Skills for (private) life: a review and multi-site case study of digital privacy initiatives in UK public libraries

Skills for (private) life: A review and multi-site case study of digital privacy initiatives in UK public libraries

Camille Regnault
Department of Information Studies, University College London

Abstract:
Digital inclusion – a proposal to provide equal opportunities access to the benefits of the Internet – is a national initiative supported by 3000 public libraries in the UK. This article focuses on the activities of exemplary public library services in the UK, in order to report on the character of their digital privacy initiatives and in doing so, identify their rationales. The research explores their relevance to existing service strategies, the risks and barriers to implementation, and the potential for wider replication within the UK and produced a number of key findings: responses confirmed that each of the libraries had collaborated with an outside organisation to offer digital privacy initiatives, including 'cryptoparties'; all of the respondents largely agreed that public libraries should engage with digital privacy issues as part of their commitment to library ethics and in order to support users make informed decisions.

Keywords: *Big data, cryptoparties, digital inclusion, encryption, intellectual privacy, mass surveillance, threat model.*

Journal of New Librarianship, *3* (2018) pp. 297-368 10.21173/newlibs/5/8

Introduction

Background information

Since at least the beginning of the 18th century, libraries in Britain have sought to lend agency to their citizenry and expand access to knowledge, as they shifted from closed parochial libraries (where books were often chained to desks) to lending libraries (Feather, 2008; Thomas, 1966).

As traditional services and print resources have been revised and eventually transformed through the power of the Web and digitisation however, so too have the paradigms of social and civic engagement as well as learning.

In 2014 the British Government's Digital Inclusion Strategy made a nationwide effort to invest in resources and digital infrastructure for places like public libraries in the hope that it would mitigate the most pronounced effects of digital exclusion in the UK. In its policy paper, which opened with a foreword by Francis Maud and the title 'This is for everyone', it addressed what it called '4 main kinds of challenge people face' (Cabinet Office, 2014). These were summarised as follows:

- access - the ability to actually go online and connect to the internet
- skills - to be able to use the internet
- motivation - knowing the reasons why using the internet is a good thing
- trust - the risk of crime, or not knowing where to start to go online

To this day many groups and enterprises which galvanised behind the message of the British government's original strategy, continue to offer services and support for underprivileged groups and communities. These range from Google's 'Digital Garage' and Barclay's 'Digital Eagles' to the Society of Chief Librarian's 'Digital Information Skills For Library Workforce', developed under the auspices of the Government's 'Digital by Default and Assisted Digital' services.

As the cost of mobile technologies has declined in recent years – providing cheap storage, inexpensive retrieval, and a global reach - studies conducted into the habits of digital consumers have also shown encouraging signs of an increasingly connected population. Reports published by OfCom for example revealed that 'two thirds of people now own a smartphone, using it for nearly two hours every day to browse the internet, access social media, bank and shop online' (The Communications Market, 2015)

Research context

Ian Clark and Eszter Hargittai both observe that as a natural consequence of this growth, research concerned with the phenomenon of the digital divide in the West has largely shifted away from whether or not an individual has adequate *access* to the Internet (the first challenge identified in the policy paper) and towards how such an individual might use it (Clark, 2016; Hargittai, 2002).

Legal scholar, Tim Wu asserts that almost every computer 'program we use is a type of thinking aid – whether the task is to remember things (an address book), to organise prose (a word processor), or to keep track of friends (social network software)' (Wu, 2012, p. 172).

Neil Richards takes this a step further and argues that 'these technologies have become not just aids to thought but also part of the thinking process itself', using the harrowing efficiency with which online searches for example can capture and inventorise our private indiscretions (Richards, 2015, p. 121).

Daniel Trottier (2012) maintains that this trend is largely a result of the seismic uptake of digital services particularly in the West. Trottier notably uses the analogy of a *dwelling* when talking about social networks to illustrate how users no longer simply regard the Internet as a gateway to online

information and learning in the way they once had but as an architecture wherein one can reside and achieve a degree of digital naturalisation.

As more and more services migrate online and people make fewer distinctions between their physical and virtual interactions, questions naturally form about whether these largely ungoverned spaces on the Internet can successfully bootstrap our social norms, behaviours and laws and whether the latter is even entirely desirable (Feather, 2008). These have been borne out through debates about 'Net Neutrality', copyright and freedom of speech and have been recently evidenced at the level of government policy-making[1].

