Article

International Federation of
Library Associations and Institutions
2018, Vol. 44(3) 195–202
© The Author(s) 2018
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/0340035218773786
journals.sagepub.com/home/ifl
SAGE

Encouraging patron adoption of privacy-protection technologies: Challenges for public libraries

Monica G. Maceli
Pratt Institute, New York, USA

Abstract

Threats to our patrons' privacy have been a long-standing concern in libraries, though our responsibilities were largely bounded by the physical library space. Today, fueled by novel technologies, the landscape is vastly different, with patrons' privacy threatened by an ever-increasing number of entities. In this complexity, libraries have continued their commitment to privacy, with public libraries now seeking to educate patrons about privacy threats, protective measures, and tools that they might employ. This review of literature seeks to identify challenges to United States public libraries in educating and advocating for patron use of privacy-protection technology tools, drawing from research in a variety of allied fields, while suggesting future research directions. Issues identified include: substantial technology-related knowledge gaps in our patrons, librarians, and library staff; the need to support a vast number of technology tools and techniques; as well as building our understanding of the perspective of the tools' underlying creators.

Keywords

Librarian education, literature review, patron training, privacy-protection technologies, privacy threats, public libraries, United States

Submitted: 13 January 2018; Accepted: 26 March 2018.

Introduction

Libraries' commitment to patron privacy has been a core value of the field since its earliest days. Previous generations of librarians and library staff crafted policies and procedures to mask the information trail patrons left behind them within the physical library space, be it from browsing the Web on public access computers or from checking out materials. Today's public libraries have taken on a much greater challenge: that of advising and educating patrons as to how to protect their privacy within the vast online landscape. A common focus of such educational efforts is introducing patrons to privacy-protection technology tools and encouraging their use. These initiatives are becoming increasingly common within public libraries, as will be the focus of this work.

Privacy-protection technology tools consist of a variety of specialized software. These include: web browser plugins that thwart behavioral tracking and data collection, tools to protect the user's data in transit, e.g. virtual private networks (VPNs), or to obfuscate one's location (e.g. the Tor browser), and encrypting various data in storage, such as one's emails or multimedia. Table 1 summarizes some of the most common types of privacy-protection tools as well as their function (for further reading, see Maceli, 2018). Along with the necessary software is the needed knowledge and ability to effectively customize, configure, and wield such tools, as well as the technical literacy needed to avoid social engineering attacks.

In recent years, notable projects originating in public libraries have focused on educating our patrons on privacy-related tools and potential threats. Several large-scale projects in United States public libraries,

Corresponding author:
Monica G. Maceli, Pratt Institute School of Information, 144 West 14th St, 6th Floor, New York, NY, 10011, USA.
Email: mmaceli@pratt.edu

Table 1. Summary of popular privacy-protection technology tools.

Privacy-protection technology tool	Function	Example
Privacy-protecting web browser plug-ins	Thwart behavioral targeting and data collection during the user's web browsing session; block ad-delivery and potentially malicious scripts.	Privacy Badger (www.eff.org/privacybadger)
Incognito or private browsing mode	Protect against later users of the same local computer viewing your stored browsing data.	Private Browsing in Firefox (https://www.mozilla.org/)
Encryption	Protect data from snooping as it travels networks or when stored on computers.	Hypertext Transfer Protocol Secure (HTTPS) for encrypting web content; VeraCrypt (www.veracrypt.fr) utility for encrypting stored data
Virtual private networks (VPNs)	Provides encrypted protection while traversing an open wireless network or from ISPs snooping into one's traffic; change visible origination IP address.	OpenVPN (https://openvpn.net/)
Tor (The Onion Router)	Hide user's identity and obfuscate the destination and origin of traffic by routing their traffic through a series of computers running Tor, known as Tor relays.	Tor Project (https://www.torproject.org/)

currently supported by the Institute of Museum and Library Services (IMLS) and other influential library and information science organizations, seek to train librarians and library staff in this area, with the goal of reaching thousands of practitioners. These include: NYU's partnership with the Library Freedom Foundation (IMLS, 2017) and the City of New York's initiative to train library staff across the city (Marden, 2017), as well as less formal projects such as the growth in the number of libraries offering Tor to their users, sparked by the Kilton Public Library's efforts (Library Freedom Project, 2015). The coming years will reveal the impact of these (and future) projects, with an anticipated sharp increase in the number of librarians and public library staff that can confidently educate, train, and advise their patrons on privacy-protection technology.

