Radical Librarians Collective Gathering 2016, Brighton

Simon Barron, Ian Clark, Rebecca Jones, SarahLouise McDonald, and Lauren Smith

ABSTRACT: This is a write up of some of the sessions held at the Radical Librarians Collective Gathering on 9th July 2016 in Brighton, UK.

Keywords: event report, privacy, professional development, surveillance, systems librarianship, web filtering

The Radical Librarians Collective Gathering 2016 was held at the Cowley Club in Brighton, UK on 9th July 2016. Although RLC aims to be non-hierarchical in nature and is not run by a central committee, an organising committee worked together to plan and promote the event and facilitate the unconference format on the day. RLC operates on a donations policy to allow anyone who would like to come access to the event, irrespective of financial ability to pay, while also ensuring it remains free from sponsorship. The Cowley Club kindly offered the use of their space for free, and provided a hot vegan buffet for £5 a head. The collective aims to support and promote equity and diversity, and care was taken to ensure that the venue was suitable to meet a range of needs. The Cowley Club is accessible via public transport and footpath, has disabled access, a disabled toilet in addition to two other toilets, a range of lighting and seating, and good acoustics ([Cowley Club, 2016](#)). Twenty-five people attended the event.

On the day, people involved in the collective supported the co-ordination of the event, inviting attendees to pitch sessions. Care was taken at this point and throughout the day to seek to reiterate the non-hierarchical nature of the collective, and although a committee was responsible for the organising on the day and ensuring the safer spaces policy was maintained, all attendees were welcomed to contribute in any way they felt comfortable. The organising committee also sought to ensure a gender balance in terms of representation, time speaking and facilitating during sessions and throughout the day, and the division of labour (such as making tea, organising and doing administrative work). As well as two rooms for discussions, an area of the venue was used as a relaxed space for zine- and badge-making.

RLC Gatherings typically take an unconference format, which means that there are not scheduled and planned talks in the style of traditional conferences. Instead, attendees are all invited to suggest sessions that could be held ahead of time, through the web page for the event. These may be facilitated by the person making the suggestion, or could be facilitated by someone else if this is felt to be appropriate and possible. The idea of this is that people who would like to take part in or observe discussions but do not feel comfortable or confident in talking in public then have the opportunity to make suggestions about critical topics and that these may still be discussed. For the first time, the gathering also included a scheduled session led by Alison Macrina, founder of the Library Freedom Project about issues of surveillance and privacy.

This paper presents brief summaries of some of the topics discussed by attendees at the event:
- What is RLC?: SarahLouise McDonald
- Critical approaches to systems librarianship: Simon Barron
- Web filtering in libraries: Rebecca Jones
- The Library Freedom Project: Ian Clark
- Continuing Professional Development (CPD): SarahLouise McDonald

What is RLC?

This discussion started the day as a way to summarize the history of the collective for those new to RLC. It began four years ago with seven like-minded people (four of whom were in attendance in 2016) who realised there were no real spaces to tackle difficult discussions about consumerism, our professional body and their response or lack thereof regarding cuts to services. These information workers had a reason for their meeting taking place but no real plan for what the collective would or could do in future. In the intervening years the collective has worked on identifying issues and discussing situations as they arise. It was suggested that there is room for more proactive responses which take a tone of protest instead of maintaining romantic or nostalgic views of our services.

Discussion moved to the topic of the recent Brexit referendum and how the provision of information was dealt with. Attendees suggested ways that this could be better executed, how making resources more freely available could help and whether this could be called direct action. Some useful articles by Lauren Smith (Smith, 2016) and Emma Coonan (Coonan, 2016) were recommended on the topic of information literacy. Other groups interested in the same ideals may have their hands tied to an extent by the party line of CILIP, but RLC should not be afraid to push buttons. Working with other Radical groups could help our cause, for example the Open Rights Group (2016a), the Radical Education Forum (2016), Anarchism Research Group (University of Loughborough, 2016) or the Feminist Library (2017).

Direct action was a topic that came up again and again as we discussed whether attendees at the CILIP conference should organise some kind of demonstration or statement. Many of those present were wary of becoming known as 'CILIP troublemakers' and already felt that an aggressive approach could be an intimidating introduction to Radical Librarianship for potential newcomers to the collective, that it might be better to lead gently to our ethics. No resolution was made.

Another topic mentioned during this session and throughout the day was accessibility. How are we restricting ourselves and others, and how can we help them engage more? It seems there is a balance to be struck for everyone as it is not possible to participate in all areas of a collective but neither is it mandatory.

