Marquette University
e-Publications@Marquette

Computer Science Faculty Research and Publications | Computer Science, Department of

9-2020

Editorial introduction: “Information privacy in the digital age”

Michael Zimmer

Jessica Vitak

Philip Wu

Follow this and additional works at: https://epublications.marquette.edu/comp_fac

Marquette University

e-Publications@Marquette

Computer Science Faculty Research and Publications/College of Arts and Sciences

***This paper is NOT THE PUBLISHED VERSION*.**
Access the published version via the link in the citation below.

Journal of the Association for Information Science and Technology, Vol. 71, No. 9 (September 2020): 997-1001. DOI. This article is © Wiley and permission has been granted for this version to appear in e-Publications@Marquette. Wiley does not grant permission for this article to be further copied/distributed or hosted elsewhere without express permission from Wiley.

Editorial introduction: “Information privacy in the digital age”

Michael Zimmer
Department of Computer Science, Marquette University, Milwaukee, Wisconsin
Jessica Vitak
College of Information Studies, University of Maryland, College Park, Maryland
Philip Wu
School of Business and Management, Royal Holloway University of London, Egham, Surrey, UK

If nothing else, the events of 2020 have highlighted a diverse set of privacy-based research questions for information and social scientists to explore. Consider two examples. First, the global coronavirus pandemic has led to governments and technology companies considering a wide range of tools to track the spread of the disease. Google and Apple's exposure notification system is especially notable for its focus on privacy-preserving practices, including using encryption and relying on Bluetooth rather than GPS; however, concerns about some data collection practices, as well as future uses of the data, remain. Second, the Black Lives Matter protests that emerged in the United States following the murder of George Floyd, an unarmed black man killed by police, have spread across the globe, leading to discussions about how social media platforms, drones, and other technologies are being used to surveil citizens. In both of these examples, there is a clear tension between developing and using

technology for social goods and how that same technology might give rise to new threats to privacy. These examples also point to the highly contextual nature of privacy, suggesting that decisions about whether a given data flow is acceptable need to account for a variety of factors ranging from who is collecting the data to the broader purpose of data collection. Considering these recent events, this *JASIST* special issue on "Information Privacy in the Digital Age" seems all too timely.

In our JASIST opinion framing this special issue (Wu, Vitak, & Zimmer, 2020), we argued for a more contextual approach to thinking about privacy (Nissenbaum, 2010, 2019), and detailed three core areas of privacy research that need to be expanded. First, we called for more engagement with "networked privacy" (Marwick & boyd, 2014), the notion 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. Second, we called for greater attention to how increased pressures on privacy rights might impact marginalized communities, including those at low socio-economic status, people of color, members of the LGBTQ+ community, those with stigmatized health conditions or chronic illnesses, or who might be living in authoritarian regimes. And third, we called for the need to grapple with the complex global nature of information flows and regulations, recognizing that privacy expectations and practices differ greatly across geopolitical borders.

These themes are even more important given current events, and the contributions collected in this special issue, while written in 2019, address each theme with an intellectual and interdisciplinary rigor that helps us better understand the privacy threats emerging in 2020 and beyond. Below, we summarize the 10 articles in this special issue, loosely organizing them around these themes while acknowledging that most articles span multiple themes.

1 PANDEMIC CONSIDERATIONS: PRIVACY IN HEALTH CONTEXTS

In our timely opening article, "Disaster Privacy/Privacy Disaster," Sanfilippo, Shvartzshnaider, Reyes, Nissenbaum, and Egelman (2020) explore how privacy expectations during emergency situations differ from normal circumstances. Mirroring the development of contact-tracing apps to help monitor the COVID-19 pandemic, the authors note how increased information flows during disasters might increase violations of privacy at both individual and community levels. Motivated by a 2019 incident when the U.S. Federal Emergency Management Agency (FEMA) inappropriately disclosed sensitive location and banking data of national disaster victims to outside contractors, the authors analyzed 15 apps that were recommended to users during disasters. They identify numerous gaps between the privacy regulations and policies governing such apps and the actual information flows generated by the platforms, noting that information flows "beyond trusted parties and beyond the disaster context." They argue that the vulnerability of disaster victims generates particular needs to ensure specific rules to govern the appropriate flows of personal information within such difficult contexts, a concern even more apparent given the current global pandemic.

