 10.1080/13676261.2014.901493.

Narayanan A and Shmatikov V (2010) Myths and fallacies of personally identifiable information. *Communications of the ACM* 53(6): 24–26.

Nelson M (2010) *Parenting Out of Control: Anxious Parents in Uncertain Times*. New York: NYU Press.

Nippert-Eng CE (2010) *Islands of Privacy*. Chicago, IL: The University of Chicago Press.

Nissenbaum HF (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

Ohm P (2010) Broken promises of privacy: responding to the surprising failure of anonymization. *UCLA Law Review* 57: 1701.

Palen L and Dourish P (2003) Unpacking 'privacy' for a networked world. In: *Proceedings of the SIGCHI conference on human factors in computing systems*, Fort Lauderdale, FL, 5–10 April, pp. 129–136. New York: ACM.

Regan PM (1995) *Legislating Privacy: Technology, Social Values, and Public Policy*. Durham, NC: The University of North Carolina Press.

Ruck M, Harris A, Fine M, et al. (2008) Youth experiences of surveillance. In: Flynn M and Brotherton D (eds) *Globalizing the Streets: Cross-Cultural Perspectives on Youth, Social Control, and Empowerment*. New York: Columbia University Press, pp. 15–30.

Schwartz PM and Solove DJ (2011) The PII problem: privacy and a new concept of personally identifiable information. *New York University Law Review* 86: 1814. Available at: http://papers.ssrn.com/abstract=1909366 (accessed 23 July 2013).

Shmueli B and Blecher-Prigat A (2010) Privacy for children. *Columbia Human Rights Law Review* 42: 759.

Solove DJ (2004) *The Digital Person: Technology and Privacy in the Information Age*. New York: NYU Press.

Spradley JP (1979) *The Ethnographic Interview*. New York: Harcourt Brace Jovanovich.

Stutzman F, Gross R and Acquisti A (2013) Silent listeners: the evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality* 4(2): 2.

Sundén J (2003) *Material Virtualities: Approaching Online Textual Embodiment*. New York: Peter Lang.

Sweeney L (2000) *Uniqueness of Simple Demographics in the US Population*. Pittsburgh, PA: Laboratory for International Data Privacy, Carnegie Mellon University.

Thomas DR (2006) A general inductive approach for analyzing qualitative evaluation data. *American Journal of Evaluation* 27(2): 237–246.

Tufekci Z (2008) Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society* 28(1): 20–36.

Vitak J, Lampe C, Ellison N, et al. (2012) 'Why Won't You Be My Facebook Friend?': strategies for managing context collapse in the workplace. In: *Proceedings of the 7th annual iConference*, Toronto, ON, Canada, 7–10 February, pp. 555–557. New York: ACM.

Wilkins RG (1987) Defining the reasonable expectation of privacy: an emerging tripartite analysis. *Vanderbilt Law Review* 40: 1077–1129.

Author biographies

Alice E Marwick is the director of the McGannon Center and an Assistant Professor of Communication and Media Studies at Fordham University. She is the author of Status Update: Celebrity, Publicity and Branding in the Social Media Age (Yale 2013).

danah boyd is a Principal Researcher at Microsoft Research and the Chief Instigator of the Data & Society Research Institute. She is the author of It's Complicated: The Social Lives of Networked Teens (Yale 2014).