OPINION PAPER

A Contextual Approach to Information Privacy Research

Philip Fei Wu*
School of Management, Royal Holloway, University of London, Egham, United Kingdom. E-mail: philip.wu@rhul.ac.uk

Jessica Vitak
College of Information Studies, University of Maryland at College Park, College Park, MD. E-mail: jvitak@umd.edu

Michael T. Zimmer
School of Information Studies, University of Wisconsin–Milwaukee, Milwaukee, WI. E-mail: zimmerm@uwm.edu

In this position article, we synthesize various knowledge gaps in information privacy scholarship and propose a research agenda that promotes greater cross-disciplinary collaboration within the iSchool community and beyond. We start by critically examining Westin's conceptualization of information privacy and argue for a contextual approach that holds promise for overcoming some of Westin's weaknesses. We then highlight three contextual considerations for studying privacy—digital networks, marginalized populations, and the global context—and close by discussing how these considerations advance privacy theorization and technology design.

Introduction

Privacy is a central issue of the information age. Advances in information and communication technologies (ICTs) and their wide adoption have exponentially increased the amount of personal information being collected by commercial and government entities. Although ICTs such as fitness trackers, smart speakers, and social media provide users with new ways to interact and learn about themselves, they also pose a number of privacy risks. For example, the Cambridge Analytica scandal in early 2018 spotlighted problematic privacy practices at Facebook (Cadwalladr & Graham-Harrison, 2018). More broadly, the promises of big data and "data-driven decision-making" raise wider concerns for the future of individual privacy (boyd & Crawford, 2012; Lane, Stodden, Bender, & Nissenbaum, 2014; Zhang, 2016; Zimmer, 2016).

Although few scholars would argue against the importance of information privacy, there are considerable differences across privacy scholarship on how to assess, improve, and regulate current industry practices for a better protection of personal information. The intertwining relationship between information technology and privacy calls for a highly interdisciplinary approach to examining information privacy issues from multiple perspectives. We believe that the information science community is particularly well positioned to contribute to the current privacy discussion and to shape the solution space with innovative ideas. Indeed, a quick survey of *JASIST* publications during the past decade (2008–2018) shows that more than 30 articles have tackled privacy issues in various empirical contexts, including mobile health (Clarke & Steele, 2015; Harvey & Harvey, 2014), social media platforms (Squicciarini, Xu, & Zhang, 2011; Stern & Kumar, 2014), as well as new ways to model and measure privacy in academic research (Rubel & Biava, 2014; Sánchez & Batet, 2016). Collectively, these studies span a broad spectrum of intellectual traditions in the community and demonstrate nuanced understandings of the relationship between ICTs and privacy.

Nevertheless, research gaps still exist. In particular, despite the diversity of intellectual resources being utilized in privacy research, there has been limited integration of these resources in proposing practical and innovative privacy-enhancing solutions. For example, there is a wide recognition that social network sites' (SNSs) privacy settings match poorly with users' privacy expectations (Liu, Gummadi, Krishnamurthy, & Mislove, 2011; Wu, 2019); however, few studies to date have proposed and empirically tested alternative designs

*Corresponding author

Received October 22, 2018; revised February 25, 2019; accepted March 12, 2019

 DOI: 10.1002/asi.24232

for a better control of privacy parameters (with Stern & Kumar, 2014, as a notable exception). Likewise, scholars taking a sociopsychological approach have identified multiple factors that affect people's privacy perceptions and behaviors, but these findings are often difficult to translate into concrete policy suggestions (Acquisti & Grossklags, 2004, 2005).

In this position article, we synthesize various knowledge gaps in information privacy scholarship and propose a contextual approach of privacy research that promotes greater cross-disciplinary collaboration. We start by critically examining Westin's (1967) conceptualization of privacy and argue for a contextual perspective that holds promise for overcoming some of Westin's weaknesses. We then highlight three contextual considerations for studying privacy, and we discuss how these considerations advance privacy theorization and technology design.

Assumptions of Westin's Theory of Privacy

Writing more than 50 years ago, Westin (1967) defined privacy as "the right of the individual to decide what information about himself [*sic*] should be communicated to others and under what condition" (p. 10). This widely cited definition contains several underlying assumptions, including that (a) "information about himself" is known and transparent to the individual, (b) "communicated to others" is the end of the information journey, and (c) individuals are capable of evaluating "conditions" and making rational decisions about their privacy rights.