Complementing the formal training opportunities in this area for librarians and library staff, numerous pragmatic guides to privacy threats, protective actions and relevant technology tools exist, both in the research literature (e.g. Fortier and Burkell, 2015) and in web-based resources (such as the Library Freedom Project's (2018) "Privacy toolkit for librarians"). The American Library Association (ALA) provides a wealth of privacy-related guidelines, checklists, and toolkits for library staff and librarians (ALA, 2014, 2016). However, such resources focus on mitigating privacy threats while fulfilling the need for "libraries to collect user data and provide personalized services" (ALA, 2016) within the context of the libraries' physical space and resource offerings, and less about guiding patrons in protecting their privacy in the context of their broader lives.

Public libraries are not the only organizations taking on the challenge of privacy-protection tool education, many human rights non-profits are active in this area as well. The highly influential Electronic Frontier Foundation (EFF) is a United States-based non-profit organization that tackles the numerous legal issues arising from the need to protect civil liberties in the digital era. The EFF maintains an extensive body of privacy-related literature and resources on their website and conducts activities ranging from litigating court cases, to developing novel software, such as privacy-protecting web browser plugins (Electronic Frontier Foundation, 2018). In fact, the aforementioned Library Freedom Project's "Privacy toolkit for librarians" includes several pointers to EFF resources. Many other non-profits educate user groups on privacy topics, including: Freedom of the Press Foundation which trains journalists and at-risk groups on digital privacy-protection, internationally, the Tactical Technology Collective and Front Line Defenders work to protect human rights advocates protect their privacy when using digital communication tools.

Public libraries have an advantage over the human rights groups working in this area, given that public libraries have an existing physical presence in many communities across the United States. Privacy-related work within public libraries therefore stands to complement the efforts of other human rights organizations. Privacy and technology have been historically well studied within the field of library and information science; a great deal of previous work has explored our roles and responsibilities in providing technology services to our patrons in a privacy-sensitive fashion, be it public Internet access (such as Nijboer, 2004) or digital library resources (e.g. Sturges et al., 2003). However, though significant effort has been focused on librarian education around privacy-protection technology tools (e.g. Fortier and Burkell, 2015; Noh, 2014), relatively little work in the information science field has looked directly at the barriers and issues surrounding users' adoption and use of such tools. These challenges have the potential to lessen the impact of librarians' work in educating and encouraging patrons in using privacy-related technologies. Libraries have historically emphasized protecting their users' privacy at all costs, but this focus has been largely bounded by the physical library space, with less attention to broader protections as users browse the Web, use mobile devices or other common technology tools, across all aspects of their lives.

This research literature review seeks to explore the work of allied fields studying and designing privacy protection tools, such as computer science and security researchers, with the goal of identifying the potential challenges to patron adoption that our librarians and library staff may face in the future. To that end, this work explores the following questions through a review of existing literature:

- What challenges to the use and adoption of privacy-protection technology tools by public library patrons in the United States are suggested by research literature?
- What potential implications do these challenges have for public libraries' educational initiatives in this area?

The next section will provide a review of related research literature, which will then be contrasted against the stated research questions in the subsequent Discussion section.

Review of related research work

Research assessing the use, understanding, and impact of privacy-protection technology tools on end users has attracted attention from researchers in a variety of security and computing-related fields. To identify and collect such work for the purpose of this literature review, the author and a graduate assistant independently searched both library-specific publications with a technology focus (such as Library Hi Tech, Information Technology & Libraries, and Association for Information Science and Technology (ASIS&T) Annual Meeting Proceedings) and broader general-purpose computing digital libraries (such as the ACM Digital Library). A total of 52 papers were then assessed to identify the purpose and findings of the work, and to determine its relevance in the context of libraries. Though, as stated earlier, the main focus of this literature review was work within the United States, several international publications were included that had particular relevance.

Many studies revealed surprising or paradoxical findings that were very sensitive to contextual factors. Notable work exploring the public's baseline privacy concerns, the impact of their technical knowledge on their actions, and their general use of privacy-protection technology tools will be summarized next.

Baseline privacy concerns

Advising and training our patrons in the use of privacy-protection technology tools is a goal much easier to achieve if patrons have pre-existing concerns about their privacy in the digital world. Though one might assume widespread privacy concern in communities, given the many recent and dramatic privacy-related news stories (e.g. the Equifax hack, NSA spying), the reality of where and when those concerns are felt and acted upon is much more nuanced.