By the time the UK government had published its policy paper in 2014 however, public discourse around concepts such as online privacy had already become animated, thanks in large part to the disclosures of NSA whistle-blower Edward Snowden. Among a great deal of other things, these conversations highlighted potentially major pitfalls in terms of the way digital inclusion practices were being implemented in places such as public libraries. Seeta Pena Gangadharan (2012) for example, argued that, 'with few exceptions, the study of digital inclusion has yet to engage with issues of privacy and surveillance that are also a marker of digitally integrated life'.

Other discussions surrounding digital inclusion have similarly attracted critiques that 'policies and practices remain trained on a bounded set of online activities and experiences that entertain only the positive aspects of digitally mediated worlds' (Mossberger, Tolbert, & McNeal, 2008).

In the post-Snowden era, those representing the library profession have credibly argued that concerns surrounding users' online 'intellectual privacy' and security, as well as the various problems

[1] See the 2017 Conservative and Unionist Party's manifesto for 'Digital Charter'. **(Conservative and Unionist Party, 2017: 76)**

posed by digital mass surveillance, were not being tackled from a position of first principles (Clark, 2016, pp. 17-18; Lamana, 2016; Macrina, 2014a; Pedley, 2015; Bradley, 2016).

Cryptographer and privacy specialist Bruce Schneier points out that responses to the development of corporate and government online surveillance have generally been slow on account of the fact that the changes have occurred quickly and covertly (and in many cases extra-legally), providing little opportunity to evaluate their effects or weigh their consequences (Schneier, 2015, pp. 8-9).

The independent inquiry into GCHQ malfeasances and the subsequent enactment of the Investigatory Powers Act (2016), has brought in to sharp relief, the extent to which poorly defined laws in the UK had in some cases legitimised state violation of civil liberties (King & Lock, 2016).

Opponents of mass surveillance maintain that normalising unchecked power in this manner would conversely result in data being gathered about marginalised groups whilst privileged groups increasingly avoided being spied on (Chesha, 2014; Soghoian, 2016).

Similar concerns are evident in research that has revealed that 92% of UK respondents are concerned about their online privacy and have a desire to learn more about how to protect themselves online (Mozilla, 2017; TRUSTe & NCSA, 2016). These concerns may in part explain the emergence of 'cryptoparties' which appear to share many of the principles enshrined in the Ethical Principles and Code of Professional Practice for Library and Information Professionals (Cryptoparty, n.d.; CILIP, 2017).

The CILIP (2015) conference in partnership with IFLA and FAIFE entitled 'Libraries and privacy in the digital age*'* as well as IFLA's (2013) report*:* 'Riding the Waves or Caught in the Tide: Navigating the Evolving Information Environment' suggest that the library profession is not only sympathetic to these challenges but that there is despite all the criticisms it has garnered, a growing appetite for discussion.

In the US however, it is interesting to note that the same set of concerns have led to the forming of compelling alliances between the ALA, ACLU, EFF and the Tor Foundation. Such partnerships have resulted in well-documented landmark initiatives, which I intend to cover briefly in the literature review chapter.

One thing that these partnerships clearly indicate, is a willingness and desire amongst public librarians to not only be better acquainted with the theoretical impacts of digital surveillance, but to have a better practical understanding of the types of free and open source technologies (FOSS) which currently exist and would allow their users to make more informed choices with regards to their online privacy (Macrina & Glaser, 2014; Macrina, 2015a; Newsletter on Intellectual Freedom, 2014).

Overall research aim and individual research objectives

Comparatively little is known about whether public library staff working in the UK, recognise these particular set of concerns in their day-to-day exchanges with library users or whether they are aware of the tensions that exist as a result of many current approaches to online learning that allegedly make little or no provisions for privacy education. Unfortunately, the resources required to carry out an enquiry of this magnitude fall outside the scope of this research.

The intention of this study therefore is to report on library services who are known to be involved in putting forward (or have previously implemented) original online privacy initiatives in the UK and explore their rationale for doing so.

By using at least three exemplary case studies, I explore whether public libraries can realistically work public awareness programs about digital privacy into their existing service strategies, what risks or barriers are likely to be indicative of the sorts of problems public libraries in the UK face more generally and ultimately whether such activities have the potential to be replicated on a wider scale.

To inform the overall direction of this research, the literature review unpacks the term 'privacy' along more general lines in the first instance and then clarifies what is meant by 'online privacy'. For the purposes of this research, attempts at understanding the term privacy rely primarily on Anglo-American perspectives which are woven into law.

It then defines the wider aims and recommendations of digital inclusion with particular regard to UK public libraries, prior to determining what role online privacy should occupy within the spectrum.

