Growing bulbs of intellectual freedom from academic libraries

As many of us are increasingly aware, data pertaining to our online behaviour- when and where we have been, what we did whilst occupying that space, etc.- have become increasingly valuable to a range of stakeholders and bad actors, including unethical hackers, commercial organisations, and the state. The weaknesses inherent across various web infrastructures, their deployment, and their ubiquitous, multipurpose uses are routinely exploited to capture the private data and information of individuals and entire communities.

For many librarians, this technological and cultural problem has been increasingly acknowledged as part of a wider political concern that is directly relevant to our professional requirement to protect the right to intellectual privacy (Fister, 2015; Smith, 2018).

Through both my professional and voluntary labour with the Library Freedom Project and the Radical Librarians Collective, I have been trying to directly offer support for individuals in their attempt to protect their privacy through their behaviours and the digital tools they choose to make use of. However, consistently weaving intellectual privacy throughout my professional praxis is a significant challenge.

Peeling back the layers of libraries and the scholarly commons

I am currently employed as the Research Support Manager for Library Services at the University of West London (UWL). A significant aspect of my role is to manage and administrate the UWL Repository, which is the institution's repository of research outputs. The repository makes these outputs discoverable and accessible through what is known as green open access.

The collection, storage, management, and sharing of information demonstrated in the administration of a repository are all core elements of library work. However, this specific aspect of library work directly contributes towards the development and maintenance of the scholarly commons as an accessible body of work that "admit[s] the curious, rather than [only] the orthodox, to the alchemist's vault" (Illich, 1973), and to allow people to re-use the research for their own purposes.

In all areas of library work, ensuring that the personal data and information of our user communities is stored securely is very important for the preservation of intellectual privacy. However, in the contemporary environment, libraries' digital connections to external sources and services can make this challenging. Libraries are reliant on services that are served externally, and as such libraries lack the ability to control how these services share data required for the use of these services.

As the University have control over the repository through an agreement with a hosting service, it has been easy enough to enable some security enhancements. As such, from January 2018, the UWL Repository has been wrapped in HTTPS to respect our user communities' information security by ensuring that all connections to it are encrypted.

Unfortunately, the scholarly commons is only as accessible as it is permitted to be on the clear-net, as there are many powerful stakeholders that have the ability to suppress access and thus censor scholars and other publics from accessing the published results of academic research and scholarship.

Onions don’t grow on trees; environmental ethics and the scholarly commons

Some popular online services and networks for scholars, such as Sci-Hub, ResearchGate, academia.edu, also offer users the option to share their scholarly and research outputs *gratis*. The latter two are capital venture funded, commercial services. Part of their business operations include providing data around research that can, it is claimed, offer insights into its ‘impact’. However, these services do not take responsibility for the frequent breaches of licences that help to calcify the commodification of scholarly knowledge (Lawson et al., 2015,). Many of these services also have vested interests in the data stored and *created* through the use of their services.

For the scholarly commons, publishing via open access (through both gold open access publishers and via institutional and subject repositories) and making use of appropriate Creative Commons licences is a significantly more effective and ethical way to share and access research and scholarly outputs. Institutional repositories are commonly sustained by institutional funding (i.e. they serve not-for-profit functions), for instance, and they also commonly run on free (libre) and open source software such as EPrints software, which is licensed under GPL v3.0.

Here, we can see that libraries actively support a *libre* approach to free, online access to scholarly information.

Layering up for intellectual privacy, access, and the scholarly commons

As referred to above, various fields of informational labour hold a broad consensus view around users’ right and need for intellectual privacy (Richards, 2015). In this context, ensuring that the research and scholarly outputs are accessible in ways that allow users to retain their privacy seems essential.

As such, I have made the UWL Repository accessible from within the Tor network as an onion service.

I briefly consulted Library Services’ director, Andrew Preater, prior to undertaking this work, but I was able to make use of Enterprise Onion Toolkit (EOTK) to create a proxy of the repository without requiring root access to the webserver of the clear-net site, and without having to make copies of the files held on that server. As a proof-of-concept, it is now accessible via https://6dtdxvvrug3v6g6d.onion, but may be moved to a more permanent .onion address in the future, subject to institutional support. (Please note that an exception has to be granted to access the onion service due to some of the complexities of HTTPS over onion services. This is something that I would hope to resolve with institutional support. Please see Murray’s post for further details).

This provision allows global access to the UWL Repository and its accessible content in a form that allows users to protect their right to intellectual privacy; neither their ISP nor UWL, as a service provider, will be able to identify their personal use of UWL Repository when using https://6dtdxvvrug3v6g6d.onion/.

Having repositories available as onion services is of significant benefit for those accessing the material from, for instance, oppressive geopolitical contexts. Onion services offer not only enhanced privacy for users, but also help to circumvent censorship. Some governments and regimes routinely deny access to clear-net websites deemed *obscene* or *a threat to national security*. Providing an onion service of the repository not only protects those that may suffer enhanced digital surveillance for challenging social constructs or social relations (which can have a severely chilling effect on intellectual freedom), but also on entire geographical areas that are locked out of accessing publicly accessible content on the clear-net.

The expansion of intellectual privacy for the scholarly commons is bringing tears to my eyes

Although this is a small step for the scholarly commons, it is an important one. In our politically fragile world, marginalised communities often suffer disproportionate risks, and taking this simple step helps to reinstate *some* safety into this digital space (Barron et al., 2017). As Ganghadharan (2012) notes, "[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".

I hope that other library and information workers, repository administrators, open access publishers, and their associated indexing services will take inspiration from the step that I have taken and help us to lead a collective charge that places intellectual privacy at the centre of both the scholarly commons and digital library services.

Acknowledgements:

I would like to thank **Murray Royston-Ward** and **Simon Barron** for their technical support (if you do not have access to a server, Murray has written a guide to trialling a Tor mirror of services via Google's Cloud Engine), **Alec Muffett** for his development of EOTK, **Alison Macrina** and the **Library Freedom Project** for their advocacy of digital rights within libraries, the **Radical Librarians Collective** for providing spaces to support my professional development and practical skills, and to all those involved in the **Tor Project** that support and provide tools that allow us to make good on our right to digital privacy.

References:

Barron, S., Regnault, C., and Sanders, K. (2017). Library privacy. Carnegie UK. [Retrieved from: https://www.carnegieuktrust.org.uk/uncategorized/library-privacy/]

Fister, B. (2015). Big Data or Big Brother? Data, ethics, and academic libraries. Library Issues: Briefings for Faculty and Administrators. [Retrieved from: https://barberafister.net/LIbigdata.pdf]

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

Illich, I. (1973). Tools for conviviality. [Retrieved from: http://web.media.mit.edu/~calla/web_comunidad/Reading-En/Illichhapters1_2_3.pdf]

Lawson, S., Sanders, K., and Smith, L. (2015). Commodification of the information profession: A critique of higher education under neoliberalism. Journal of Librarianship and Scholarly Communication, 3 (1). [Retrieved from: http://dx.doi.org/10.7710/2162-3309.1182]

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

Smith, L. (2018). Surveillance, privacy, and the ethics of librarianship. Cambridge Libraries Conference, 11/01,2018. [Retrieved from: https://www.slideshare.net/laurensmith/surveillance-privacy-and-the-ehtics-of-librarianship