Each of these assumptions is contestable in today's digital information environment. As our daily activities are being facilitated (for example, shopping) and sometimes deeply embedded (for example, social networking) in various digital technology platforms, we leave data trails that are recorded, monitored, and shared with or without our knowing. Hence, individuals rarely have a complete picture of what "information about themselves" is out there. Furthermore, privacy policy development and implementation has lagged behind technological advancements; for example, although the U.S. Federal Trade Commission recommended a one-stop "privacy dashboard" in 2013 for smartphone users to review information being accessed across mobile apps (Federal Trade Commission, 2013), such recommendations have not yet been widely adopted by the industry. In fact, as digital businesses create "walled gardens" to lock in users and maintain a competitive advantage, a cross-app, cross-platform, comprehensive privacy dashboard is unlikely to become a reality. It is also important to note that in this hyperconnected era (Floridi, 2015), individuals have less control over information about themselves, with data being comanaged with friends, family, and others who can post or share your personal information to a variety of online channels. For example, Besmer and Richter Lipford (2010) found that photo tagging on SNSs reduces users' control over their information disclosures when images are shared across their many overlapping social circles.

Control over, access to, and communication of personal data are still key aspects of information privacy. Yet information privacy today is more than just who has access to what information. A significant development in recent years is the technological capability of analyzing large volumes of data from diverse sources to identify patterns in consumption, lifestyle, sexual orientation, political inclinations, and more (for example, Ohm, 2009). An individual's privacy is at risk not only because information about her/himself may be "communicated to others" without consent, but also because existing dots can now be connected with high efficiency to reveal intimate details about the person.

Lastly, Westin's definition assumes a knowledgeable and rational human who is capable of making the best decision for their privacy under different scenarios, yet research reveals this is not always the case (Acquisti, Taylor, & Wagman, 2016). Often, there are transparency and information asymmetries that prevent individuals from obtaining complete and perfect information for decision making. Further, humans are known for making poor decisions due to cognitive biases and changing preferences. For example, in evaluating the risks and benefits of revealing personal information, people frequently make decisions that favor short-term gains over long-term consequences, both known and unknown (Acquisti & Grossklags, 2005). A number of empirical studies have demonstrated inconsistencies and difficulties of making the "best" privacy trade-off in various circumstances (see, for example, Acquisti et al., 2016).

A Contextual Approach to Privacy Research

Recognizing that the "transparency-and-choice" scenario in Westin's conceptualization of privacy does not fit well with the digital reality of privacy today, a growing number of privacy scholars are advocating for a more a contextual approach to information privacy, emphasizing the importance of understanding and respecting the conditions and context that guide individuals' decision to disclose sensitive data. One of the foundations for this approach is Helen Nissenbaum's theory of "privacy as contextual integrity" (Nissenbaum, 2004; Nissenbaum, 2010), which links the protection of personal information to the norms of information flow within specific contexts. Rejecting the traditional dichotomy of public versus private information—as well as the notion that a user's preferences and decisions of privacy are independent of context—contextual integrity provides a framework for evaluating the flow of personal information between different agents and explaining why certain patterns of information flow might be acceptable in one context but viewed as problematic in another.

Researchers have applied contextual integrity to various privacy-sensitive contexts, such as search engines (Zimmer, 2008), social network sites (Shi, Xu, & Chen, 2013), location-based technologies (Barkhuus, 2012), electronic medical records (Chen & Xu, 2013), student learning analytics (Rubel & Jones, 2016), smart home devices (Apthorpe, Shvartzshnaider, Mathur, Reisman, & Feamster, 2018), and

DOI: 10.1002/asi

big data research ethics (Zimmer, 2018), among others. These studies have identified more nuanced explanations for perceived "inconsistencies" or "paradoxes" in privacy behaviors, suggesting that breaches in contextual integrity can help explain why users would be concerned with uses of information that go beyond the original purpose or context in which they were initially disclosed.

In light of the critical importance of contextual integrity in studying privacy, we advocate for an even broader contextual view of privacy at all analytical levels—individual, group, and societal. Below, we briefly discuss three specific contextual considerations that are likely to shape future directions of privacy research: privacy in networked contexts, privacy for marginalized groups, and privacy in a global regulatory context.