It then looks at precedents for public libraries who provide digital privacy initiatives in the US before moving on to frontrunners in the UK, who form the focus of multiple case study research.

In summary, two approaches will be used to carry out this research: firstly, an in-depth review of the relevant literature is undertaken to explore the growing influence of privacy and surveillance on digital inclusion within public libraries based specifically in the US and the UK. Secondly, the collection and analysis of empirical data derived from interviews with librarians representing leading public libraries in the UK, is used to provide insight into the barriers and future pathways of privacy as a digital inclusion project in the UK.

Value of this research

By shifting attention to the public libraries in the UK which are involved in extending the boundaries of digital inclusion and online learning to include concepts such as intellectual privacy, it is hoped that this research will contribute to an improved understanding of the forces likely to be shaping digital inclusion in public libraries across the Atlantic. By reporting on UK initiatives in a qualitative and exploratory capacity to begin with, it is also hoped that opportunities to pursue more quantitative or explanatory research approaches – particularly with regards to digital privacy awareness in UK public libraries - will follow in the future.

Defining privacy

In the UK, *privacy* is defined primarily as a human right by Article 8 of the Human Rights Act (1998). This states that 'Everyone has the right to respect for his private and family life, his home and his correspondence*'*(Pedley, 2011, p. 160).

According to the Oxford dictionary of Law, the right is extremely broad in its implications, concerning itself with respect for individual sexuality, respect for family life (such as cases involving deportation of one family member), the right not to be subject to arbitrary evictions or unlawful entry and the right to uninterrupted and uncensored communication with others (Webb, 2009, p. 396).

Neil Richards agrees that the concept of privacy is for the most part construed as 'an umbrella term that encompasses a variety of related meanings' and which lacks precision because of its dependency on context (Richards, 2015a, pp. 8-9). The elasticity of the term is also widely explored by Shami Chakrabarti and Paul Pedley who establish privacy as the basis upon which the progress of other human rights appears to hinge. Like Richards, they argue that whilst privacy cannot be defined in absolute terms, it is nonetheless critical to the provisions of many of the freedoms we rely on, including privacy as a condition to guarantee sound elections by 'secret ballot' (Article 3 of Schedule 1, Part 2) as well as fair trials which rely on access to confidential legal counsel (Article 6) (Chakrabarti, 2014, pp. 9-10; Pedley, 2017a).

Commentators highlight the confusion arising when privacy principles clash with rights of freedom of expression, particularly those associated with a free press (Richards, 2015a, p. 27; Pedley, 2011, p. 159). Notions of privacy are often defined within the context of tort law (which deals with wrongful acts) and specifically 'disclosure tort'. In the US, disclosure tort was co-opted into law around 1890, as a solution to the 'excesses of the press' and to 'protect elites against emotional harm' (Richards,

2015a, pp. 17-18). Significantly later in the UK, injunctions with similar aims developed to allow 'celebrities to keep private, unflattering facts about themselves out of the newspapers' (Richards, 2015a, p. 41; Pedley, 2011, p. 161).

Scholars argue that it is unhelpful to interpret privacy solely along these lines because, in doing so, it further entrenches the idea that privacy is an outmoded, bourgeois value (Chakrabarti, 2014, p. 5) and that privacy torts are barely concealed pretexts for censorship (Richards, 2015a, pp. 50, 95).

In various cases, UK courts have rejected arguments for a generic tort of breach of privacy which judges envisaged 'could give rise to as many problems as it is sought to solve ' (Wainwright, 2001, cited in Markesinis,Cinneide, Fedtke, & Hunter-Henin, pp. 2-3). This is not to imply that the judiciary systemically undervalues privacy or that privacy rights should always be jettisoned in favour of freedom of expression. Bad faith arguments, according to Richards (2015a, pp. 78-82, 96), ignore the fact that the courts have always tended to move cautiously in order to avoid setting complex precedents for the future.

Markesinis et al. take a far more critical position, insisting that 'judicial timidity' has lead to a culture of opting for the path of least resistance which in turn has undermined a credible law on privacy from advancing. Moreover, the authors argue that this has stretched existing torts out of shape to meet new requirements in the 21st century (Markesinis,Cinneide, Fedtke, & Hunter-Henin, 2004, pp. 1-2).

Chakrabarti (2014, p. 6) concludes that these different attitudes promote an instinctive rather than an entrenched approach towards privacy as a wholly protected right. Whilst this makes cases challenging to defend on privacy grounds alone, it allows each case to be examined in context and balanced against other interests (breach of confidence, defamation, statutory data protection, etc.) (Webb, op. cit.).

