Public Perceptions of Networked Privacy: Past, Present, and Future

Miriam J. Metzger
Department of Communication
University of California, Santa Barbara
Santa Barbara, CA 93106-4020
USA
metzger@comm.ucsb.edu

Ji Young Suh
Department of Communication
University of California, Santa Barbara
Santa Barbara, CA 93106-4020
USA
suh@umail.ucsb.edu

Abstract
This extended abstract focuses on public perceptions of networked privacy. It begins by critically evaluating the literature on privacy in online social networks, it then discusses how data from a recent study conducted by the authors can contribute new insight into networked privacy perceptions and behavior. It concludes with an agenda for future research that aims to spark discussion among workshop participants.

Author Keywords
Networked privacy; information disclosure, social media

ACM Classification Keywords
H.5.m. Information interfaces and presentation (HCI): Miscellaneous.

CSCW 2015, March 14-18, 2015, Vancouver, BC, Canada.
ACM XXX-X-XXXXX-XXX-X/XX/XX.

Introduction
The rise of social networking online has brought issues of privacy into focus. Yet, at the same time, getting a clear picture of users' privacy perceptions and how those perceptions guide behavior is difficult. Part of the problem is that public perceptions of privacy can shift suddenly in response to technical, social, or cultural events, as well as the introduction of new forms or iterations of technology (i.e., new platforms, interfaces, services, etc.). Recent examples include abrupt fluctuations in public norms and attitudes toward privacy after the Heartbleed virus [11], and after the revelations of NSA data surveillance [9]. These fluctuations can make understanding public privacy perceptions elusive, as most research investigates privacy perceptions statically.[1]

Another problem of understanding public privacy perceptions is that while research in this area is burgeoning, with both academics and opinion pollsters seeking to track, understand, and predict public attitudes and behavior regarding privacy online, each of these efforts has significant limitations in the information they have provided thus far. Problems such as narrow sampling frames, single-platform focus,

[1] One important exception is a longitudinal study by Stutzman, Gross, and Acquisti (see [14]).

inconsistent measurement, and lack of theory to guide the research tend to plague the literature.

But understanding public perceptions concerning privacy and any attendant behavioral outcomes is crucial, not just to the social science enterprise, but to the technical and commercial sectors in terms of the capacity for this understanding to guide product design. Understanding public conceptions, tolerances, and behaviors toward privacy in social networking environments also has significant import for devising privacy regulation that is fair to all stakeholders. Thus, our aim in this workshop is to try to bring into clearer focus what is currently known about public perceptions of privacy in online social networks, and in so doing to identify what is still needed or lacking in our knowledge as we look toward the future of networked privacy.

To open the discussion, this abstract critically evaluates existing literature on public perceptions of privacy in online social networks, and presents some new concepts that extend the current literature to enhance our understanding of privacy perceptions in online social networks. The abstract concludes with an agenda for future research on privacy perceptions intended to spark discussion among workshop participants.

Critique of the Existing Privacy Literature

Research on privacy within the academic community spans several disciplines and has focused largely on such topics as conceptualizing privacy, understanding the antecedents and outcomes of users' privacy concerns, and strategies people use to protect or manage their privacy online [2, 13]. Privacy has also been the focal topic of many public opinion polls in the last several years, which typically seek to gauge levels of public awareness and concern about privacy, information disclosure behavior, and use of available self-protection mechanisms or tools in response to privacy threats (e.g., [12, 7]). While both academic and applied research add to our knowledge of privacy perceptions in digital networked environments, they each suffer from problems that constrain our ability to adequately understand and explain privacy attitudes and behavior in highly complex and rapidly evolving technical and social circumstances.

For example, within the academic literature on privacy perceptions, there is often little consistency in the concepts or measures used from study to study, or from field to field. For example, concepts such as privacy concern, desire for privacy, or privacy paradox are often conceptualized and measured in different ways across studies and fields [2, 5]. Inconsistencies in conceptual and operational definitions used in the privacy literature render detecting over-time patterns tricky, as comparisons between studies can be difficult to make. Moreover, the vast majority of academic studies of privacy perceptions employ college students as participants, which likely skews understandings of users' needs and concerns [2]. Although social networking site (SNS) users were primarily young in the beginning, that is no longer true today [14]. For findings that are generalizable to current SNS users, we need more insight into privacy perceptions of users across a greater range of age groups.