Another contribution appropriate for our current challenges with the COVID-19 pandemic is "'To protect my health or to protect my health privacy?' A mixed-methods investigation of the privacy paradox," in which Fox (2020) investigates the complicated arrangement of privacy concerns and perceived benefits when users consider adopting mobile health apps. Through both quantitative surveys and qualitative interviews, Fox reveals that users had strong concerns regarding unauthorized

secondary use or data outside the healthcare context, including unauthorized access to health data and the general lack of control of who might gain access to their health data. Her findings also warn that some might withhold certain data to protect their privacy given concerns about who might gain access to their electronic health records and how it might be used outside the healthcare context. Fox's study reveals that while the perceived benefits of mobile health apps positively influenced their willingness to adopt new digital health platforms, there was great concern over the potential leakage of data outside the healthcare context, and worry that app developers might not respect the transmission principles typically found in the healthcare setting. Fox's analysis also highlights the challenges of users managing their privacy when information flows becoming increasingly dictated by the platforms and networks within which we interact. This premise, central to the notion of "networked privacy," is discussed numerous other contributions.

2 CONNECTIONS AND CONTEXTS: NETWORKED PRIVACY

Bawden and Robinson's (2020) conceptual piece draws upon Luciano Floridi's philosophy of information to reflect on how to build privacy into models of information behavior and information literacy, both topics central to the discipline of library and information studies (LIS). As the authors show, there is a parallel between Floridi's ethics-based theorization of information and the contextual approaches advocated by various privacy scholars. In Floridi's "infosphere," the context would include other individuals, social groups, technology objects, and a plethora of informational entities that need protection and respect. This means, as Bawden and Robinson put it, "any group, including those defined by algorithm, may be just as valid an entity as an individual in the sense of being defined by their information, and hence just as entitled to informational privacy." Yet, privacy protection is not merely about "access" and "control"; rather, it is "a function of the informational friction in the infosphere" where the free flow of information is facilitated or constrained by technology, people, and norms and regulations. This again reminds us of Nissenbaum's (2010) fundamental thesis of contextual integrity: privacy is the appropriate flow of personal information. As Bawden and Robison's privacy vignettes—and the empirical studies by Jones et al. and Rieks et al., also in this volume—have shown, information flows in various networked systems can create frictions that undermine the contextual integrity of privacy.

Student data is increasingly networked as technologies enable data collection and sharing with many groups, including the students and teachers, as well as parents, administrators, and others. In higher education, this collection and analysis of student data to predict a variety of outcomes is known as "learning analytics" (LA), and several scholars have identified privacy concerns about the data being collected and the inferences being drawn by universities. In "'We're being tracked at all times': Student perspectives of their privacy in relation to learning analytics in higher education," Jones et al. (2020) focus on an often-ignored stakeholder in this process—the students' whose data is being collected and analyzed. They note that "privacy must be considered part of the success calculus of LA initiatives, but the treatment of privacy has at times been thin and under-represented." Therefore, this paper presents important insights—through interviews with more than 100 students across eight U.S. universities—into students' knowledge of and privacy concerns regarding LA. Findings highlight a lack of data privacy literacy and knowledge, especially regarding student data collection practices, but an underlying trust that their institutions are using the data in responsible and beneficial ways.

The rapid expansion of the Internet of Things (IoT) within homes has brought with it a similar expansion in the amount of potentially sensitive data being continuously collected and shared with providers and third parties. Smart electric meters, for example, can potentially improve efficiency and reduce emissions but also generate data that can be used to infer private activities normally hidden within one's home. This networked privacy concern is the focus of “Risks, Benefits, and Control of Information: Two Studies of Smart Electric Meter Privacy,” where Rieks, Dedrick, and Stanton (2020) engage in a mixed-method investigation of how U.S. consumers perceive privacy issues related to smart meters. In eight focus groups across four U.S. cities, research participants were shown a set of narratives—brief stories, combining text, data, graphics, and video—that highlighted various aspects of smart meter data collection and use, and then were asked to react to what they have seen. In each session, the authors reported that “privacy issues and concerns were raised spontaneously by group members.” Building from these results, the authors also conducted an experimental test to measure whether varying what a utility did with smart meter data would impact customers' perceived benefit, perceived risk and perceived control over their data. They found that sharing smart meter data with a third party increased the sense of risk but had no discernible impact on perceived control or benefits. Their findings suggest that utilities need to better inform their customers of what smart meters do, what benefits they can provide, and how their data is collected, used, and shared.