Many researchers have studied users' privacy concerns and their perceptions of control in this area. Efforts to understand the public's privacy concerns and categorize these accordingly have taken place for decades. Starting in the 1970s, Westin conducted a number of surveys (for example – privacy concerns on the growing "Net" (Freebies and Privacy: What Net Users Think, 1999), consumer privacy issues (Consumer Privacy and Survey Research, 2003) and many others) aiming at assessing and tracking privacy worries over time through construction of privacy indexes. Kumaraguru and Cranor (2005) provide a concise survey of Westin's corpus of findings, which notably include grouping of consumers into the categories of: privacy *fundamentalists* (who are greatly protective of their privacy), *pragmatics* (who weight the personal benefits of revealing their information), and the *unconcerned* (who are generally trusting of data-collecting organizations).

Over the many decades and many studies Westin conducted, the pragmatics consistently formed the largest percentage of those studied, ranging from 55% to 63% of respondents. Bergmann (2009), in a large-scale international survey to assess users' privacy awareness based on exposure to a website's privacy policy, found privacy fundamentalists represented 34% of participants, pragmatists were 48%, and unconcerned users 18%. Though users may be easily categorized in interacting with a particular system or scenario, as in the Bergmann study, other research suggests that users' privacy concerns are highly context dependent and variable, with users fluctuating from extreme concern to apathy about privacy depending on contextual and environmental cues (Acquisti et al., 2015). On a more general level, the 2015 Pew Internet survey (Madden and Rainie, 2015) found that 93% of American adults feel it is important to control who can acquire information about them, and 90% of adults find controlling what information is collected about them to be important, so these are clearly widespread values.

Privacy-protection actions

Though the previous work indicates that the majority of the public is at least somewhat (or intermittently) concerned with their privacy, much smaller portions of the population are taking significant measures to protect their privacy in digital environments. Bashir et al. (2015) aptly term this the "privacy paradox", noting the incongruity between people's stated desire for privacy and their actions (or rather – their inactions). In 2015, American survey respondents reported a range of reasons they did not take privacy-protection actions including: the perceived difficulty it would entail, feeling they have nothing to hide, lacking the time and/or technical expertise, the fear of attracting greater scrutiny, and valuing the perceived safety afforded by surveillance (Rainie and Madden, 2015).

Research work emphasizes that those who do take privacy-protecting actions are in the minority, and their actions may be relatively ineffective (e.g. Aldhafferi et al., 2013; Daniel et al., 2014; Madden and Rainie, 2015; Wills and Zeljkovi, 2011). Wills and Zeljkovic (2011) found that simple website privacy measures, such as removing browser history, are done by less than 20% of users. Of users that take action to protect their privacy, the previously mentioned survey of American adults found that 59% cleared cookies, 34% disabled cookies, 15% reported using a search engine that does not track users' search history, 9% of participants added a privacy-enhancing browser plugin, and 9% used anonymizing technologies, e.g. Tor, VPN, proxy server (Madden and Rainie, 2015). One of the simplest means of controlling privacy on an application-by-application basis is changing the default privacy settings; a substantial body of privacy research in the context of social media sites estimates that very few users do so (e.g. Aldhafferi et al., 2013; Daniel et al., 2014), even in response to life changes such as entering the job market (Hargittai and Litt, 2013).

Furthermore, significant struggles were noted in those users that do attempt to take action to protection their privacy. Users that do modify their privacy settings often end up with incorrect settings that do not match their original sharing intentions (Madejski et al., 2012) or are confused by the interfaces and jargon presented (Leon et al., 2012). A 2016 study exploring digital literacy among African American young adult Internet users, found that a large percentage struggled with privacy and safety-related tasks and less than half could complete simple privacy-protection actions, such as adjusting the web browser's security settings or clearing cookies (Park and Jang, 2016). Trepte et al. (2015) suggest that a lack of "privacy literacy" prevents users from effectively taking action to assuage their privacy-related concerns.

Privacy-protecting technology tools

The use of privacy-protecting technology tools themselves also raises many troubling issues and questions. For participants that were studied while using privacy-protection tools, the impact of such technologies was often paradoxical. In exploring a variety of privacy-related browser plugins, Schaub et al. (2016) found that the use of such tools in fact *increased* users' privacy concerns, instead of allaying their fears. A notable emergent concern of participants was sharing information with the privacy tool itself, as their data was visibly processed and intercepted by such technologies.

