Privacy Literacy: Extending Information Literacy in the Age of Social Media and Big Data

Zablon Pingo and Bhuva Narayan
University of Technology Sydney, Australia

Abstract
This paper argues that there is a need for extending the concept of *information literacy* to include *privacy literacy*, which we conceptualise as the awareness and tools needed to understand and navigate our contemporary world of connected information and synergistic technologies whilst also protecting ones personal information. The paper is based on an interview study of participants in combination with online ethnographic observations of social media, and a cognitive walkthrough of their social media use.

Background

In our information age, all of our lives are increasingly monitored and configured by digital technologies (Lupton, 2015) and this has implications on the goods and services we receive, including health, car, and home insurance (Pingo & Narayan, 2016). Google, Facebook, Twitter, and YouTube provide platforms for people to create a personal profile, share information, link to others, befriend strangers, connect with others, subscribe to channels, and follow people. This involves the sharing of personal information for verification that is later used to profile individuals for advertisements and other purposes (Buchman, 2013; Meikle, 2016). Such massively generated data from use of digital devices or applications is referred to as "big data" (Agnellutti, 2014), with a huge trend in data mining and machine learning in order to understand users' preferences, and behaviour patterns. Such personal information can potentially be used beyond intended purposes (Pierson, 2012), and has sparked discussions on how they simultaneously empower and disempower users in various ways, creating opportunities and exposing users to vulnerabilities (Christiansen, 2011; Pierson, 2012; Rosenblat, Kneese, & Boyd, 2014). They also point to a shift in the responsiility of privacy to the user as is evident from the messaging from the Office of the Australian Information Commissioner, which says 'privacy in your hands.' (OAIC, 2016). This raises the question of whether users have the awareness, knowledge, and tools to take privacy in their hands. Therefore, the research question this study addresses is: *Do everyday users of social media understand its implications for personal information privacy, and what measures do they take to protect their privacy?*

Conceptual framework

Westin (1967) defined privacy as 'the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'. The process of regulating privacy is a dynamic process of optimizing two psychological needs: the need to preserve one's privacy and control access to and distribution of personal information, and the need to interact socially, where one has to disclose personal information (Altman, 1975). Hence, privacy is constructed and negotiated in social processes (Solove, 2002).

Information privacy is often considered a technical design problem in information systems research (Cavoukian & Jonas, 2012, p. 863; Lehikoinen, 2008). Rather than this system-centred approach, Debatin (2011, p. 57) recommends that people need to develop an understanding of technology and its unintended consequences. In other words, users of digital technologies need to develop an *informed concern* about their privacy, avoiding both moral panic and ignorant or naïve indifference towards information technologies (Debatin, 2011, p. 57). Christiansen (2011) notes two distinct information sharing practices which users of technologies need to know or understand: voluntary sharing and involuntary disclosures.

Debatin (2011) defines privacy literacy as 'an informed concern for individuals privacy and effective strategies to protect it'. From an information literacy perspective, privacy literacy is proposed as one's level of understanding and awareness of how personal information is tracked and used in online environments, and how information can retain or lose its private nature (Givens, 2015, p. 53). Möllers and Hälterlein's (2013) argue that people need to exhibit active participation in negotiating for their privacy through understanding what is at stake when using digital technologies. When people use digital devices or applications, they need to decide on whether to give personal information by consciously considering the terms and conditions of the service (Debatin, 2011), which often requires high-level cognitive effort, which users hardly have the time or the tools for (Gindin, 2009; Solove, 2012), and hence avoid engaging with it. This information avoidance is a stress and coping method deployed by humans to deal with cognitive dissonance or is a result of cognitive bias (Case, Andrews, Johnson, & Allard, 2005). Narayan, Case, and Edwards (2011) note that 'people tend to seek out information that agrees with their pre-existing world-view and cognitive skill levels rather than acknowledge or seek new information that may cause an uncomfortable conflict in their minds'. The negotiated nature and commodification of privacy (Barnes, 2006; Thrift, 2005) causes such a cognitive dissonance and hence attracts information behaviour perspectives. The reason people avoid this information is not deliberate, but due to the sheer amount of time needed to read the privacy terms and the complexity of the language [and the interfaces] used (Potter, 2015).

Methodology

Perik, de Ruyter, and Markopoulos (2005) noted that there is a methodological problem especially in the domain of privacy in computer-mediated communication research. In a study of people's information privacy perceptions though observations of actual use of a system, many respondents demonstrate risk-taking behaviours compared to interview responses (van de Garde-Perik, 2009, p. 21). To address these issues, a triangulation of methods was used in our study (Yin, 2013); we used a combination of online observations or *digital ethnography* (Talip, Narayan, Edwards, & Watson, 2015) and cognitive walkthroughs (Blackmon, 2004) alongside interviews with participants about their perceptions, awareness, and use of social media. Six university students participated in this study.

Findings

Findings show that privacy is a negotiated process wherein users decide on how much personal information they want to disclose online, and for what returns. Participants also exhibited various information behaviours such as information avoidance, due to information overload and the lack of cognitive tools to process the information. The cognitive walkthrough revealed that the interface of social media sites was a huge issue also — they are designed to be seamless which also means that most users did not know how to work the privacy settings. That said, we found two distinct groups amongst the participants. Those who, when there are two competing needs, choose to ignore their need for privacy over the immediate gains they can get from a transaction or interaction, while others were so paranoid about their privacy that it inhibited their online social interactions. We believe that both of these groups can benefit from privacy literacy that helps them engage with the online world without compromising their personal information. This calls for a need to incorporate privacy literacy as an essential complement to information literacy.