Privacy in Networked Contexts

With a contextual perspective, privacy can be understood as a process of managing boundaries across different social contexts. The boundaries may shift, collapse, or reemerge as social circumstances change. For example, on Facebook, users navigate a variety of audiences and social contexts, with different boundaries for their disclosures. In private groups, they may feel more open in making sensitive disclosures because only other group members can see the content; contrast these disclosures with status updates that may be viewable to all friends or an even wider audience, depending on whether the post is public or if other users have been tagged in the post. In these spaces, therefore, privacy becomes an "ongoing negotiation of contexts in a networked ecosystem in which contexts regularly blur and collapse" (Marwick & boyd, 2014, p. 1063). Users must constantly negotiate questions about the content they are sharing, and who the perceived audience for the post is, who the potential audience is, among other considerations. Furthermore, users of these spaces may quickly discover that they comanage their privacy with other users (who might share content related to them) and the platforms themselves (who make various pieces of personal information more or less visible in the system).

The concept of "networked privacy"—that individuals lack full control over how and what information about them is shared online and that privacy is collaboratively managed by both individuals and other users of a platform—highlights two key aspects of privacy in a networked environment: (a) privacy norms about appropriate information flow are in flux as individuals move within and/or across social boundaries; (b) privacy management is a collective, rather than individual, practice.

In evaluating how norms around privacy and sharing change across time and space, networked privacy researchers have studied the challenges arising when social contexts collapse. Context collapse, broadly describing the flattening of social networks into homogeneous groups, which can affect disclosure and privacy practices in a variety of ways. For example, some users stop sharing on social media completely or significantly censor their posts because platforms offer few technical strategies for more nuanced sharing (Marwick & boyd, 2011; Vitak, 2012). Furthermore, researchers have considered how the sociotechnical affordances of social media platforms shape users' experiences, encourage sharing, and make it more challenging to discern how information flows through (and beyond) the platform. These studies (for example, Bangasser-Evans, Pearce, Vitak, & Treem, 2017; Treem & Leonardi, 2013) highlight how the features of various platforms afford different outcomes, with some sites affording high levels of visibility or spreadability of content, whereas others may afford greater degrees of obscurity or anonymity. Finally, studies suggest that the collective nature of privacy in these spaces leads users to engage in a variety of privacy management strategies, including social steganography or vaguebooking (Marwick & boyd, 2014), constant curation of connections and content (Vitak, Blasiola, Patil, & Litt, 2015), and using more private platforms for sensitive disclosures (Piwek & Joinson, 2016).

Privacy for Marginalized Groups

When looking at the subjects of privacy research, it quickly becomes clear that some subsets of the population are largely overlooked or understudied. A key demographic receiving little empirical attention is economically disadvantaged Internet users. As a group, these individuals have lower digital literacy, less access to the Internet and computers, and fewer connections in their social network to go to for help with technology (Van Dijk, 2005). Therefore, a contextual approach is needed to examine how socioeconomic and other contextual factors affect the group's privacy concerns and practices. Numerous studies have considered the broader effects of the digital divide (see, for example, Rice & Katz, 2003; Stanley, 2003), but few have addressed privacy issues across socioeconomic spectrums. In one notable exception, research by Vitak, Liao, Subramaniam, and Kumar (2018) highlighted that low socioeconomic status (SES) families face a range of privacy and security risks online and many lack trust in companies to protect their personal information. Continuing to evaluate low-SES Internet users is increasingly important in a time when job applications, tax forms, and government benefits require users to complete online forms and submit sensitive personal information.

Marginalized and stigmatized groups also face heightened risks around identity-based disclosures; therefore, their disclosure strategies and privacy-protection behaviors in digital spaces are more important than for the general population. For example, LGBTQ+ adults and adolescents may have heightened privacy concerns around when and where they make identity disclosures online (Blackwell et al., 2016), and such disclosure decisions may be difficult, especially in spaces where others can "out" an individual and users have less control over their self-presentation (Duguay, 2016). Individuals with stigmatized health conditions or chronic illnesses may possess greater privacy concerns about sharing their data online, even when disclosures may help facilitate

DOI: 10.1002/asi

social, informational, and emotional support (Choudhury & De, 2014). Likewise, individuals living in authoritarian regimes or under restrictive governments may have greater privacy concerns and face greater risks when speaking out against the government than those living in more democratic countries (Pearce, Vitak, & Barta, 2018).