As a newcomer to RLC and its work the idea that resonated most with me from this session was that librarians simply doing their job properly does not equate to radicalism. We should strive to do better rather than appease others; inactivity becomes a political action by its complicity. I found this discussion really helpful in figuring out why I might want to call myself a Radical Librarian and how I can make that happen. It seems that as a collective we have got a range of personalities and with them viewpoints on where RLC should go from here, but what I am beginning to understand now is that it can be what you make of it.

Maybe RLC can be all the things to all the people if everyone puts in what they are willing to get out of it.

Critical systems librarianship

Specialist library systems are essential to the functioning of a modern library. Software controls book circulation and management of user data. A combination of hardware and software controls access to physical library space. Given the centrality of library systems to operational management of a library service, there is a distinct lack of critical discussion of library systems or systems librarianship.

This #RLC16 session provided an example of critical systems librarianship focusing on one aspect of the uneven power relations between libraries and the suppliers of library systems: the lack of security in many well-used library systems products.

The balance of power in the relationship between libraries which purchase systems and the companies that supply those systems is skewed in favour of the suppliers. In Foucauldian terms (Foucault, 1991), there are unequal power relations between these two parties. 'Power relations' refers to the means by which different groups (and individuals) relate to one another in terms of control or lack of control: if one group can compel or influence a second group to do something against their (the second group's) will or against their (the second group's) own best interests, then the first group can be said to have power over the second group.

Considering the power relations inherent in library systems and applying that to practice is an aspect of critical systems librarianship. Adopting a critical attitude to the use of technology should involve "a willingness to challenge commonsense assumptions and to question the status quo. In other words, to open up the 'black box' of information technology and scrutinize the power relations inscribed within it which may repress or constrain" (Doolin, 1998, p. 307).

The transactional nature of the library–supplier relationship is the most obvious manifestation of these skewed power relations: the exchange of capital inherently gives power to the group receiving the capital. But the financial aspect is only one aspect of the power relations between suppliers and libraries. Systems suppliers use a range of technical, organisational, and psychological means to exert control over their customers. Software suppliers can restrict library access to certain software functions claiming that this is necessary for technical support and ultimately maintaining their control over the software; suppliers can enforce their own standards for systems integrations or the data in the system to keep customers tied to one particular ecosystem; suppliers can use server logs or the software itself to monitor the activities of customers. Perhaps the most problematic element of control is the suppliers' control over library patron data: in the case of cloud-hosted library management systems, suppliers use patron data—which the libraries have a duty of

care to protect—for private data analysis to adjust their services accordingly and, ultimately, to improve their own profits at the expense of the privacy of library users.

One further element of control is the security of library systems. On one hand, libraries are prevented from accessing crucial systems functions in order for suppliers to retain control over software and keep libraries beholden to them for (often expensive) technical support. On the other hand, compared to software and systems in other sectors, library systems are notoriously insecure. Suppliers use the security of their systems as a selling point exploiting the unfortunately common technical ignorance of library systems teams and library managers making purchasing decisions. In reality, the systems that libraries rely on for day-to-day functioning are weak in terms of information security, weak in data encryption, and weak in infrastructure.

In this session, participants looked at specific security weaknesses in well-used library systems covering self-circulation software, access control software, library management systems, and discovery systems. All these systems contain security weaknesses by design as well as exploits and hacks that an adversary can use to manipulate the systems and access what should be protected data. Examining the various security weaknesses of library systems helps us to figure out how to better protect our systems and the data within. There is also an element of digital disobedience (in the spirit of civil disobedience) in being aware of these weaknesses: by disrupting closed library systems, we are able to highlight the issues of security that plague these systems and either force suppliers to take action to fix them or persuade libraries to adopt more secure, open-source technologies (Schneier, 1999) which would allow them more control over systems security.

Examples of poor security in library systems included means of exploiting insecure printed barcode technology, tools and techniques for reading, editing, and deleting data on MiFare chips (used in security cards) and RFID chips (used in print books specifically with the RFID data model standard, ISO 28560 (ISO, 2014)) using the NFC functions commonly found in modern smartphones (Fortune, 2013), use of VPNs and the Tor network to get around IP range restrictions and test off-campus access to e-resources, obfuscation techniques (Brunton & Nissenbaum, 2015) using APIs and loan data to protect user privacy, and library management systems which store passwords in cleartext either in the central database or in server logs. Tangentially, we also discussed the issue of Sci-Hub—the platform for illegally accessing copyrighted scholarly journal articles—and the morality of their practices including flagrant breach of copyright and allegedly undertaking phishing campaigns or harvesting login credentials for e-resources from insecure library systems servers.

