"It Works by *Not* Doing Things That Everybody Else Does": Designing for User Privacy

Monica G. Maceli
School of Information,
Pratt Institute
New York, NY USA 10011
mmaceli@pratt.edu

Abstract

Though protecting one's privacy is a common concern of users in today's world, the body of privacy-related literature suggests numerous paradoxes including: high privacy concerns, but little action; the use of protective tools increasing privacy concerns; and the effect of greater perceived control over one's data encouraging more sensitive information revealed. These existing findings, combined with the author's privacy-related research work, suggests numerous challenges for designers of privacy-sensitive interfaces, particularly in social settings. This workshop paper summarizes the author's related research findings, as well as poses challenges to be addressed by the proposed workshop.

Author Keywords

Privacy protection technology tools; privacy interfaces; information professionals; privacy actions and inactions; future challenges.

ACM Classification Keywords

H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

Introduction

Literature both within and outside of the field of Human-Computer Interaction (HCI) has emphasized the paradoxical and complex nature of users' privacy-related concerns, thoughts, actions and inactions. Though wide-scale studies, particularly within the USA, have clearly indicated that the average web user is highly concerned with their privacy in online and mobile environments [5,6], these studies tend to indicate little action on the part of users to improve their perceived state of threatened privacy, e.g. [1]. In this landscape, libraries - particularly public libraries - and human rights organizations - especially those oriented towards protecting vulnerable populations such as journalist or political dissidents - have been at the forefront of educating, advising, and assisting users in changing their behaviors and encouraging the use of privacy-protection technology tools.

This humanitarian work has tended to take a defensive approach in assuming the worst of websites, internet service providers, mobile apps, and others who share your network, and advocating for blanket protection using the available privacy-protection tools. Such tools may include using tracking-thwarting browser plugins, the use of virtual private networks (VPNs), using encrypted https websites, among other tools, as well as behavioral changes to avoid social exploits such as email phishing. To add confusion to this technical landscape, users must often pick and choose between privacy-protection tools with no one tool offering complete protection.

In contrast to this pragmatic educational approach, much of the designing-*for*-privacy awareness literature has focused on the users' interpretation of privacy policies, ability to effectively customize privacy settings (particularly in the social media context) [e.g. 7], and, in the mobile environment, the understanding of granting of permissions to mobile applications [e.g. 9]. Numerous design suggestions have emerged from such research, including the "privacy nutrition label" as a proposed standard for presenting privacy information to users [3].

The research findings are rife with paradoxical challenges, not limited to the high-concern-but-little-action issue related previously in [1]. Studies have also found that the use of privacy-protection tools in fact raises users' privacy concerns and suspicions, instead of allaying these fears, as might be expected [10]. And when users do employ systems that make them feel confident and in control of their personal information, they may be apt to reveal more sensitive information than they would otherwise [2].

Author's Related Work

In prior work [e.g. 4], the author has conducted a broad review of privacy-related literature in pursuit of developing a series of challenges for privacy educators to address, directed towards public libraries as an increasingly important educator in this area. This work was expanded in an empirical research study, currently under review for publication in another venue, exploring librarians' mental model of the function of the Internet and how that impacted their understanding and use of privacy-protection technology tools.

For the purposes of this study, 22 librarian participants from libraries local to the New York City area were recruited for the study. In individual sessions, participants were asked to complete a brief survey

describing their familiarity with privacy and technology-related concepts, draw their understanding of the Internet, use a series of privacy-protection technology tools, and then explain what (if any) effect the use of the tools had on their perceived function of the Internet. Sketching was used to elicit librarians' mental models of the Internet and how these processes differ when using the series of privacy-protection technology tools. A sample participant sketch is included in Figure 1, below.

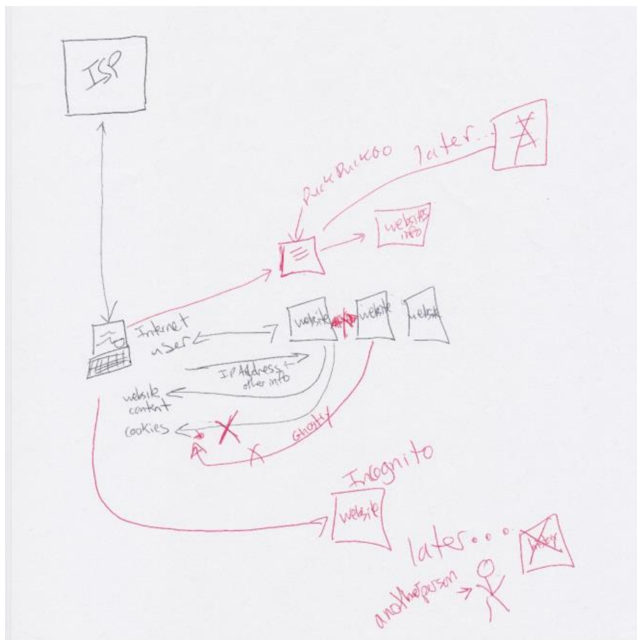

Figure 1: Participant's sketch of "how the Internet works", including the use of several privacy-protection technology tools