Though privacy fears were increased, there was little impact noted on users' underlying understanding of what data might be collected and why. Privacy tools increase awareness of privacy-threatening techniques, such as third-party tracking; however, when using personalized logged-in sites, the users' privacy worries often increased and their trust in privacy tools decreased (Schaub, 2016). Additionally, findings indicate that simply becoming aware of a potential privacy issue does not increase the user's underlying comprehension of how such violations may occur (Bergmann, 2009; Schaub, 2016).

As noted earlier, contextual cues play a large role in the users' trust of the technology tool and the perceived information gathered. The users' expectations and the purpose of why sensitive resources are used have a major impact on users' subjective feelings and their trust decisions (Lin, 2012). Tools that offered greater perceived control over the data collected or revealed to others were observed to make users more likely to disclose riskier sensitive information (Brandimarte et al., 2012). And the more confident users felt in their ability to manage their privacy with a particular tool or setting, then the less they would consider revealing personal information to be a privacy risk at all (Chen and Chen, 2015).

Technical knowledge and privacy choices

Many researchers have questioned the role of users' technical knowledge in the privacy choices and actions that they take, with the assumption that technological novices may behave quite differently than those with more expertise. Users' technical knowledge has been assessed through a variety of research means, including eliciting mental models of technical concepts, such as asking users to explain or sketch how the Internet (Kang et al., 2015) or home computer security works (Wash, 2010), and surveying users on their use and experience with technology tools and techniques (e.g. Kang et al., 2015). Here too, results are surprising and the "privacy paradox" (Bashir et al., 2015) is similarly evident.

Malandrino et al. (2013) found that users with greater levels of technology knowledge had a better understanding of privacy-related threats; however, all users generally expressed a concern for privacy but less effort to take any protective actions. Kang et al. (2015) found no clear relationship between users' technical background and knowledge, and their privacy-protection actions. Less technology-savvy users reported greater concerns about their privacy but were generally unwilling to modify settings, change their behaviors, or install privacy-protection technologies, particularly if there was a perceived personal benefit to revealing their information (Malandrino, 2013).

Discussion

Overall, the body of research in this area suggests a significant percentage of the public (which encompasses the public library patron base) are concerned with their privacy, but lack the motivation, knowledge, and digital literacy necessary to consistently and effectively act on these concerns. Privacy-protection technology tools are by no means a panacea, with prior research suggesting they may increase privacy concerns or be used ineffectively. And concern alone would appear to have little impact on users' underlying understanding of what data might be collected, why, and through what technical means (e.g. Bergmann, 2009; Schaub, 2016). The current trend in public libraries, towards providing privacy-related guidance for their patrons and communities, means that library staff and librarians will be directly impacted by the findings of the research reviewed here. The review of literature yields several issues of relevance to the first research question – What challenges to the use and adoption of privacy-protection technology tools by public library patrons in the United States are suggested by research literature? These challenges will be explored next, and presented in the context of the second research question –What potential implications do these challenges have for public libraries' educational initiatives in this area?

Bridging the (many) knowledge gaps

The findings highlighted above clearly illustrate numerous knowledge gaps preventing patrons (and likely library staff and librarians themselves) from effectively adopting, understanding, using, and explaining privacy-protection technologies. Bashir et al. (2015) describe several key knowledge gaps in users' understanding of Internet infrastructure and function, emphasizing a deep problem of information asymmetry (in this case between Internet service providers and their customers) making it difficult for the users to truly comprehend and give consent for their information's collection and use.

These knowledge gaps create serious problems woven throughout all aspects of protecting one's privacy in a digital world, from the initial step of giving consent, to deciding to use, and attempting to customize, privacy-protection tools. The lack of privacy literacy identified by Trepte et al. (2015) is a challenging issue and one that libraries are uniquely positioned to tackle. Wissinger (2017: 380) emphasizes the distinction between *privacy literacy* and *digital literacy*, with privacy literacy focused on the "understanding of the responsibilities and risks associated with sharing information online", while digital literacy focuses on "the task-based use of information in a digital environment." Framed in this way, privacy literacy becomes a deeply personal and challenging critical thinking activity (Wissinger, 2017: 380). Rotman (2009) presents a privacy literacy framework consisting of: *understanding* how personal information is used online, *recognizing* where information may be shared, *realizing* the consequences of sharing, *evaluating* the benefits or drawbacks to sharing online, and *deciding* when it is appropriate to share information. This framework illustrates the many dimensions that must be considered in managing one's information sharing in online environments.