There is also broad consensus that notions of privacy reflect longstanding values associated with human dignity. This considers, amongst other things, the capacity for an individual to be afforded some protection or measure of control over information pertaining to themselves, depending on the context (Chakrabarti, 2014, pp. 9-10; Pedley, 2017a; Richards, 2015a, p. 8).

In the UK, this has been most commonly assured through safeguards such as the Data Protection Act 1998 (DPA)[2] which controls how personal information is used by organisations, businesses or the government (Pedley, 2011: 120; Privacy International, N.D.).

Unlike the recent development of expensive injunctions, the DPA regulates the flow (or 'processing') of personal and sensitive data concerning not just social elites but any living identifiable person, where these are held as part of a 'relevant filing system' (Pedley, 2011, p. 120; Feather, 2008, p. 146).

The DPA also offers practical and nuanced solutions to pre-emptively tackle misuses of personal data as well as wrongful or irresponsible disclosures of sensitive facts about ordinary individuals (Richards, 2015a, p. 162).

The DPA is however limited in some important ways and whilst data, as Richards (2015a, p. 90) points out, will sometimes be tied to important expression (such as religious views or political affinity), the third principle of the DPA - which specifically limits the *gathering* and sharing of personal data about subjects which is excessive – is clearly not intended to refer more widely to speech and other critical activities which lie outside of its scope.

Interestingly, the DPA is couched in the language of confidentiality, rather than privacy per se,

[2] A model which so far has proved instrumental in shaping the forthcoming General Data Protection Regulation (GDPR) which is expected to become UK law in May 2018. **(Information Commissioner's Office, 2017).**

and highlights the act as a duty of confidence between the data controller and the data subject. Futhermore, the legislation is geared around personally identifiable information of individuals (PII) but does not anticipate 'situations where we are talking about bulk datasets, where the target wasn't necessarily one individual at all, but where it then has consequences for a number of individuals. It is defective in many regards as a result' (Pedley, 2017b).

So privacy at least in UK law, is a qualified right, which although supported strongly in principle, is underdeveloped in certain areas of practice. The reluctance of the courts to create a generic tort of invasion of privacy or occasionally adjust the bounds of specific torts to suit novel situations that impact on our lives in the digital age is not necessarily without some sound justifications.

Judges, as we have read, argue for the most part that case law has actually proven to be far more effective at tackling 'different privacy interests and infringement situations' whilst remaining consistent to obligations of freedom of expression (Markesinis, Cinneide, Fedtke, & Hunter-Henin, 2004, p. 4).

Richards says that at a general level, not all privacy problems will be resolved by a single tool such as the DPA but warns that even a raft of different torts, of the types currently favoured by English courts, would have to be cautiously crafted to meet the problems of privacy in a digital society (Richards, 2015a, p. 72).

To arrive at a sound definition of 'online privacy' therefore it is worthwhile considering the types of problems privacy theory is expected to deal with in the digital age.

Defining online privacy

Online privacy (also known as Internet privacy) unsurprisingly contends with many of the same issues as privacy as defined by Article 8. The right to respect for private and family life, property and correspondence however is thrown into practical disarray when we consider the pervasiveness of digital

technologies which now have the capacity to both disrupt our social norms (Schneier, 2015, pp. 128-9) as well as create and retain records of our online activities as a matter of course (Schneier, 2006; Richards, 2015a, p. 96).

Respect for private and family life online for example, is often understood as a *reputational* issue which carries with it implications for the way we present ourselves and our ideas (through our online identities) depending on whether we are with our intimates, friends, family, professional acquaintances or complete strangers.

Just as they do in the physical world, online identities rely on certain boundaries which establish usually by degrees, the levels of trust between individuals before they can become accepted confidants (Morozov, 2014; Richards, 2015a, p. 146). Payton and Claypoole (2015, p. xi) describe these private boundaries as 'concentric circles with ourselves in the centre':

> In the middle, held closest to us, are the secrets, thoughts, and rituals that we keep entirely to ourselves and share with no one. Further out are the conversations we have and the actions we take that involve others but that we expect to remain private. We also expect a measure of privacy toward the outer circles, as some issues are kept within the family or inside our company without further publication.

But in a networked environment designed with persuasive techniques to maximise the social reciprocity of its users and the amount of personal information that they share across platforms, such boundaries can become blurred to spectacular effect **(Harris, 2016).** This often leaves users' reputations as well as general information vulnerable to abuse (The Electronic Frontier Foundation, 2014).