3 PRIVACY CONSIDERATIONS FOR MARGINALIZED GROUPS

In “I Don't Want Someone to Watch Me While I'm Working”: Gendered Views of Facial Recognition Technology in Workplace Surveillance,” Stark, Stanhaus, and Anthony (2020) examine perceptions of facial recognition technologies in the workplace through a secondary analysis of a Pew Internet dataset. The authors note critical concerns related to increased use of surveillance and monitoring technologies in the workplace, including function creep, whereby the scope of data use is expanded as more data can be collected. In their analysis, the authors focus on self-identified gender differences in the perceived acceptability of facial recognition technologies used at work to reduce theft, noting that research on gender and power highlight significant differences between men's and women's attitudes toward surveillance. Their findings support past work that women are much less accepting of this surveillance; however, men and women expressed similar attitudes about privacy. Interpreting their findings through the lens of contextual integrity, the authors discuss an important gender difference, finding that women expressed much greater concern than men for themselves as a data subject. This suggests that women have particular concerns about workplace surveillance and these differences should be considered when companies adopt technologies to monitor their employees.

Quan-Haase and Ho (2020) express concern that most research on online privacy focuses on young adults, while the privacy concerns and practices of older adults, those aged 65 and older, are overlooked. Thus “we have only a rudimentary understanding” of this growing community of internet users who are too often characterized as “passive,” and risk being overlooked by technology developers and policymakers. Their contribution, “Online Privacy Concerns and Privacy Protection Strategies Among Older Adults in East York, Canada” is a step toward ensuring older adults are properly understood as internet users who actively engage with managing their privacy. Through interviews with 101 older adults from East York, Ontario, Canada, the authors find that older adults' privacy concerns differ from younger generations, with a greater emphasis placed on security and

institutional privacy, rather than privacy across social networks. And rather than being passive internet users, their findings revealed that older adults actively countered potential privacy threats by avoiding some social networking platforms, limiting the amount of personal information they share online, and relying on hardware and software solutions to help manage their privacy. The implications of this work include supporting the design of technologies that older adults will be more willing to adopt so long as they address the types of privacy concerns that matter to this population. Technology designers need to treat older adults as active internet users who are willing to take specific actions to support their particular privacy needs.

4 BEYOND THE UNITED STATES: GLOBAL PRIVACY CONSIDERATIONS

The rise of smart cities—which rely on various technologies and sensors to collect and analyze data with the goal of creating "data-driven urbanism"—provides a useful example in the different ways data privacy is imagined and enacted at a large scale. In "#BlockSidewalk to Barcelona: Technological Sovereignty and the Social License to Operate Smart Cities," Mann, Mitchell, Foth, and Anastasiu Cioaca (2020) compare two approaches—Google's Sidewalk Labs development in Toronto and Barcelona's Digital City plan. As the authors note, the development of smart cities requires a symbiotic relationship between the cities and the technology companies; however, there are critiques that this "ongoing corporatization of urban governance has done little to ameliorate deeply rooted social problems." The authors frame these corporate-related privacy concerns as "anxieties of control," which reflect citizens' desire to know what data is being collected about them and direct the flow of their data. They suggest the pushback against Sidewalk Labs in Toronto resulted from anxieties regarding Google's plans for data collection, as well as Google's inability to obtain buy-in from the community. The authors contrast Toronto with Barcelona's focus on "technological sovereignty," where control is centered in the community's hands rather than a corporate entity. Technological sovereignty provides citizens with greater autonomy and control over data by inverting power relationships between governments, citizens, and companies and provides more opportunities for citizens to decide what data will be collected and how it will be used.

In her contribution, "The Personal Information Sphere: An Integral Approach to Privacy and Related Information- and Communication Rights," Eskens (2020) outlines how European Union (EU) law provides various fundamental privacy rights: confidentiality, freedom of thought and the right to hold opinions, and the freedom to receive—or not receive—information. Eskens groups these rights into what she calls a "personal information sphere," which empowers people to take control over how they "situate themselves in networks of information and communication and how they interact and engage with online news media." Eskens argues that, even beyond protections put forward in laws like the EU's General Data Protection Regulation, controlling one's personal information sphere "is different from the kind of control enabled by data protection law, which focuses on consent, transparency, and data access rights." Instead, through her detailed discussion of algorithmic recommendation systems, Eskens argues for a more contextual approach to privacy regulation that focuses on fundamental rights beyond the limited scope of existing data protection rules.