The knowledge gaps preventing users from fully understanding the digital world's impact on their privacy and information are quite daunting, in particular the technological aspects facilitating the underlying ability of information to be shared, as it traverses networks, storage locations, and data collectors.

Nearly every day brings a novel privacy-threatening exploit to the news, requiring constant vigilance and shifting of protective techniques and tools over time. Though it may be relatively simple to advocate for and train users in the use of, say, a particular tracking-blocking browser extension, this clearly does not endow users with a deeper understanding of the function of such tools and the flexibility to apply this knowledge in future novel scenarios. A one-time workshop or infrequent training series is likely not enough to both instill deeper knowledge and encourage the addition of privacy-protection technology tools into one's daily life, particularly given the many reasons users cite for their privacy inactions.

Supporting the vast range of tools and techniques

The literature shows the extensive set of techniques, tools, and actions needed to fully protect one's privacy in today's digital environments. Actions such as reading a privacy policy or running the Tor browser require very different levels of technical knowledge and skill yet may be equally important in protecting one's privacy. The necessarily complementary nature of tools and techniques creates many barriers to use, namely in requiring the users' time and effort to customize the tools to fit their individual needs, as well as the related time and effort on the libraries' side in educating users in these areas. An individual instruction session, which might involve assisting the user in customizing their sharing settings on each social media site, and perhaps installing a series of privacy-related software tools, could be very time-intensive and not scale well to serving larger communities.

The implication for library educators, as is the focus of the several large funded projects mentioned earlier, are that deep technical knowledge, flexibility, and confidence are required to navigate the numerous tools and systems, which we ourselves may or may not be users of. Reference sessions may require the ability to elicit a patron's particular concerns (for example – ads that track them from webpage-to-webpage), suggest a tailored set of privacy-protection tools, as well as bring additional privacy concerns to the user's attention, which they may not have been aware of.

Researching our recommendations

Many of the privacy technology guidelines and toolkits provided by library-related organizations focus on the *how to*, with relatively little explanation of the mission and goals of the software tools' creators or maintainers. The research detailed above demonstrates that privacy tools may in fact increase users' privacy concerns, without giving them insight into the underlying functionality or purpose of the tools. In educating their patrons, libraries must take care to (as much as possible) convey why specific tools should or should not be trusted; this assessment of authenticity and trustworthiness falls under the larger need for digital literacy.

Given the low barrier to software creation and distribution on the Web and mobile app environments, users may mistakenly employ technology tools that have malicious intent. In recent years, this was seen on a wide scale when highly-publicized current events about government surveillance and corporate data breaches drove many people to employ virtual privacy networks (VPNs) for the first time. However, subsequent reviews of the myriad of VPN mobile app options available to users found that many offered little robust protection, threatened the users' privacy by collecting their data, or even contained malware (Ikram et al., 2016). So simply advocating for the use of a general technology, such as VPNs or ad-blocking plugins, may lead users to make personally damaging technology choices, all the while thinking they are taking action to protect themselves. As mentioned earlier, the pace of technological change makes this a particularly difficult issue to keep pace with as new tools enter the market on a near-daily basis.

Future educational and research efforts

It is striking that little of the research presented above, exploring the use of privacy-protection technology tools, assessed library patrons or librarians directly, though the general themes can be extrapolated to this group. Prior research on the technology skills employed by librarians in practice indicates a lack of engagement with deeply technical tasks (e.g. Maceli and Burke, 2016) and it is reasonable to assume that a similar problem of information asymmetry and the privacy paradox of inaction exists for librarians and library staff, mirroring the general population findings. These findings are therefore of interest both in our own educational practices, as well as in educating our patrons and communities, and numerous questions for future research efforts emerge. On the educational front, the Masters of Library Science (MLS) and allied degrees likely need deeper coverage of the underlying technical infrastructure and data flow of the Internet, related directly to privacy threats and vulnerabilities. For practicing librarians and library staff, this knowledge may need to be disseminated through continuing education or professional development opportunities; as the funded privacy-related projects mentioned earlier come to fruition, these opportunities will likely increase.