Privacy in a Global Regulatory Context

Context matters not only in understanding individuals' privacy needs and behaviors, but also in addressing regulatory challenges in a globalized world. Governments have struggled with whether and how to regulate information flows across global platforms and services to protect citizens' privacy. Given the diversity of interests, histories, and cultural contexts, a complicated terrain of transnational laws and policies for the protection of privacy and personal data flows across networks has emerged (Greenleaf, 2017). Some jurisdictions have opted for broad, and relatively strict, laws regulating the collection, use, and disclosure of personal information, such as Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and the European Union's General Data Protection Regulation (GDPR). The United States, however, maintains a more sectoral approach to privacy legislation, with laws addressing only specific types of personal information. For example, the Health Insurance Portability and Accountability Act (HIPAA) offers protection of personal medical information; the Fair Credit Reporting Act regulates the collection and flow of personal financial data; and the Video Privacy Protection Act makes the wrongful disclosure of video rental records illegal.

The differences between the Canadian/E.U. approach to privacy, and that of the United States, have been well documented and analyzed (Bennett & Charles, 2006; Krotoszynski, 2016). Although the E.U. and Canada focus on direct and preemptive regulation of the collection and use of personal data, prohibiting "excess" data collection and restricting use to the original and stated purposes of the collection, the U.S. approach begins with the assumptions that most data collection and use is both acceptable and beneficial, that guidelines should be primarily voluntary and noninvasive, and that any regulation should only address documented instances of misuse or harm. This difference in regulatory approaches to privacy—and the underpinning tensions between different jurisdictions' views toward the rights of data subjects—becomes complicated further given the increasing flows of personal information between transnational networks and across borders. Internet companies such as Google and Facebook have customers accessing their products and services from across the globe, with data processing and storage facilities equally scattered. A Canadian citizen, for example, might be accessing a Google product in the United States, while the record of the particular information exchange might be stored on a server in Ireland. Each jurisdiction has its own complex set of regulations and rights assigned to the treatment of any personal information shared and stored.

These kinds of scenarios have prompted debate about whether the global diversity of privacy governance will result in a "trading up," where information platforms develop practices and policies that meet higher privacy standards to be perceived as the "best" protector of personal information flows irrespective of the borders the personal information might cross, or a "race to the bottom" where corporate interests in processing personal data will migrate to jurisdictions with little or no control over the circulation and capture of personal information flows. Researchers wishing to embrace a more contextual approach to privacy will need to grapple with the complex global nature of information flows and regulations, recognizing that privacy expectations and practices differ greatly across geopolitical borders. For the information science community, this will require continued focus on global research studies and collaborations.

Conclusion and a Design Recommendation

Our brief review of three contextual considerations above highlights the challenges of designing a one-size-fits-all solution for informational privacy needs that span multiple contexts. For example, privacy researchers have long observed a "privacy paradox" phenomenon (that is, people claim to care about privacy but behave as if they do not care), but few have systematically examined in what contexts this attitude–behavior dichotomy is likely to manifest, or how to resolve the dichotomy through technology design. Many current systems and platforms fail to protect user privacy because privacy is an afterthought of system design (Papacharissi & Gibson, 2011). More effective privacy protections, as Cavoukian (2011) argues, may require a Privacy by Design approach where privacy considerations are an integral part of design and implementation from the outset, with design decision-making situated in the relevant local and global contexts. Such a privacy-sensitive design could even embed a choice architecture (Thaler, Sunstein, & Balz, 2013) where privacy choices are contingent on the use context and the platform's technological affordances, thereby nudging users to take privacy-protective actions when necessary (Wang et al., 2013). Almuhimedi et al. (2015) demonstrated in a field study that even a simple nudge on mobile devices can lead participants to adjust their mobile app privacy settings and bring their data sharing behaviors into alignment with their privacy preferences. To this end, designing for privacy should move beyond mainstream mechanisms that protect already-generated personal data, and instead develop creative ways of steering both individuals and organizations toward preventative behaviors in various contexts.

To conclude, we have explained how a contextual view of information privacy may open up new venues of research. Prior research based on Westin's assumptions does not provide the full picture of people's privacy behaviors and decision-making strategies in the information age. Today, we find that privacy management is negotiated not

DOI: 10.1002/asi

just at the individual level, but between many individuals at a group or community level, with companies and third parties who collect and share data, and with governments and regulators in different regions. Considering privacy from a contextual approach is more difficult, but it more accurately reflects the reality of data sharing and privacy management in the 21st century. Investigating how individuals, groups, and businesses deal with information sharing in all types of contexts is critical to extending theories of privacy and to designing privacy-sensitive tools that address the needs and concerns of a wider range of users and communities. We believe the information science community can lead this line of inquiry due to their interdisciplinary knowledge and experience in social and computational sciences and their well-established tradition of respecting use context in information system research and design.

