Selected Papers of #AoIR2017:
The 18th Annual Conference of the
Association of Internet Researchers
Tartu, Estonia / 18-21 October 2017

TOWARDS A NETWORKED PRIVACY PARADIGM: ASSUMPTIONS AND IMPLICATIONS

Ralf De Wolf
imec-MICT-Ugent

Rob Heyman
Imec-SMIT-Ugent

In the last decade, many researchers have studied privacy in the context of new media, often inspired by *individual* (e.g., Warren and Brandeis, 1890; Westin, 1967) or *contextual* privacy theory (e.g., Nissenbaum, 2004, 2010; Petronio, 1991, 2010). Individual conceptualizations employ a restricted access or control conceptualization. In addition, contextual privacy theory also accentuate the importance of the environment and other people when conceptualizing privacy. Recently, a *networked* perspective on privacy is suggested that takes into account the affordances and dynamics of networked publics (Marwick and boyd, 2014; Vitak et al., 2015; Hargittai and Marwick, 2016) where privacy is defined as an "ongoing negotiation of contexts in a networked ecosystem in which contexts regularly blur and collapse" (Marwick and boyd, 2014 p.13). That said, it is unclear what makes networked privacy new, how it relates to previous established frameworks and what are its implications. In a critical literature review we therefore analyze and compare Warren and Brandeis' right to be let alone, Westin's privacy control, Nissenbaum's contextual integrity, Petronio's communication privacy management theory and recent work on networked privacy. Rather than providing an exhaustive framework of all theoretical perspectives we focus on how privacy is approached with the goal of further theorizing a networked perspective on privacy. Our main research questions are as follows:

RQ1: How does networked privacy relate to earlier established privacy frameworks?
RQ2: What are the assumptions and implications of networked privacy?

Suggested Citation (APA): De Wolf, R. & Heyman, R. (2017, October 18-21). *Towards a Networked Privacy Paradigm: Assumptions and Implications*. Paper presented at AoIR 2017: The 18th Annual Conference of the Association of Internet Researchers. Tartu, Estonia: AoIR. Retrieved from http://spir.aoir.org.

Our study shows how networked privacy is different in some fundamental epistemological and ontological assumptions. Contrary to Warren and Brandeis (1890) who focus on the negative effects of technological advances on individual's privacy and the right to be let alone, it is noticeable how a networked perspective is more descriptive and less judgmental when describing privacy: "how are individuals or groups managing privacy in networked publics and what are the factors influencing these decisions?" can be seen as the pivotal question. Second, whereas Westin (1967) and Altman (1975) describe privacy as selective control of access to the self or optimizing between the withdrawing or disclosing of information, a network perspective assumes individuals to be fallible agents with only partial knowledge of the networked context. Third, a networked perspective takes the affordances of networked publics as a given as well as the sociability that constitutes a networked self. Hence, context collapse and invisible audiences are not necessarily perceived as problematic for privacy management.

In addition to its contribution to privacy theory, our critical literature review also clarifies the implications a networked environment has for people's privacy management, privacy technology and public policy.

Managing privacy has always been dialectical and requires an ongoing process of opening and closing boundaries (Petronio, 2002), but with the emergence of networked technologies where temporal, spatial and social boundaries are very open and fluid, the ongoing negotiation of boundaries should be given a greater emphasis. After all, individuals have to coordinate this openness, which can be considered both an opportunity and burden. Technical skills are necessary but not sufficient for adequate privacy management. People need to know how the networked context influences their privacy management. The latter implies social skills in the form of boundary reflexivity and communicating with others to construct norms about networked privacy.

Next to hiding and controlling users also need to understand the networked environment and the role they are attributed for adequate privacy management to be possible. The latter has two implications for the further development of privacy technology. First, privacy technology should not only focus on restricting access or controlling information, but also on making users aware of the networked self, the collapsed and networked audiences and the ways service providers operate as a curator. Users need to be aware of the networked environment, have agency in controlling the social situation, free from surveillance or interference for which no consent is given. A second implication, and requirement to the first implication, is that a shift in perspective is necessary from "users need protection because of their limited capabilities" to "users need transparency, control and protection to support and facilitate their privacy management". The latter perspective acknowledges the reflexive role that is required rather than underlining the bounded rationality of users.

Acquisti et al. (2015, p.514) believe that a baseline framework of privacy protection is also necessary besides offering control options and transparency. An increased reflexivity is required of users for adequate privacy management, but protection is also needed to prevent that reflexivity from becoming excessive. Certainly when users are treated as an object (top-down surveillance and commodification) the goal of public policy should be to balance the relationship more equally and involve users as an active agent in the negotiation process. However, it is also needed to meet the limited capabilities of users and offer clear principles on privacy protection.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. doi:10.1126/science.aaa1465

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding.* Monterey, CA: Brooks/Cole.

boyd, danah, & Marwick, A. E. (2011). Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies. Presented at the Proc. A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society. Retrieved from http://papers.ssrn.com/abstract=1925128

Hargittai, E., & Marwick, A. (2016). "What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy. International Journal of Communication, 10, 3737-3757.

Marwick, A. E., & boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*(7), 1051–1067. doi:10.1177/1461444814543995

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, *79*(1), 119–158.

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford Law Books.

Petronio, S. (1991). Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information Between Marital Couples. *Communication Theory*, *1*(4), 311–335. doi:10.1111/j.1468-2885.1991.tb00023.x

Petronio, S. (2002). *Boundaries of Privacy: Dialectics of Disclosure*. Albany: State University of New York Press.

Vitak, J., Wisnieuwski, P., Page, X., Lampinen, A., Litt, E., De Wolf, R., Gage Kelley, P., & Sleeper, M. (2015). The future of networked privacy: challenges and opportunities. Proceedings of the 18th ACM Conference Companion on Computer Cooperative Work & Social Computing, ACM press, New York 267 -272.

Warren, S., & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193–220.

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