Relatively little is known of librarians' existing use of privacy-protection technology tools, and this area could benefit from further study. Current work of the author's is exploring librarians' current personal use of privacy-protection tools and how that relates to their technical knowledge and experiences, to close this gap. On the patron side, as the large-scale funded projects mentioned earlier continue to progress, there will be a need to assess the success of patron education efforts and their rate of privacy-protection tool adoption.

Conclusion

There is a clear need for library and information science practitioners, researchers, and organizations to take a larger role in building the corpus of research knowledge about the public's privacy concerns, actions or inactions, and use of privacy-protection tools. The review of literature presented in this article poses several challenges to existing projects training librarians to educate patrons in privacy threats, as well as protective tools and techniques. These challenges include: significant technical knowledge gaps in our patrons (and librarians and library staff as well), the need to support a staggering number of technology tools and techniques, as well as taking care to understand the underlying mission and goals of the suggested tools' creators. Further work is needed to integrate privacy-protection technology topics more deeply into the Masters of Library Science (MLS) and its allied degrees, study librarians' and library staff's current use and understanding of privacy-protection tools, and evaluate the effect of ongoing patron education efforts in this area.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

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

Aldhafferi N, Watson C and Sajeev AS (2013) Personal information privacy settings of online social networks and their suitability for mobile Internet devices. *International Journal of Security* 2(2).

American Library Association (2014) Privacy Tool Kit. Available at: http://www.ala.org/advocacy/privacy/guidelines (accessed 10 December 2017).

American Library Association (2016) Library Privacy Guidelines. Available at: http://www.ala.org/advocacy/privacy/toolkit (accessed 2 March 2018).

Bashir M, Hayes C, Lambert AD, et al. (2015) Online privacy and informed consent: The dilemma of information asymmetry. *Proceedings of the Association for Information Science and Technology* 52(1): 1–10.

Bergman M (2009) Testing privacy awareness. In: Matyáš V, Fischer-Hübner S, Cvrček D, et al. (eds.) *The Future of Identity in the Information Society*. Vol. 298. Berlin,H eidelberg: Springer, pp. 237–253.

Brandimarte L, Acquisti A and Loewenstein G (2012) Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science* (4)3: 340–347.

Chen HT and Chen W (2015) Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior, and Social Networking* 18(1): 13–19.

Daniel WK, Xu X, Bai M, et al. (2014) Privacy issues in online social networks: User behaviors and third-party applications. In: *PACIS 2014 Proceedings* 42. Available at: http://aisel.aisnet.org/pacis2014/42/ (accessed 24 April 2018).

Electronic Frontier Foundation (2018) About EFF. Available at: https://www.eff.org/about (accessed 19 March 2018).

Fortier A and Burkell J (2015) Hidden online surveillance: What librarians should know to protect their own privacy and that of their patrons. *Information Technology & Libraries* 34(3): 59–72.

Hargittai E and Litt E (2013) New strategies for employment? Internet skills and online privacy practices during people's job search. *IEEE Security & Privacy* 11(3): 38–45.

Ikram M, Vallina-Rodriguez N, Seneviratne S, et al. (2016) An analysis of the privacy and security risks of android VPN permission-enabled apps. In: *Proceedings of the 2016 ACM internet measurement conference*, Santa Monica, CA, USA, 14–16 November 2016, pp. 349–364. New York: ACM.

Institute of Museum and Library Services (2017) New York University & Library Freedom Project: Privacy in Libraries. Available at: https://www.imls.gov/grants/awarded/re-95-17-0076-17 (accessed 14 December 2017).

Kang R, Dabbish L, Fruchter N, et al. (2015) 'My data just goes everywhere': User mental models of the Internet and implications for privacy and security. In: *Symposium on Usable Privacy and Security (SOUPS)*, Ottawa, Canada, 22–24 July 2015. Available at: https://www.usenix.org/system/files/conference/soups2015/soups15-paper-kang.pdf (accessed 24 April 2018).

Kumaraguru P and Cranor LF (2005) *Privacy Indexes: A Survey of Westin's Studies*. Pittsburgh, PA: Institute for Software Research International, School of Computer Science, Carnegie Mellon University.

Leon P, Ur B, Shay R, et al. (2012) Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising. In: *Proceedings of the SIGCHI conference on human factors in computing systems*, Austin, TX, USA, 5–10 May 2012, pp. 589–598. New York: ACM.