Government surveillance practices vary by country, as do citizens' attitudes toward these practices. However, as Thompson, McGill, Bunn, and Alexander (2020) note, few studies have evaluated the role national culture plays in acceptance of government surveillance and engagement in privacy protection

strategies. Furthermore, the vast majority of research on this topic has focused on U.S. practices, while other parts of the world may have very different attitudes toward and practices around surveillance. To address this, the researchers focus on two countries that recently passed surveillance legislation: Australia and Sri Lanka. These countries also differ culturally in two key areas related to privacy: individualism/collectivism and power distance. Using survey data collected in each country, the authors find significant differences between the two samples. Notably, Australians' privacy concerns about data collection predicted their acceptance of government surveillance, but those concerns were unrelated to Sri Lankans' acceptance. On the other hand, privacy concerns about secondary data use were unrelated to surveillance acceptance for participants in both countries. The authors also highlight how cultural norms—and specifically power distance—are important to consider when evaluating citizens' attitudes toward government surveillance practices.

Taken together, these 10 papers showcase cutting-edge research on information privacy in the JASIST community. With intellectual sophistication and empirical richness, the papers cover various contexts in which privacy is examined, be it social, cultural, or technological. We hope this special issue not only deepens our understanding of information privacy in the digital age, but also inspires future research that makes a meaningful impact on the academic community and beyond.

REFERENCES

Bawden, D., & Robinson, L. (2020). “The dearest of our possessions”: Applying Floridi's information privacy concept in models of information behavior and information literacy. *Journal of the Association for Information Science and Technology*, 71(9), 1030– 1043.

Eskens, S. (2020). The personal information sphere: An integral approach to privacy and related information and communication rights. *Journal of the Association for Information Science and Technology*, 71(9), 1116– 1128.

Fox, G. (2020). “To protect my health or to protect my health privacy?” a mixed methods investigation of the privacy paradox. *Journal of the Association for Information Science and Technology*, 71(9), 1015– 1029.

Jones, K. M., Asher, A., Goben, A., Perry, M. R., Salo, D., Briney, K. A., & Robertshaw, M. B. (2020). “We're being tracked at all times”: Student perspectives of their privacy in relation to learning analytics in higher education. *Journal of the Association for Information Science and Technology*, 71(9), 1044– 1059.

Mann, M., Mitchell, P., Foth, M., & Anastasiu Cioaca, I. (2020). # BlockSidewalk to Barcelona: Technological sovereignty and the social license to operate smart cities. *Journal of the Association for Information Science and Technology*, 71(9), 1103– 1115.

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

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

Nissenbaum, H. (2019). Contextual integrity up and down the data food chain. *Theoretical Inquiries in Law*, 20(1), 221– 256.

Quan-Haase, A., & Ho, D. (2020). Online privacy concerns and privacy protection strategies among older adults in East York, Canada. *Journal of the Association for Information Science and Technology*, 71(9), 1089– 1102.

Rieks, A. R., Dedrick, J., & Stanton, J. (2020). Risks, benefits, and control of information: Two studies of smart electric meter privacy. *Journal of the Association for Information Science and Technology*, 71(9), 1060– 1073.

Sanfilippo, M., Shvartzshnaider, Y., Reyes, I., Nissenbaum, H., & Egelman, S. (2020). Disaster privacy/privacy disaster. *Journal of the Association for Information Science and Technology*, 71(9), 1002– 1014.

Stark, L., Stanhaus, A., & Anthony, D. L. (2020). "I don't want someone to watch me while I'm working": Gendered views of facial recognition technology in workplace surveillance. *Journal of the Association for Information Science and Technology*, 71(9), 1074– 1088.

Thompson, N., McGill, T., Bunn, A., & Alexander, R. (2020). Cultural factors and the role of privacy concerns in acceptance of government surveillance. *Journal of the Association for Information Science and Technology*, 71(9), 1129– 1142.

Wu, P. F., Vitak, J., & Zimmer, M. (2020). A contextual approach to information privacy research. *Journal of the Association for Information Science and Technology*, 71(4), 485– 490.