Selected Papers of #AoIR2020:
The 21st Annual Conference of the
Association of Internet Researchers
Virtual Event / 27-31 October 2020

LAYERS OF "NETWORKED PRIVACY": CONTEXT COLLAPSES ACROSS RELATIONS, TECHNOLOGIES, INSTITUTIONS, AND DATA

Jeeyun (Sophia) Baik
University of Southern California

Introduction

Informational privacy means an ability of individuals to self-determine their information flow by controlling the data's whereabouts (Westin, 1966). The understanding of privacy has constantly evolved as new communication technologies introduce a set of problems that go beyond traditional settings one's privacy is expected (Igo, 2018). "Networked privacy" (boyd & Marwick, 2011; Marwick & boyd, 2014) is one of the frameworks that theorize what privacy looks like in the digital era characterized by popular social media platforms. Marwick and boyd (2014) suggest considering "ongoing negotiation of contexts…[where] contexts regularly blur and collapse" (p. 1063) in the networked new media environment. While "networked privacy" as suggested by Marwick and boyd (2014) provides a useful lens to analyze privacy challenges arising with new media in terms of *horizontal* privacy–privacy of individuals from other individuals like family members or friends (Quinn & Epstein, 2018), it does not address *vertical* privacy–privacy of individuals from institutions such as government or corporations.

This paper seeks to expand the "networked privacy" framework, identifying different areas of "context collapses" in the current networked information environment. It includes the original dimension of (1) interpersonal relations and additional layers of (2) technologies, (3) institutions, and (4) data. By doing so, this study teases out multiple layers of networked contexts that complicate privacy and regulations thereof in recent years. That is, the extended framework is aimed to more holistically investigate the moments "collision of information norms" occurs (Marwick and boyd, 2014, p. 1054). Marwick and boyd (2014) emphasize that "information norms and contexts are co-constructed by participants and frequently shifting" (p. 1064), and we are at a critical juncture where information norms are becoming enshrined in privacy regulations in different parts of the world including the EU's GDPR (General Data Protection Regulation) and the CCPA (California Consumer Privacy Act) in the U.S. As such, understanding complex layers of context collapses can shed light on the legal grey areas that would need further examination and sophistication.

Suggested Citation (APA): Baik, J. (2020, October). Layers of "Networked Privacy": Context Collapses Across Relations, Technologies, Institutions, and Data. Paper presented at AoIR 2020: The 21th Annual Conference of the Association of Internet Researchers. Virtual Event: AoIR. Retrieved from http://spir.aoir.org.

Method

The study collected U.S. news media articles published between January 2018 and June 2020: the period encompasses key moments such as the Cambridge Analytica scandal and enforcements of GDPR and CCPA. I collected news on digital privacy published by the 2018 U.S. top newspapers via MediaCloud, which resulted in 5,874 articles. I sampled 300 articles for close qualitative examinations: the first top 150 articles were selected based on Facebook share counts, and the remaining 150 articles were solicited by randomly selecting 5 articles from each month during the 30-month-long period. I conducted a Critical Discourse Analysis (CDA) (Fairclough, 2013) on the sampled articles, exploring any layers/moments of "context collapses" with regard to privacy.

Findings and Discussion

The key component of the original "networked privacy" framework is (1) networked *relations*. People are connected to others coming from separate contexts on digital platforms. For example, even if a teenager posts about one's school drama on Facebook expecting only friends would respond, a concerned family member may go on to reply (Marwick and boyd, 2014). Digital platforms usually provide different privacy settings to their users, but the settings would vary across all the people one is networked with, challenging the person's particular expectation of privacy. Basically, the management of self-presentation goes through a "context collapse" as diverse relationships merge in one digital platform. In this regard, the news coverage was presenting issues such as online revenge porn and digital surveillance of students by parents and schools. A context of an interpersonal action can be misappropriated online in other contexts, reinforced by power dynamics.

The original "networked privacy" concept also points out that privacy can be violated by "a system's technical architecture" (Marwick and boyd, 2014, p.1062). For instance, a platform's default privacy setting may be frequently changing and challenge one's boundary management. My analysis of news coverage suggests that privacy issues around such technical elements are not limited to one platform's architecture. The layer of (2) networked *technologies* instead includes *partnerships* among companies as to a feature (e.g., one can simultaneously upload to Instagram, Facebook, Twitter, and Tumblr) or a business model (e.g., sharing of user data among partners), or *mergers* between companies (e.g., Facebook acquired Instagram), all of which create a deeply networked technical architecture individuals may likely find hard to navigate.

The growing entanglement of data practices between the private and the public sectors introduces another type of "context collapse" around (3) networked *institutions* as well. States have long collected data about citizens for the sake of governance, yet the scale and type of data they obtain and use are far encroaching on personal data garnered by private companies. A "market for consumer data" has been created across institutions by data brokers partnering with both the private sector and state agencies (Crain, 2018, p. 99). The Cambridge Analytica scandal in 2018, covered heavily in my dataset, was a

sensational case that showed the unprecedented extent personal data collected by a private firm can be used by political actors supposed to serve public interests.

Moreover, it is not necessarily a piece of personally identifiable information (PII) these networked institutions look for; what matters is (4) networked *data* gleaned from lots of individuals (Tisne, 2018). That is, the "economic value of personal data is largely realized in the aggregate" when "data points are linked together through data analytics" (Cinnamon, 2017, p. 615). People are generally targeted for their membership in specific social groups, rather than for their purely individual identities (Eubanks, 2018). Therefore, one type of personal data collected in a specific context is put together with the other types of personal data captured in a separate context, creating a "context collapse" again.

Conclusion

Privacy is a "collective value" as it can be guaranteed when all the people have "a similar minimum level of privacy" (Regan, 1996, p. 213). Rethinking the framework of "networked privacy," I argue, can help us better ensure the similar minimum levels of privacy across *relations, technologies*, *institutions*, and *data*. As we negotiate the rules to protect data privacy along various regulatory efforts, the extended concept of networked privacy could provoke conversations in privacy rulemaking to identify the multi-layered networked privacy harms emerging in different context collapses.

References

Cinnamon, J. (2017). Social Injustice in Surveillance Capitalism. *Surveillance & Society*, *15*(5), 609–625.

Crain, M. (2018). The limits of transparency: Data brokers and commodification. *New Media & Society*, *20*(1), 88–104.

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

Fairclough, N. (2013). *Critical discourse analysis: The critical study of language*. Routledge.

Igo, S. E. (2018). *The Known Citizen: A History of Privacy in Modern America*. Harvard University Press.

Maier, D., Waldherr, A., Miltner, P., Wiedemann, G., Niekler, A., Keinert, A., Pfetsch, B., Heyer, G., Reber, U., Häussler, T., Schmid-Petri, H., & Adam, S. (2018). Applying LDA Topic Modeling in Communication Research: Toward a Valid and Reliable Methodology. *Communication Methods and Measures*, *12*(2–3), 93–118.

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

Quinn, K., & Epstein, D. (2018). #MyPrivacy: How Users Think About Social Media Privacy. *Proceedings of the 9th International Conference on Social Media and Society*, 360–364.

Tisne, M. (2018, December 14). It's time for a Bill of Data Rights. *MIT Technology Review*. https://www.technologyreview.com/s/612588/its-time-for-a-bill-of-data-rights/

Westin, A. F. (1966). Science, privacy, and freedom: Issues and proposals for the 1970's. Part I--The current impact of surveillance on privacy. *Columbia Law Review*, *66*(6), 1003–1050.