Public opinion polls do provide information about a wider array of users, and are particularly helpful in describing basic trends and shifts in perceptions of privacy over time, but are limited in helping to develop and test theories about privacy, and thus in explaining why those trends and shifts occur. Yet understanding the principles underlying privacy perceptions is critical

to understanding emerging and future privacy challenges.

Added to these problems, both academic and applied research on privacy tends to be cross-sectional in nature and tends to focus on a single platform at a time. A search of the social scientific literature on privacy yielded only one longitudinal study of privacy by Stutzman and colleagues [15]. These researchers analyzed Facebook users in the Carnegie Mellon University network to examine how their privacy management behavior changed from 2005 to 2011. An important finding was that changes in the SNS environment (i.e., Facebook structure) during the study affected user behavior, revealing that privacy choices are more than simple expressions of individual subjective preferences. This result highlights the importance of longitudinal research by providing crucial insight into privacy dynamics within social networking platforms that could only be revealed by studying privacy over time. Similarly few studies consider cross-platform privacy management strategies, even though more and more users are accessing social media from multiple devices and applications [16]. This is surprising given the potential for cross-platform social media use to exacerbate 'context collapse' [8, 17] and privacy problems stemming from it.

Clearly, new research on privacy perceptions is needed that includes a wider assortment of both users and platforms, extends across time, and is based on and/or helps to develop theory in order to accurately model user attitudes and behavior, and thus to design technical solutions to help users negotiate their privacy. Such efforts are equally important from a regulatory standpoint, as a clear understanding of public perceptions is necessary to formulate equitable policy solutions to protect users from privacy challenges that arise from future technological developments.

New Concepts, New Data

A prime example of where more research is needed connects to the legal arena. The number of privacy lawsuits stemming from the use of SNSs rises each year. Privacy regulation in the U.S. rests on the determination of whether the plaintiff had a 'reasonable expectation' of privacy within a given context. The law moreover states that a person's expectation of privacy within a given context may only be considered to be reasonable if "society" deems it as such. And yet, while many studies have examined public concerns or desires about privacy, there is little published research on either societal or SNS users' *expectations of privacy* as pertains to the law (but see [6]). The result is that judges are forced to decide whether or not the expectation of privacy in SNS is reasonable in society's eyes devoid of any data that could inform them about societal expectations of privacy in networked environments [10]. Not surprisingly, this has lead to conflicting rulings in this area of law as judges base their decisions on subjective criteria. More research on privacy expectations is thus invaluable to future privacy jurisprudence, and has significant implications for understanding privacy perceptions and behavior more widely as users' expectations are intrinsically linked to their attitudes and behavior.

At the workshop, we will present empirical data on public perceptions of "reasonable privacy expectations" in online social networks that are relevant to privacy jurisprudence. Collected from a nationally-representative sample of 1,156 SNS users in the U.S. ranging in age from 18 to 86, these data provide new insight into how users conceptualize privacy in SNS to

form beliefs about what is reasonable to expect in terms of their privacy from multiple audiences, including fellow SNS users, platform and third-party operators, and the government. Further data from the same study provides insight into other important, yet little-studied concepts that may help to better understand the full landscape of privacy perceptions in digital networks. For example, data from the survey reveal an interesting phenomenon of *optimistic bias* in privacy perceptions whereby SNS users tend to feel they are personally less susceptible to privacy risks than are others. This sense of overconfidence may help to explain the well-documented "privacy paradox," which refers to the persistent yet puzzling finding of a negative relationship between SNS users' stated privacy fears and their privacy protection behavior. Indeed, this study empirically investigates competing theoretical explanations of the privacy paradox, and results will be shared at the workshop in March.

Future Directions and Pathways Forward

By looking across both prior and current research on privacy perceptions in SNS, an agenda for future research on privacy perceptions begins to emerge for discussion at the workshop. For example, in addition to the points raised above, (i.e., the need for future studies that examine privacy perceptions across multiple platforms, from a longitudinal perspective with consistency in measures, and employing broad rather than narrow sampling frames), future research needs to move beyond documenting public concerns and privacy management strategies, and it needs to engage theory in more meaningful ways to better account for when privacy perceptions do or do not lead to specific behavior. To date, some of the more common theoretical accounts of networked privacy are social exchange theory, the theory of planned behavior, and communication privacy management theory, which are all based on the premise of rational actors. Yet mounting evidence, including optimistic biases in privacy perceptions, points to potentially less rational privacy decision-making within social media contexts (see [1, 3]). Heuristic processes of privacy risk assessment and the role of emotion in disclosure decisions within SNS contexts are not well understood, but may hold important keys to explaining both privacy perceptions and the privacy paradox.