References

Agnellutti, C. (2014). *Big Data: An Exploration of Opportunities, Values, and Privacy Issues*. New York: Nova Science Publishers, Inc.

Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Monterey: Brooks/Cole.

Blackmon, M. H. (2004). Cognitive Walkthrough. In W. S. Bainbridge (Ed.), Encyclopedia of Human Computer Interaction, 2 volumes (Vol. 1, pp. 104–107). Great Barrington, MA: Berkshire Publishing Group. Accessible from xhttp://autocww2.colorado.edu/~blackmon/Papers/CognitiveWalkEncycHCI2004.pdf

Buchmann, J. (2013). Internet Privacy: Options for adequate realisation. Springer Berlin Heidelberg.

Case, D. O., Andrews, J. E., Johnson, J. D., & Allard, S. L. (2005). Avoiding versus seeking: the relationship of information seeking to avoidance, blunting, coping, dissonance, and related concepts*. *Journal of the Medical Library Association*, *93*(3), 353.

Cavoukian, A. (2012). Privacy by design. Retreived from https://www.ipc.on.ca/wp-content/uploads/Resources/PbDBook-From-Rhetoric-to-Reality.pdf

Christiansen, L. (2011). Personal privacy and Internet marketing: An impossible conflict or a marriage made in heaven? *Business Horizons*, *54*(6), 509-514.

Clark, I. (2016). The digital divide in the post-Snowden era. Journal of Radical Librarianship, [S.l.], v. 2, mar. 2016. Available at: https://journal.radicallibrarianship.org/index.php/journal/article/view/12

Debatin, B. (2011). Ethics, privacy, and self-restraint in social networking. In Trepte, S., & Reinecke, L. (2011). *Privacy online: Perspectives on privacy and self-disclosure in the social web*. Springer Science & Business Media.

Gindin, S. E. (2009). Nobody reads your privacy policy or online contract: Lessons learned and questions raised by the FTC's action against Sears. Nw. J. Tech. & Intell. Prop., 8, 1.

Givens, C. L. (2015). *Information Privacy Fundamentals for Librarians and Information Professionals*: Rowman & Littlefield.

Haynes, D., & Robinson, L. (2015). Defining user risk in social networking services. *Aslib Journal of Information Management, 67*(1), 94-115.

Lehikoinen, J. T. (2008). Theory and application of the privacy regulation model. In Lumsden, J. (ed.) *Handbook of Research on User Interface Design and Evaluation for Mobil Technology*, 863-876. Hershey, PA: IGI Global.

Lupton, D. (2015). *Digital sociology*: Routledge.

Meikle, G. (2016). *Social Media: Communication, Sharing and Visibility*: Routledge.

Narayan, B., Case, D. O., & Edwards, S. L. (2011). The role of information avoidance in everyday‐life information behaviors. *Proceedings of the American Society for Information Science and Technology*, 48(1), 1-9.

Office of the Australian Information Commissioner (OAIC). (2016). Retreived from https://www.oaic.gov.au/paw2016/

Perik, E., de Ruyter, B., & Markopoulos, P. (2005). *Privacy & Personalization: Preliminary Results of an Empirical Study of Disclosure Behavior*. Paper presented at the Proceedings of PEP, Edinburgh, UK.

Pierson, J. (2012). Online privacy in social media: A conceptual exploration of empowerment and vulnerability.

Pingo, Z., & Narayan, B. (2016). When Personal Data Becomes Open Data: An Exploration of Lifelogging, User Privacy, and Implications for Privacy Literacy In: Morishima A., Rauber A., Liew C. (eds) Digital Libraries: Knowledge, Information, and Data in an Open Access Society. ICADL 2016. *Lecture Notes in Computer Science*, vol 10075. Springer, Cham.

Posner, R. A. (1978). *Economic theory of privacy* (F. D. Schoeman Ed.): Cambridge University press.

Rosenblat, A., Kneese, T., & Boyd, D. (2014). Networked Employment Discrimination. *Open Society Foundations' Future of Work Commissioned Research Papers*. doi: http://dx.doi.org/10.2139/ssrn.2543507

Solove, D. J. (2012). Introduction: Privacy self-management and the consent dilemma. Harv. L. Rev., 126, 1880.

Solove, D. J. (2002). Conceptualizing privacy. *California Law Review*, 1087-1155.

Talip, B. A., Narayan, B., Edwards, S. L., & Watson, J. (2015). Digital Ethnography as a Way to Explore Information Grounds on Twitter. QQML: *Qualitative and Quantitative Methods in Libraries Conference*, 26-29 May 2015.

van de Garde-Perik, E. (2009). Ambient intelligence & personalization: people's perspectives on information privacy. Doctoral thesis. Eindhoven University. Available at http://repository.tue.nl/642224

Westin, A. F. (1967). *Privacy and freedom* (Vol. 25). New York: Athenaeum.

Yin, R. K. (2013). *Case study research: Design and methods*: Sage publications.