References

Acquisti, A., & Grossklags, J. (2004). Privacy attitudes and privacy behavior. In L.J. Camp & S. Lewis (Eds.), Economics of information security (pp. 165–178). Boston: Springer US.

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. IEEE Security Privacy, 3(1), 26–33.

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. Journal of Economic Literature, 54(2), 442–492.

Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., … Agarwal, Y. (2015). Your location has been shared 5,398 times!: A field study on mobile app privacy nudging. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (pp. 787–796). New York: ACM.

Apthorpe, N., Shvartzshnaider, Y., Mathur, A., Reisman, D., & Feamster, N. (2018). Discovering IoT smart home privacy norms using contextual integrity. In Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (Vol. 2, p. 2).

Bangasser-Evans, S., Pearce, K., Vitak, J. & Treem, J. (2017). The affordances test: A conceptual model for understanding affordances in communication research. Journal of Computer-Mediated Communication, 22, 35–52.

Barkhuus, L. (2012). The mismeasurement of privacy: Using contextual integrity to reconsider privacy in HCI. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 367–376). Austin, TX.

Bennett, C.J., & Charles, D.R. (2006). The governance of privacy: Policy instruments in global perspective. Cambridge, MA: MIT Press.

Besmer, A. & Richter Lipford, H. (2010). Moving beyond untagging: Photo privacy in a tagged world. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 1563–1572). New York: ACM.

Blackwell, L., Hardy, J., Ammari, T., Veinot, T., Lampe, C., & Schoenebeck, S. (2016). LGBT parents and social media: Advocacy, privacy, and disclosure during shifting social movements. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (pp. 610–622). New York: ACM.

boyd, D., & Crawford, K. (2012). Critical questions for big data. Information, Communication & Society, 15(5), 662–679.

Cadwalladr, C. & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge analytica in major data breach. The Guardian. Retrieved from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Cavoukian, A. (2011). Privacy by design in law, policy and practice: A white paper for regulators, decision-makers and policy-makers. Information and Privacy Commissioner, Ontario, Canada. Retrieved from http://www.ontla.on.ca/library/repository/mon/25008/312239.pdf

Chen, Y., & Xu, H. (2013). Privacy management in dynamic groups: understanding information privacy in medical practices. In Proceedings of the 2013 conference on Computer Supported Cooperative Work (CSCW '13; pp. 541–552). New York: ACM.

Choudhury, M.D. & De, S. (2014). Mental health discourse on reddit: Self-disclosure, social support, and anonymity. In Eighth International AAAI Conference on Weblogs and Social Media. Retrieved from https://www.aaai.org/ocs/index.php/ICWSM/ICWSM14/paper/view/8075

Clarke, A., & Steele, R. (2015). Smartphone-based public health information systems: Anonymity, privacy and intervention. Journal of the Association for Information Science and Technology, 66(12), 2596–2608.

Duguay, S. (2016). "He has a way gayer Facebook than I do": Investigating sexual identity disclosure and context collapse on a social networking site. New Media & Society, 18(6), 891–907.

Federal Trade Commission. (2013). Mobile privacy disclosures: Building trust through transparency: a federal trade commission staff report. Retrieved from https://www.ftc.gov/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission

Floridi, L. (Ed.). (2015). The onlife manifesto: Being human in a hyperconnected era. Cham, Switzerland: Springer Open.

Greenleaf, G. (2017). Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey. 145 Privacy Laws & Business International Report, 10–13; UNSW Law Research Paper No. 17-45. Retrieved from SSRN https://ssrn.com/abstract=2993035

Harvey, M.J., & Harvey, M.G. (2014). Privacy and security issues for mobile health platforms. Journal of the Association for Information Science and Technology, 65(7), 1305–1318.

Krotoszynski, R.J. (2016). Privacy revisited: A global perspective on the right to be left alone. Oxford, UK; New York: Oxford University Press.

Lane, J., Stodden, V., Bender, S., & Nissenbaum, H. (Eds.). (2014). Privacy, big data, and the public good: Frameworks for engagement. New York: Cambridge University Press.

Liu, Y., Gummadi, K.P., Krishnamurthy, B., & Mislove, A. (2011). Analyzing Facebook privacy settings: User expectations vs. reality. In Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference (pp. 61–70). New York: ACM.

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

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

Nissenbaum, H. (2004). Privacy as contextual integrity. Washington Law Review, 79(1), 119–157.

Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford, CA: Stanford University Press.