The networked structure of privacy in the contemporary media environment also highlights linkages between the individual and the social groups in which individuals are embedded that are largely ignored in the privacy literature [2, 13]. The vast majority of existing research considers privacy at the individual level, but there is growing evidence that privacy is conceptualized and managed at both the individual and group levels. For example, although individuals manage personal information flows, group information is connected to the self but is often beyond the control of the individual [4]. Moreover, organizational and group culture undoubtedly impact privacy perceptions and behavior in significant ways [2]. This is a particularly promising avenue for scholarly exploration, with group-level theories such as social identity theory, self-categorization theory, and even evolutionary psychology poised to provide a strong foundation upon which to guide hypothesizing.

These are just a few of the directions that future research could take to better meet the current and future challenges of networked privacy posed by emerging communication and information technology. It is our aim to engage with workshop participants to discuss these and other ideas concerning how best to

understand privacy perceptions and behavioral outcomes in a rapidly evolving social media environment.

References

[1] Acquisti, A., and Grossklags, J. What can behavioral economics teach us about privacy? In A. Acquisti, S. Gritzalis, S. Di Vimercati, C. Lambrinoudakis (Eds.), *Digital Privacy: Theory, Technologies, and Practices*, Auerbach Publications (2007), 363-379.

[2] Bellanger, F., and Crossler, R. E. Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly 35, 4* (2011), 1017-1041.

[3] Carey, R. and Burkell, J. A. Heuristics Approach to Understanding Privacy-Protecting Behaviors in Digital Social Environments. In I. Kerr, V. Steeves, and C. Lucock (eds.). *Lessons From the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*. Toronto: Oxford University Press (2008), 65-82.

[4] De Wolf, R., Willaert, K., and Pierson, J. Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook. *Computers in Human Behavior*, *35* (2014), 444–454.

[5] Litt, E. Understanding social network site users' privacy tool use. *Computers in Human Behavior 29*, 4 (2013), 1649–1656.

[6] Liu, Y., Gummadi, K., Krishnamurthy, B., & Mislove, A. Analyzing Facebook privacy settings: Expectations vs. reality. Proc. *IMC2011* ACM Press (2011), 1-7.

[7] Madden, M., Fox, S., Smith, A., and Vitak, J. *Digital Footprints: Online identity management and search in the age of transparency* (2007), 1–50. Washington, DC.

[8] Marwick, A. and boyd, d. I tweet honestly, I tweet passionately: Twitter users, contect collapse, and the imagined audience. *New Media & Society, 13* (2010), 114-133.

[9] Pew Research Center for the People & the Press. *Public says investigate terrorism, even if it intrudes on privacy: Majority views NSA Phone Tracking as Acceptable Anti-Terror Tactic* (pp. 1–13). Washington, DC (2013).

[10] Pure, R. A. *Privacy expectations in online contexts*. Ph.D. Dissertation. Department of Communication, University of California at Santa Barbara, 2013.

[11] Rainie, L., and Duggan, M. *Heartbleed's Impact* (2014), 1–12.

[12] Rainie, L., Kiesler, S., and Madden, M. *Anonymity, Privacy, and Security Online* (2013), 1–35. Washington, DC.

[13] Smith, H. J., Dinev, T., and Xu, H. Information privacy research: An interdisciplinary review. *MIS Quarterly, 35, 4* (2011), 989-1015.

[14] Social Networking Fact Sheet. (n.d.). Retrieved November 03, 2014, from http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/

[15] Stutzman, F., Gross, R., and Acquisti, A. (2012). Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality 4*, 2 (2012), 7–41.

[16] Suh, J. *What they think vs. what they do. Online privacy management via different devices in different locations.* Undergraduate honors thesis, Northwestern University, 2014.

[17] Vitak, J. The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting and Electronic Media*, *56*, 4 (2012), 451–470.