Library privacy

Historically, surveillance and interference with the generation of ideas as a practical matter, has been both labour-intensive and expensive to implement (Schneier 2015) as "[t]he state, market, and our social contacts could not monitor our thoughts, our reading habits, and our private conversations, at least not in an efficient, comprehensive, and unobtrusive way" (Richards, 2015).

After the Snowden leaks of 2013, however, citizens across the world have seen the extent of corporate and state digital surveillance (Clark, 2016**;** King and Lock, 2016). The extent of the concern this has caused is evidenced in a recent survey undertaken by Mozilla (2017). Amongst other things, the survey shows that 92% of respondents have a desire to learn more about how to protect themselves online (Mozilla, 2017).

This desire to protect one's privacy online should come as nothing of a surprise; as the use of interconnected digital tools has become embedded in our social practices, the data and information that we transmit both knowingly and unknowingly has become highly prized by various parties. Through weaknesses in the technologies, the way they are deployed, and the way they are used, these technologies have been exploited to routinely capture our private data and information.

Some technology companies have responded by offering users enhanced security options on their digital products and services. However, many providors have failed to make sufficient protections available, and so further data breaches that have affected both individuals and organisations (Quick et al., 2017). Governments have also accelerated their states' programmes of broad, dragnet surveillance. Such aggressive moves limits citizens' human right to privacy by coercing and forcing technology companies to comply with their preference for software designed with weaknesses that can be exploited.

Just last year, the UK Government implemented the Investigatory Powers Act 2016, which has replaced the Regulation of Investigatory Powers Act 2000. This legislation has been widely criticised for an apparent lack of understanding of some technologies, the over-regulation of technology, the lack of proper independent oversight, and the not insignificant issue that the Government themselves are unable the estimate the scale and cost involved in operating the act. (Nuridzhanian, 2016; Bradley, 2016; King and Lock, 2016).

However, it is still possible for users to try to protect their privacy. Users now have the knowledge of the surveillance machinery, and more have started investing labour in creating better and alternative technologies and cultures of use that are oriented at protecting privacy and designing security in rather than out. Balancing some of the operational and technological solutions is crucial, and library workers, who are considered only second to doctors as fiduciaries of citizen's information, are in a strong position to help their communities to address this need to protect themselves (A Society of Chief Librarians/Arts Council survey, cited in Pedley, 2015).

Collecting, storing, and managing information and its accessibility is a core element of what libraries do. But ensuring the personal data and information that we manage on behalf our users is protected, and that our networks, systems, and devices are secure is merely a baseline for library workers. We need to educate our communities about the risks they are exposed to in the digital environment.

As a professional community, library workers share advanced digital skill sets, and our ethical parameters of information management position us as candidates to organise, educate, and advocate for the use of security enhanced behaviours, practices, skills, and technologies to help protect our users' privacy. After all, citizens "need intellectual privacy to make up [their] minds, but [...] often need the assistance and recommendations of others as part of this process, be they librarians search engines, or other intermediaries. The norms of librarians suggest one successful and proven solution to this paradox" (Richards, 2015).

Essential components of a library's critical and digital information literacy programme should include: offering training on threat modelling; password creation and storage; web browsers and plug-ins; search engines; operating systems; communications and encryption tools; and corporate surveillance technologies. All of these are elements of what is sometimes conceived as "digital citizenship", again, making it very clear that this whole area is well within the remit, scope, and capacity of our library services. Internationally, library workers integrate these areas into their professional practice (Pedley, 2015), and in the UK, there has been increased support in these areas, both inside and outside of the workplace (RLC, 2015; Charillon, 2016).

In our politically incoherent and volatile world, with marginalised communities suffering disproportionate risks, libraries can help to reinstate safety into digital spaces. As Ganghadharan (2012) noted, "[u]ntil policy–makers begin a frank discussion of how to account for benefits and harms of experiencing online worlds and to confront the need to protect collective and individual privacy online, oppressive practices will continue". With the Investigatory Powers Act 2016 and the emerging Digital Economy Bill 2016-2017 on the horizon, now is the time for libraries to offer the support our patrons need, even if they may not yet realise the extent to which they need it.


Bradley, P. (2016). *UK Government Spying law moves forward.* Available: http://philbradley.typepad.com/phil_bradleys_weblog/2016/03/uk-government-spying-law-moves-forward.html?utm_source=twitterfeed&utm_medium=twitter. Last accessed 15 March 2017

Charillon, A. (2016). CryptoParty Newcastle and user privacy in libraries. The Informed: http://theinformed.org.uk/2016/06/cryptoparty/. Last accessed 13 March 2017

Clark, I., 2016. The digital divide in the post-Snowden era. Journal of Radical Librarianship 2.

Gangadharan, S. P. (2012). Digital inclusion and data profiling. First Monday, 17(5).

King, E. and Lock, D. (2016). *Investigatory Powers Bill: Key Changes Made by the Lords.* Available: https://ukconstitutionallaw.org/2016/12/01/eric-king-and-daniella-lock-investigatory-powers-bill-key-changes-made-by-the-lords/. Last accessed 16 March 2017.

Mozilla. (2017). Hackers, Trackers and Snoops: Our Privacy Survey Results. Available: https://medium.com/@mozilla/hackers-trackers-and-snoops-our-privacy-survey-results-1bfa0a728bd5#.j844ubv38. Last accessed 13 March 2017.

Nuridzhanian, G. (2016). *The Investigatory Powers Act: The Official Entrenchment of Far-Reaching Surveillance Powers.* Available: https://blogs.ucl.ac.uk/law-journal/2016/12/08/the-investigatory-powers-act-the-official-entrenchment-of-far-reaching-surveillance-powers/. Last accessed 16 March 2017.

Pedley, P. (2015). What are librarians doing to protect the privacy of their users? CILIP UPDATE, April 2015: 42–43.

Quick, M. et al. (2017). *World's Biggest Data Breaches: Selected losses greater than 30,000 records.* Available: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/. Last accessed 15 March 2017.

Richards, N. (2015). Intellectual privacy: Rethinking civil liberties in the digital age. Oxford University Press, USA.

RLC. (2015). Radical Librarians Collective CryptoParty. Library Freedom Project. Available: https://libraryfreedomproject.org/rlccryptoparty/ Lat accessed 15 March 2017

Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: Norton.