Furthermore, Richards (2015a, p. 147) argues that the online world distorts our perception of who and where our confidants and 'trusted' intermediaries really are, citing Internet service providers, multinational search engines, cloud storage providers and social networks as entities who are all competing for information proximity.

The concept of private property, whether it is online or physical, has a wide range of associated meanings but can generally be understood as something that we own or is of value to us and therefore requires a basic level of protection. In both cases, property rights are regarded as a concern of *security*. Business ideas for example require a degree of privacy or protection in the development stage (i.e. before they are ready for public consumption) in order to compete successfully in the marketplace (Payton & Claypoole, 2015, p. xi).

In security terminology the things we wish to protect are referred to as *assets.* When discussing digital security, the assets in question are typically sets of information which could include, but are not limited to: emails, contact lists, instant messages and personal files (The Electronic Frontier Foundation, op. cit.). When using 'free' websites such as Facebook however, users effectively agree to relinquish their privacy, at least in part because the benefits of doing so loom more largely then the losses (Acquisti & Grossklags, 2006).

This is less surprising when we consider how services' obligations to protect information are increasingly bound by highly technical privacy policies which have the capacity to redraw the lines of trust and diminish informed consent. When users under estimate the long-term value of their personal information in this way, they are often described by security experts as succumbing to a Faustian-style contract whereby the information they impart continues to be brokered long after the initial period of agreement (Schneier, 2015, p. 58; Williams, 2013).

What becomes startlingly apparent online, are the tensions that exist between the expectations for our private information to be used responsibly and the pressures to use technologies and participate in digitally mediated worlds that increasingly utilize mass surveillance and big data techniques as part of their business models.

Schneier **(2015, p. 24)** attributes this paradigm shift to declining costs in computing technology which in turn has opened the door to trickle down surveillance:

> As computer technologies improved, corporations were able to collect more information on everyone they did business with. As the cost of data storage became cheaper, they were able to save more data and for a longer time. As big data analysis tools became more powerful, it became profitable to save more information.

Facebook is also ubiquitous around the Internet by virtue of its shares buttons and its cross-platform authentication features (Schneier, 2015, p. 31). According to Cheshire (2017) 'It follows you around the Internet, tracking your every click. It then combines that information it gathers with third party sources like Experian, which builds up consumer profiles based on credit card spending and other sources'.

Equally problematic, is the notion that whilst some organisations do not take sufficient steps to adequately protect users' data from online breaches or attacks (McCandless, 2017, Goldacre, 2017) those that do, are often pressurised by governments intent on exploiting software and technology with security vulnerabilities as part of their mass surveillance regimes (Schneier, 2015, p. 146; Kelion, 2017). This proved to be the case when the NSA was found to have links with the WannaCry ransomware, used to target the vulnerabilities in Windows XP software around the world. It is widely believed that other vulnerabilities (known as 'zero day exploits') are regularly stockpiled by such agencies in order to spy on their government's adversaries, but which then have severe ramifications for all users of that software (Smith, 2017; Snowden, 2017).

Like private information, personal correspondence is similarly characterised by concerns for *security.* Being able to speak freely with our contacts for instance relies on secure communication practices that are best assured through systems of online trust and techniques such as encryption (Richards, 2015b).

Where guarantees of trust can be difficult to establish even in the physical world, ephemerality and 'conversations that disappear as soon as they occur', are social norms that have previously allowed us to be more relaxed and comfortable. Such norms allow us moments of indiscretion, the possibility to change our minds about certain topics as we learn, and the capacity to explore new or controversial ideas without being bound to them forever. In the digital sphere, 'losing the ephemeral will be an enormous social and psychological change, and not one that […] society is prepared for' (Schneier, 2015, pp. 128-9).

Richards (2015b) expresses similar concerns in his defence of principles such as online anonymity and encryption, which he argues matter to everyone 'because [they protect] our intellectual privacy -- our ability to be protected from surveillance or interference when we are making sense of the world by thinking, reading and speaking privately with those we trust'.

So whilst *privacy* is often inaccurately used as a synonym for *secrecy* and regularly mischaracterised as the need to hide embarrassing details or "bad" behaviour (Payton & Claypoole, 2015, pp. 2-4), most scholarly literature reveals it to be much more multifaceted. In the online world, privacy impinges on a raft of different issues including our reputations, how we set our boundaries, who we trust and how they are accountable to us, our security threat models, and our agency as individuals.

My research is therefore concerned with many of these facets whilst using Richards' model of *intellectual privacy* as a vehicle to explore digital privacy initiatives in UK public libraries.

How is online privacy accounted for in UK digital inclusion programmes?