Library Freedom Project (2015) Tor exit relays in libraries: A new LFP project. Available at: https://libraryfreedomproject.org/torexitpilotphase1/ (accessed 10 December 2017).

Library Freedom Project (2018) Privacy toolkit for librarians. Available at: https://libraryfreedomproject.org/ (accessed 12 January 2018).

Lin J, Sadeh N, Amini S, et al. (2012) Expectation and purpose: Understanding users' mental models of mobile App privacy through crowdsourcing. In: *14th ACM Ubicomp*, Pittsburg, PA, USA, 5–8 September 2012, pp. 501–510. New York: ACM.

Maceli M (2018, forthcoming) Privacy-protection technology tools: Libraries and librarians as users, participants, and advocates. In: Varnum KJ *The Top Technologies Every Librarian Needs to Know: A LITA Guide*. Chicago, IL: ALA TechSource.

Maceli M and Burke J (2016) Technology skills in the workplace: Information professionals' current use and future aspirations. *Information Technology and Libraries* 35(4): 35–62.

Madden M and Rainie L (2015) Americans' attitudes about privacy, security and surveillance. Available at: http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ (accessed 2 December 2017).

Madejski M, Johnson M and Bellovin SM (2012) A study of privacy settings errors in an online social network. In: *Pervasive computing and communications workshops (PERCOM Workshops)*, Lugano, Switzerland, 19–23 March 2012, pp. 340–345. IEEE.

Malandrino D, Scarano V and Spinelli R (2013) How increased awareness can impact attitudes and behaviors toward online privacy protection. In: *Proceedings of the 2013 international conference on social computing (SOCIALCOM'13)*, Washington, DC, USA, pp. 57–62. IEEE.

Marden W (2017) Brooklyn, Queens, and New York Public Libraries launch a new digital privacy initiative. Available at: http://www.oif.ala.org/oif/?p=11782 (accessed 10 January 2018).

Nijboer J (2004) Big Brother versus anonymity on the Internet: Implications for Internet service providers, libraries and individuals since 9/11. *New Library World* 105(7): 256–261.

Noh Y (2014) Digital library user privacy: Changing librarian viewpoints through education. *Library Hi Tech* 32(2): 300–317.

Park YJ and Jang SM (2016) African American Internet use for information search and privacy protection tasks. *Social Science Computer Review* 34(5): 618–630.

Rainie L and Madden M (2015) Americans' privacy strategies post-Snowden. Available at: http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/ (accessed 3 December 2017).

Rotman D (2009) Are you looking at me? Social media and privacy literacy. Poster presentation. In: *iConference*, Chapel Hill, NC, USA, 8–11 February 2009.

Schaub F, Marella A, Kalvani P, et al. (2016) Watching them watching me: Browser extensions' impact on user privacy awareness and concern. In: *USEC'16: NDSS workshop on usable security*, San Diego, CA, USA. DOI: 10.14722/usec.2016.23017.

Sturges P, Davies J, Dearnley J, et al. (2003) User privacy in the digital library environment: An investigation of policies and preparedness. *Library Management* 24(1/2): 44–50.

Trepte S, Teutsch D, Masur PK, et al. (2015) Do people know about privacy and data protection strategies? Towards the 'Online Privacy Literacy Scale' (OPLIS). In: De Hert P and Gutwirth S (eds) *Reforming European Data Protection Law*. Netherlands: Springer, pp. 333–365.

Wash R (2010) Folk models of home computer security. In: *Sixth symposium on usable privacy and security* (SOUPS), Redmond, WA, USA, 14–16 July 2010, pp. 1–16. New York: ACM.

Wills CE and Zeljkovic M (2011) A personalized approach to web privacy: Awareness, attitudes and actions. *Information Management & Computer Security* (19)1: 53–73.

Wissinger CL (2017) Privacy literacy: From theory to practice. *Communications in Information Literacy* 11(2): 378–389.

Author biography

Monica Maceli is Assistant Professor at Pratt Institute School of Information, focusing on emerging technologies in the information and library science domain. She earned her PhD and MSIS from the College of Information Science and Technology (iSchool) at Drexel University. She has an industry background in web development and user experience, having held positions in e-commerce, online learning, and academic libraries. Her research areas of interest include end-user development, human-computer interaction, and information technology education.