Highlighting the (often unquestioned) security deficiencies in library systems raised the question of why library workers not only accept these insecure, inefficient systems but pay extortionate license fees to third-party, private companies for the use of them. With regards

to systems, libraries suffer from diminished expectations as a result of decades of sub-standard software, they fail to hire or develop staff with the technical abilities to make intelligent decisions on systems procurement, and, centrally, they are manipulated and controlled by an increasingly limited number of library systems suppliers.

Being aware of and reflecting on security deficiencies and uneven power relations in library-supplier relationships is useful and has a part to play in overcoming these problems but more important is acting on these reflections to change how libraries and library workers approach the systems they work with every day. We can demand more from our library systems suppliers, we can educate ourselves on technical issues and technology ethics, we can encourage others to question dominant power relations and prevalent systems, and we can envision and create alternative systems using shareable, community-driven, open-source code.

Web filtering in libraries

One of the most interesting discussions of the day was that about web filtering in libraries. Partly this was because it was the result of something practical that RLC have achieved, partly because of the guest from the Open Rights Group but also because it's something where it is easy to see how this issue can impact on vulnerable people. For many people the public library is the only place they can access information and blocking websites hinders this.

SL discussed the work that they and a number of RLC volunteers had done to find out some of the facts behind this issues. All councils in the UK were contacted and asked (using the Freedom of Information Act) a number of questions including 'Do you use content filtering software?', 'Full list of categories blocked', 'Annual cost of filtering software', and 'Do you have a policy document for gaining access to blocked material?' The dataset of responses can be found on figshare (Payne et al., 2016). Some of the results include the details that 98% of public libraries filter categories and 56% block specific websites. These sites include those covering topics such as 'abortion', 'LGBT', and 'sex education.' The group discussed how this could impact on someone for whom library computers are the only way of accessing information or support they might need for sensitive subjects.

RLC's work links nicely with the 'Blocked' project of the Open Rights Group (ORG). This group aims to extend civil liberties into cyberspace. Both projects discussed their concerns about how difficult it is to overturn a decision and get ISPs and public libraries to allow websites to be viewed again. The Internet Watch Foundation have a list of blocked sites but people are not allowed to see what has been included.

On the website Blocked (Open Rights Group, 2016b), you can check a URL to see if it has been blocked by filters of ISPs. They have found that strict filters have blocked 21% (as of 29 July 2016) of the sites that have been checked. This means that under 18s have limited

access to information. ORG are working to make filtering more transparent and accountable.

So what can be done by people who need to use public libraries to access this type of information? The group discussed the fact that Tor browsers can bypass filters or, if this can't be installed, Tails could possibly be used via an external device.

Both projects talked about their plans for future work in this area. ORG would like to collaborate with RLC because they want to investigate filtering across more networks including public wifi. Members of RLC have used FOI to check what filtering is used by academic libraries. The data has been gathered but SL is looking for volunteers to help compile this information into a spreadsheet so that it can be analysed. If you are interested please email rlc@riseup.net.

Library Freedom Project

Established in the aftermath of Edward Snowden's disclosures, the Library Freedom Project has played a key role in highlighting the need to protect the privacy of library patrons. Alison Macrina, Director of the Library Freedom Project, delivered a session covering some of the key issues we face as librarians in terms of internet surveillance and privacy, including pointing to a number of useful resources that library workers can use and advocate for.

In terms of privacy concerns, the Investigatory Powers Bill (also known as the Snooper's Charter) is of key concern to UK based library workers. Currently working its way through the legislative process, the Investigatory Powers Bill provides a serious threat to the communities that libraries serve. There is a particular threat to the institution of the public library given that a key role for the public library in society is to facilitate access to information freely and privately (International Federation of Library Associations, 2014). The Investigatory Powers Bill directly threatens these principles, not least because it requires public libraries (amongst others) to store wifi users' data and forces them to make it available to authorities (Travis, 2016).