Digital inclusion built on the original Skills for Life agenda in the UK (which supported public literacy, numeracy and ICT initiatives in places such as public libraries) in order to help the British

population fulfil their civic obligations, receive their entitlements and realise their potential in society (Department for Business, Innovation and Skills, 2012, pp. 3-4; CILIP 2014; Feather, 2008, p. 144).

According to a 2012 report, which examined the distribution of these skills across the country, the main benchmark for assessing online competencies involved how proficient respondents were in the use of email. Other components of the assessment were limited to word processing and the use of spreadsheets (op. cit.).

Around this time Sena Pena Gangadharan (2012) cogently argued as DiMaggio et al had before in 2001 that digital inclusion initiatives were not teaching its beneficiaries about the social implications of using such technologies from first principles (DiMaggio, Hargittai, Neuman, & Robinson, 2001).

In 2014 a digital inclusion strategy was officially undertaken in the UK to confront the findings of earlier reports which evidenced what became widely known as the digital divide. The term, according to Segev (2010, p. 7) referred to:

> The gap and inequality in accessing online information, the capacity and skills of ICT use, the technical quality of the network, the government and social investment for online infrastructure and education, the overall ability to translate and evaluate information, and the social diversity of its users.

As with previous years, the government was concerned about claims that people with poor basic skills knowledge were less productive at work, earned lower wages, were more likely to suffer from ill health and experience social exclusion (Department for Business, Innovation and Skills, 2012, p. 11; Cabinet Office, 2014). Unlike earlier years, the government's new proposed digital skills stimulus coincided with ambitious plans to move a huge swath of its services online, making them 'Digital by Default'. Many including the MP for Newcastle-upon-Tyne in 2014, Chi Onwurah, criticised the government's approach arguing that it risked further isolating long marginalised communities and

'putting the cost of going digital onto them and not where it belongs, with the government' (Rust, 2014; Feather, 2008, p. 131).

It is unsurprising as Clark (2016, p. 2) remarks that initial efforts were therefore focussed, first and foremost, on improving infrastructural access to the Internet. This was achieved in part by investing in a reported 42,914 public computer terminals, in addition to free Wi-Fi, across public libraries in Britain (CILIP: 2014; Feather, 2008, p. 185). In addition to this, the 2014 Government Digital Inclusion Strategy identified three other areas that it considered crucial to the challenges of nationwide online access (Cabinet Office, op. cit.). These included:

- skills - to be able to use the internet
- motivation - knowing the reasons why using the internet is a good thing
- trust - a fear of crime, or not knowing where to start to go online

The Challenges that people face

Access	Skills	Motivation	Trust
Accessibility	Literacy skills	Risks	Identity
Location	Digital skills	Necessity	Security
Cost	Security skills	Financial benefits	Standards
Technology	Confidence	Social benefits	Reputation
Infrastructure		Health and wellbeing benefits	
Language			

Table 1. Table identifying 4 main kinds of challenge (and their subdivisions) that people face with regards to going online – Government Digital Inclusion Strategy (Cabinet Office, 2014).

One of the most salient things to emerge from the strategy was the fact that the word 'privacy' itself was almost entirely absent from view (Cabinet Office, op. cit.). (The one notable exception was where it cited external research compiled by post-graduate students at the London School of Economics who identified privacy concerns as a barrier to going online, affecting almost 36% of respondents (Annex 3: Digital inclusion landscape review cited in Cabinet Office, op. cit.).

On reviewing the definitions of 'online privacy' outlined in chapter 2.2 however, it is still possible to unpack privacy interests from the associated headings of: *security skills, trust, identity* and *reputation.*

Throughout annex 1 of the paper dealing with challenges, privacy although not mentioned explicitly, is allied with the notion of *online safety,* which is generally understood to be:

> The knowledge of maximizing the user's personal safety against security risks to private information and property associated with using the Internet, and the self-protection from computer crime in general (Scheff, 2015).

Security risks are largely identified in the paper as structural insecurities (database breaches) and criminal activity such as online attacks and data theft (ID fraud). The use of the word *safety*, meaning a contrivance to prevent injury or avert danger, is also significant and to some extent avoids having to deal with the grey areas of legally tolerated forms of online social engineering, known as *nudging*, (Bercovici, 2016; Harris, 2016) or what Mai (2016) refers to in his research as the 'surveillance, capture and datafication' models of privacy.

The report's definitions of trust are similarly limited to targeted online manipulation such as *phishing* by criminals impersonating personal contacts or official services in order to gain access to private information. Disappointingly though unsurprisingly, it does not address the widespread problems associated with profiling (Schneier, 2015, p. 109; Gangadharanm 2012; Information

Commissioner's Office, 2017a, p. 3) or other abuses of trust which occur as result of state or corporate surveillance opportunism.