Ohm, P. (2009). Broken promises of privacy: Responding to the surprising failure of anonymization. UCLA Law Review, 57, 1701.

Papacharissi, Z., & Gibson, P.L. (2011). Fifteen minutes of privacy: Privacy, sociality, and publicity on social network sites. In S. Trepte & L. Reinecke (Eds.), Privacy online: Perspectives on privacy and self-disclosure in the social web (pp. 75–90). Heidelberg: Springer.

Pearce, K.E., Vitak, J., & Barta, K. (2018). Privacy at the margins| socially mediated visibility: Friendship and dissent in authoritarian Azerbaijan. International Journal of Communication, 12(0), 22.

Piwek, L., & Joinson, A. (2016). "What do they snapchat about?" Patterns of use in time-limited instant messaging service. Computers in Human Behavior, 54, 358–367.

Rice, R.E., & Katz, J.E. (2003). Comparing internet and mobile phone usage: Digital divides of usage, adoption, and dropouts. Telecommunications Policy, 27(8), 597–623.

Rubel, A., & Biava, R. (2014). A framework for analyzing and comparing privacy states. Journal of the Association for Information Science and Technology, 65(12), 2422–2431.

Rubel, A., & Jones, K.M.L. (2016). Student privacy in learning analytics: An information ethics perspective. The Information Society, 32(2), 143–159.

Sánchez, D., & Batet, M. (2016). C-sanitized: A privacy model for document redaction and sanitization. Journal of the Association for Information Science and Technology, 67(1), 148–163.

Shi, P., Xu, H., & Chen, Y. (2013). Using contextual integrity to examine interpersonal information boundary on social network sites. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 35–38). New York: ACM.

Squicciarini, A.C., Xu, H., & Zhang, X. (2011). CoPE: Enabling collaborative privacy management in online social networks. Journal of the American Society for Information Science and Technology, 62(3), 521–534.

Stanley, L.D. (2003). Beyond access: Psychosocial barriers to computer literacy special issue: ICTs and community networking. The Information Society, 19(5), 407–416.

Stern, T., & Kumar, N. (2014). Improving privacy settings control in online social networks with a wheel interface. Journal of the Association for Information Science and Technology, 65(3), 524–538.

Thaler, R.H., Sunstein, C.R., & Balz, J.P. (2013). Choice architecture. In The behavioral foundations of public policy (pp. 428–439). Princeton, NJ: Princeton University Press.

Treem, J.W., & Leonardi, P.M. (2013). Social media use in organizations: Exploring the affordances of visibility, editability, persistence, and association. Annals of the International Communication Association, 36 (1), 143–189.

Van Dijk, J.A.G.M. (2005). The deepening divide: Inequality in the information society. Thousand Oaks: Sage.

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

Vitak, J., Blasiola, S., Patil, S., & Litt, E. (2015). Balancing audience and privacy tensions on social network sites. International Journal of Communication, 9, 1485–1504.

Vitak, J., Liao, Y., Subramaniam, M., & Kumar, P. (2018). "I knew it was too good to be true": The challenges economically disadvantaged internet users face in assessing trustworthiness, avoiding scams, and developing self-efficacy online. In Proceedings of the ACM: Human-Computer Interaction, 2(CSCW), Article 176, 1–25.

Wang, Y., Leon, P.G., Scott, K., Chen, X., Acquisti, A., & Cranor, L.F. (2013). Privacy nudges for social media: An exploratory facebook study. In Proceedings of the 22nd International Conference on World Wide Web (pp. 763–770). New York.

Westin, A.F. (1967). Privacy and freedom. New York: Atheneum.

Wu, P.F. (2019). The privacy paradox in the context of online social networking: A self-identity perspective. Journal of the Association for Information Science and Technology, 70(3), 207–217.

Zhang, S. (2016). Scientists are just as confused about the ethics of big-data research as you. Wired Magazine. Retrieved from https://www.wired.com/2016/05/scientists-just-confused-ethics-big-data-research/

Zimmer, M. (2008). Privacy on planet Google: Using the theory of contextual integrity to clarify the privacy threats of Google's quest for the perfect search engine. Journal of Business & Technology Law, 3(1), 109–126.

Zimmer, M. (2016). OkCupid study reveals the perils of big-data science. Wired Magazine. Retrieved from https://www.wired.com/2016/05/okcupid-study-reveals-perils-big-data-science/

Zimmer, M. (2018). Addressing conceptual gaps in big data research ethics: An application of contextual integrity. Social Media + Society, 4(2), 1–11.