Given it is home to the NSA, similar threats to intellectual privacy are evident in the United States. As a result, the Library Freedom Project has been active in educating both users and library workers across the country. One of the Project's key successes has been the successful installation of a Tor relay at Kilton Public Library in Lebanon, New Hampshire, despite the efforts of the Department of Homeland Security to shut it down (Farivar, 2015). Although there have been no equivalent attempts yet in the UK to install a Tor relay in a public library, the efforts in Lebanon reinforce the difficulties faced when trying to ensure user privacy, a reality that will undoubtedly become increasingly apparent as the Investigatory Powers Bill makes its way through parliament.

A range of tools were highlighted for library workers to use and to advocate for amongst their communities. As well as Tor, tools such as Signal (smartphone – Android and iOS),

Ricochet (desktop), and PGP for email were highlighted as key tools that can help ensure a degree of privacy in online activity and communications. VPNs were also recommended, although it is important to ensure that they operate in privacy friendly jurisdictions and have a robust approach to law enforcement requests. However, all such tools come with a number of caveats. For example, smartphone applications tend to leak metadata and are not the most secure method of communicating, even using highly recommended apps such as Signal (the grugq, 2015). Even the more secure option of PGP email requires the user to be aware that the metadata it creates is vulnerable (including subject lines, as well as the more obvious To, CC, and BCC elements). However, although these tools offer general protection from mass surveillance if used effectively, they offer little protection should an individual be subject to targeted surveillance by nation states (the grugq, 2015). In short, whilst they minimise threats to intellectual privacy, they do not *eliminate* them completely.

Although efforts in the UK are somewhat less advanced than in the US, there have been moves to replicate the work of the Library Freedom Project in public libraries. As well as crypto parties being held to help library workers develop their skills and ensure their intellectual privacy (Radical Librarians Collective, 2015), the past year has also seen the first crypto party held in a UK public library. Co-ordinated with the north-east branch of the Open Rights Group, the Newcastle City Library crypto party was a big step forward in terms of public libraries as a mechanism by which to protect communities from invasions of their intellectual privacy (Charillon, 2016). Given the impending investigatory powers bill and the increasing pressure to monitor the resources individual's access (see the Prevent strategy for example), it may be that this was a rare one-off event. However, as Alison has demonstrated through her Library Freedom Project, there is clearly a need that we can and should be fulfilling.

Continuing Professional Development (CPD)

Chartership is the route of professional development that is advocated by our professional body in the UK. It is understood—though not stated outright—that most people could complete this portfolio building task a year or two, but we recognise it may take individuals much longer depending on their privilege and circumstances. The discussion for this session centred on whether this system of career development is inherently ableist and if so how we may go about challenging this accepted norm.

We discussed barriers to inclusion such as a lack of support from workplaces and the resulting strain of extra-curricular publishing, visual or written literacy difficulties, information on who to speak to when asking for help, how personal circumstances may restrict ability to engage and lack of information available on how to deal with these barriers. Ideas such as pre-joining questionnaires regarding additional support, venue information and better organisation of space were mentioned, as were childcare solutions and alternative

types of submission to written communication.

Most of this session was relevant to event organisation so these ideas may be taken forward to create a briefing article that may help organisers in the future. As a person currently in the midst of building my Chartership portfolio for CILIP I found the whole discussion on the expectations of CPD very relevant. Our conversations forced me to examine my own privilege and consider how tasks I consider annoying must be near impossible to others, and I came away with the impression that encouraging inclusion can begin from the simple premise of caring enough to ask more questions and challenge assumptions.

Summary

In summary, the gathering provided the opportunity for attendees to discuss a wide range of issues affecting and influencing the library and information profession. Key questions raised included those around the role of direct action, issues of accessibility, power dynamics between individual library and information workers and professional bodies and library vendors, technical and security issues in library services and the role of library workers in relation to this, and issues of equity in relation to professional development opportunities. As always, more questions were raised than answers devised, but solid action points were taken away from each of the sessions, both for individuals to focus on and for RLC to work to develop collectively.

Following the 2016 RLC national gathering in Brighton, a "Barriers to Engagement" document was created on our RLC Sandstorm site. It was advertised via email, Facebook and Twitter. The aim of the document was to facilitate positive feedback that would help RLC improve its behaviours and practices. A blog post about the development of practices for future gatherings was published in March 2017 (Radical Librarians Collective, 2017a).

The next RLC Gathering will be held at Glasgow Women's Library on 15th July 2017, from 12–4pm. For more information see the event page on the RLC website (Radical Librarians Collective, 2017b).