In the US, the most well-known cases of profiling include racial profiling, redlining, and medical profiling (Schneier, 2015, p. 109; Gangadharan, 2012). In the UK, these techniques allow gambling companies to successfully target poor households and ex-gamblers (Busby, 2017). According to the ICO (2017a, pp. 3-6) such techniques involve the gathering of information about individuals or groups (usually without their knowledge) and analysing their characteristics or behaviour patterns in order to place them into categories or groups. Inferences are then made about their ability to perform a task, their interests or their likely behaviour, all of which can be derived from a range of disparate sources of data, using sophisticated technologies which until recently have received little public scrutiny.

Furthermore, the ICO (2017a, p. 6) claims that even if no decision is made on the basis of the profiles, the ramifications remain nevertheless profound because of 'the potential for the data to be harvested or mined for information and its commercial value'. They then go on to enumerate the risks which reaffirm Gangadharan's (op. cit.) earlier research that surveillance technologies and practices disproportionately affect vulnerable communities who have little or no resources to challenge them.

Benefits	Risks
Better market segmentation	Infringement of fundamental rights and freedoms
Permits analysis of risks and fraud	Certain sectors of society may be underrepresented – e.g. older generation/vulnerable individuals or those with limited social media presence
Adapting offers of goods and services as well as prices to align with individual consumer demand	Can be used to deduce sensitive personal data from non-sensitive personal data, with a reasonable degree of certainty
Improvements in medicine, education, healthcare and transportation	Unjustifiable deprivation of services or goods
Provide access to credit using different methods to traditional credit-scoring	Risk of data broking industry being set up to use information for their own commercial interests without individuals' knowledge
Can provide more consistency in the decision making process	Using profiling techniques can jeopardise data accuracy

Table 2. Table highlighting some of the more widely recognised benefits and risks of profiling – Information Commissioner's Office (Information Commissioner's Office, 2017a, p. 6)

For many users, the idea of identifying 'credible' online services, as the paper correctly highlights, is also fraught with uncertainties. What the paper fails to recognise however is the fact that user confidence is perpetually undermined when the services and websites being recommended are themselves operating on the edges of the law or as a result of large power differentials which render them difficult to challenge in the abstract (Schneier, 2015, p. 162). This was highlighted around the time of the strategy's implementation when the reputable security firm AVG was found to 'sell search and browser data to advertisers in order to "make money" from its free anti-virus software' (Clark, 2016; Temperton, 2015). In the same year, a study revealed that two out of three people deliberately obfuscated information in online forms because they didn't trust companies to use their data responsibly (Griffin, 2015).

There are many potentially valid reasons why a strategic paper whose aim, to provide a rationale for assisting learners get online, may not consider it suitable to broach such complex subjects. But even

if we were to take a generally benevolent view of the government, such omissions leave an incomplete picture of the reality of online experiences and deprive the individual of making informed choices. As Ganagadharan (op. cit.) states in her research:

> [A] conventional framework of digital inclusion prepares individuals for participation in idyllic online worlds. But such visions are blind to established histories of state and corporate surveillance and exploitation of chronically underserved communities. Until 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.

In the year following the Snowden disclosures of 2013, when the Guardian had already published details of GCHQ's controversial Tempora program (MacAskill, Borger, Hopkins, Davies, & Ball, 2013), the near absence of the word privacy in the digital inclusion strategy paper may arguably have struck some as disconcerting.

The strategy paper nevertheless went on to inform the structure of many digital initiatives and lesson plans including 'Learn My Way' (formerly known as 'Go-ON UK'), the official resource of the Online Centres Network. This included 2,931 public libraries and was known to be used by at least 857 public libraries across the UK between 2015-2016 (Wilson, 2016).

Since 2014, the online resources delivered by the free course provider Learn My Way have been updated and now provide guidance on how to set up Facebook profiles as well as how to manage one's digital footprint (Learn My Way, 2017). Stakeholder feedback on the Online Centres Network's website however, revealed that the resource supported by almost 3000 public libraries in the UK did not make sufficient provisions for meeting online privacy concerns (Online Centres Network, 2017).

Given the huge interest in the online commercialisation of personal data, the reality of resources such as Learn My Way is that (at the time of writing) they do very little to emphasise the importance of

reviewing online privacy settings or challenge the use of nominally free[3] services (where the cost is hidden from the user) (Learn My Way, 2017). Rather, they direct learners systematically to services that rely on advertising revenue or monetising users' online personal data by other means (ibid.). The resource also gives no indication of how to evaluate or research services in order to determine their reputation or accountability and only explores the positive motivations that companies have for collecting personal information (ibid.).