In nearly all participants studied, a significant mismatch was noted between participants' mental models of how the Internet and privacy-protection tools functioned and how they actually functioned. Though most participants reported conceptual understanding of technical terms such as cookie or IP address, more complex topics such as virtual private networks or SSL were poorly understood. Over half of participants' sketches were rated poor or fair by expert raters in the participant's ability to accurately express how the Internet functions. This led to troubling scenarios of use such as the perception that a privacy-protection tool was offering greater protection than it actually did (or could).

A particular challenge was reconciling their knowledge of what the tool did with what they could visually infer or see from the designed interface. As one participant said, when using a privacy-protection search engine: "I guess it works by not doing things that everybody else does." This difficulty extended into their understanding of the basic functioning of the Internet as well. This has been observed in prior work, such as in [8] where participants struggled to conceive the existence of the invisible underlying Internet infrastructure.

This research yielded several challenges for future privacy-related theory and design, including:

- Significant knowledge gaps in understanding Internet infrastructure and function in the public and in information professionals [e.g. as in 7]. Most notably, knowledge gaps that arose from the inability to conceptualize "invisible" infrastructure and functionality.
- Numerous barriers to the use of privacy-protection technology tools, including: difficulty in assessing developers'

trustworthiness, the constant need to keep pace with new threats, and the perception of increased user inconvenience.

- Difficulty in designing systems that effectively conveying the "privacy trustworthiness" of the tool.

Contribution to Workshop

Though the prior work presented here has sought to learn from the broader field of privacy research and tailor it to the needs of practicing librarians, their patrons, and communities, these groups are less involved in design and development activities and thus have little opportunities to contribute to the design of user-privacy-sensitive interfaces. However, these user groups can greatly inform our understanding of user needs and interface design for systems desiring to be transparent around privacy practices and data use. A notable finding of prior work, indicates that design challenges, such as showing what one is "not" doing are highly relevant in this domain.

Given that users may trust privacy-protection tools, without a great deal of underlying understanding, thoughtful privacy-related interface design is of upmost importance in this realm, particularly in the design of collaborative, social systems. This workshop offers the potential to bring these, and other issues, to an interdisciplinary group, focused on the many social dimensions of system use today and guiding users in making choices and taking actions appropriate to their desired level of privacy.

References

1. Masooda Bashir, Carol Hayes, April D. Lambert, and Jay P. Kesan. 2015. Online privacy and informed consent: The dilemma of information asymmetry. *Proceedings of the Association for Information Science and Technology* 52, 1: 1–10.
2. Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. 2013. Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science* 4, 3: 340-347. http://spp.sagepub.com/content/early/2012/08/08/1948550612455931
3. Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (SOUPS '09). http://dx.doi.org/10.1145/1572532.1572538
4. Monica G. Maceli. 2018. Encouraging patron adoption of privacy-protection technologies: Challenges for public libraries. *International Federation of Library Associations and Institutions* 44, 3: 195–202. https://doi.org/10.1177%2F0340035218773786
5. Mary Madden. 2015. Americans' Attitudes About Privacy, Security and Surveillance. Retrieved August 18, 2018 from http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/
6. Mary Madden. 2015. Americans' Privacy Strategies Post-Snowden. Retrieved September 20, 2018 from http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/
7. Michelle Madejski, Maritza Johnson, and Steven M. Bellovin. 2012. A study of privacy settings errors in an online social network. In *Proceedings of the 4th IEEE International Workshop on Security and Social Networking* (SESOC '12). http://dx.doi.org/10.1109/PerComW.2012.6197507

8. Marina Papastergiou. 2005. Students' mental models of the Internet and their didactical exploitation in informatics education. *Education and Information Technology* 10, 4: 341–360. https://doi.org/10.1007/s10639-005-3431-7

9. Jamie Pinchot and Karen Paullet. 2015. Use of Preventative Measures to Protect Data Privacy on Mobile Devices. *Journal of Information Systems Applied Research* 8, 2: 44-51.

10. Florian Schaub, Aditya Marella, Pranshu Kalvani, Blase Ur, Chao Pan, Emily Forney, and Lorrie F. Cranor. 2016. Watching them watching me: Browser extensions' impact on user privacy awareness and concern. NDSS workshop on usable security (USEC'16), 1-10. http://dx.doi.org/10.14722/usec.2016.23017