Acknowledgements

References

Brunton, F. and Nissenbaum, H. (2015). *Obfuscation: a user's guide for privacy and protest*. London: The MIT Press. Retrieved from: https://www.docdroid.net/Rbujq6c/obfuscation-a-users-guide-for-privacy-and-protest.pdf.html [Accessed 14 March 2017]

Charillon, A. (2016). CryptoParty Newcastle and user privacy in libraries. *Informed*. Retrieved from: http://theinformed.org.uk/2016/06/cryptoparty/ [Accessed 14 March 2017]

Coonan, E. (2016). The mongoose librarian. Retrieved from: https://librariangoddess.wordpress.com/ [Accessed 14 March 2017]

Cowley Club (2016). Accessibility. Retrieved from: http://www.cowleyclub.org.uk/%3fAccessibility/ [Accessed 14 March 2017]

Doolin, B. (1998). Information technology as disciplinary technology: being critical in interpretative research on information system. *Journal of Information Technology*, 13(4), 301–311. https://dx.doi:10.1057/jit.1998.8

Farivar, C. (2015). Library's Tor relay—which had been pulled after feds noticed—now restored. *Ars Technica*. Retrieved from: https://arstechnica.com/tech-policy/2015/09/small-town-library-restores-tor-relay-which-had-gone-dark-for-weeks/ [Accessed 14 March 2017]

Feminist Library (2017). The Feminist Library: Archiving our herstories since 1975. http://feministlibrary.co.uk/ [Accessed 14 March 2017]

Fortune, M. (2013). Security, false alarms and excursions into the world of NFC. *Changing Libraries*. Retrieved from: http://www.mickfortune.com/Wordpress/?p=1001 [Accessed 14 March 2017]

Foucault, M. (1991). *Discipline and Punish: The Birth of the Prison*. Translated from French by Alan Sheridan. London: Penguin Books. Retrieved from: https://zulfahmed.files.wordpress.com/2013/12/disciplineandpunish.pdf [Accessed 14 March 2017]

The grugq (2015). Signals, Intelligence. Retrieved from: https://medium.com/@thegrugq/signal-intelligence-free-for-all-5993c2f72f90#.8shqx01wb [Accessed 14 March 2017]

International Federation of Library Associations (2014). *Internet Manifesto 2014*. Retrieved from: https://www.ifla.org/publications/node/224 [Accessed 14 March 2017]

International Organisation for Standardisation (ISO) (2014). ISO 28560-1:2014. https://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=65203 [Accessed 14 March 2017]

Open Rights Group (2016a). Our Work. Retrieved from: https://www.openrightsgroup.org/ourwork/ [Accessed 14 March 2017]

Open Rights Group (2016b). Blocked. https://www.blocked.org.uk/ [Accessed 14 March

2017]

Payne, D., Arkle, S., Gallagher, J., Lawson, S., Richardson, J., Smith, L., Stephan, K. (2016). Content filtering in UK public libraries: dataset. Retrieved from: https://doi.org/10.6084/m9.figshare.2059998.v2 [Accessed 14 March 2017]

Radical Education Forum (2016). Radical Education Forum's Blog. Retrieved from: http://radicaleducationforum.tumblr.com/ [Accessed 14 March 2017]

Radical Librarians Collective (2017a). Follow-Up to Barriers to Engagement. Retrieved from: https://rlc.radicallibrarianship.org/2017/03/08/follow-up-to-barriers-to-engagement/ [Accessed 14 March 2017]

Radical Librarians Collective (2017b). RLC Gathering 2017: Glasgow Women's Library, 15th July. https://rlc.radicallibrarianship.org/gatherings/rlc-gathering-2017-glasgow-womens-library-15th-july/ [Accessed 14 March 2017]

Schneier, B. (1999). Crypto-Gram: September 15, 1999. *Schneier on Security*. https://www.schneier.com/crypto-gram/archives/1999/0915.html [Accessed 14 March 2017]

Smith, L. (2016). Lauren Smith. https://laurensmith.wordpress.com/ [Accessed 14 March 2017]

Travis, A. (2016). Snooper's charter: cafes and libraries face having to store Wi-Fi users' data. *The Guardian*. Retrieved from: https://www.theguardian.com/world/2016/jan/13/snoopers-charter-theresa-may-cafes-wifi-network-store-customers-data [Accessed 14 March 2017]

University of Loughborough (2016). Anarchist Research Group. http://www.lboro.ac.uk/departments/phir/research/arg/ [Accessed 14 March 2017]