In a module entitled 'using a touchscreen', no guidance is given on how to review or configure the privacy and permission settings of Android devices which are amongst the most popular because of their relative affordability to Apple products. At the current time of writing, Apple unlike its rival, bakes privacy into its business model and encrypts its video chat and messaging services by default (Schneier, 2015, pp. 50-51). Christopher Soghoian (2016) explains that its steep price differential however creates 'not just a digital divide but a digital security divide' (Simonite, 2015). In spite of this, simple measures do exist to improve mobile privacy and protect the data held on Android devices (DuckDuckGo: 2017) but in the absence of such guidance, Learn My Way advances a reactive rather than a preventative approach to concerns about loss of privacy.

Alternative online workshops which are being promoted in public library venues but are increasingly delivered by private companies have been similarly criticised. Clark (2016, p. 17) for instance says that the Barclays Digital Eagles scheme offers 'no guidance regarding privacy protection tools online'. He goes on to say 'the main services recommended by Barclays include Google (for search and

[3] 'Free' in this context refers to the Internet business models that rely predominantly on selling personal data to advertisers in order to make a profit. In this research it is distinguished from 'FOSS' (free and open source software).

email), Yahoo!, and Outlook.com – all of which have been either forced to hand over data to, or have had a relationship with, the NSA'.

Websites such as 'Get Safe Online', which is referred to as the 'UK's leading source of unbiased, factual and easy-to-understand information on online safety', present a considerably more honest account of intellectual privacy issues although they are still far from perfect and it is unclear to what extent they are used to teach online privacy in public libraries. On the Get Safe Online website, concepts such as surveillance for example, are only alluded to in terms of 'cyberstalking' or physical surveillance 'shoulder surfing'. And whilst tools such as VPNs are mentioned, they are considered to be of relevance only to 'businesspeople' (Get Safe Online, n.d.).

Looking for precedents of digital privacy initiatives and the need for new research focussed on the UK

In spite of the continued relevance of staff-mediated services in libraries, where librarians for instance undertake searches on behalf of users (Feather, 2008, p. 185), Internet technologies have increasingly come to occupy that space and mediate the activities of thinking, reading, and communicating. (Richards, 2015a, p. 175).

As a result, we have become gradually more reliant on the digital intermediaries of software engineers and online services whose conscious, as well as unintended, business and design choices have come to shape our online behaviours and experiences. Richards (2015a, p. 176) says that since intellectual privacy has become a digital issue and is increasingly dependent on intermediaries in the online world, it naturally follows that we should seek to understand their ethical starting positions, as we have done in the past with more traditional information fiduciaries in the fields of medicine and law.

In the UK the standards and practices of librarianship, as a profession, are governed by the 'CILIP Ethical Framework' (CILIP, 2017). Point 8 of the ethical principles for example, explicitly states 'that the

conduct of information professionals should be characterized by respect for confidentiality and privacy in dealing with information users' (Pedley, 2011, p. 163, CILIP, op. cit.). The fourth responsibility to information users within the codes of professional practice also states that information professionals should 'protect the confidentiality of all matters relating to information users, including their enquiries, any services to be provided, and any aspects of the users' personal circumstances or business' (CILIP, ibid.).

In the US, the American Libraries Association (ALA) explores the concept of reader privacy and its relationship to intellectual freedom in a document entitled 'Privacy: An Interpretation of the Library Bill of Rights' (American Library Association, 2006). Within it, the policy provides clear definitions of privacy as 'the right to open inquiry without having the subject of one's interest examined or scrutinized by others' as well as confidentiality (the keeping of such information private on behalf of the user) and in doing so, builds unambiguously on the rights to privacy that have been upheld by the ALA since 1939. Its first commitment, under 'Rights of Library Users' for instance plainly states that:

> Lack of privacy and confidentiality has a chilling effect on users' choices. All users have a right to be free from any unreasonable intrusion into or surveillance of their lawful library use.

The second commitment asserts that because the 'library profession has a long-standing commitment to an ethic of facilitating, not monitoring, access to information' libraries should take care to only collect personal information where it is 'necessary for the fulfilment of the mission of the library' (ibid.).

Intellectual privacy theory and library ethics thus reveal an interesting paradox:

> [W]e need intellectual privacy to make up our minds, but we 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, 2015a, p. 180).

Experts observe that such ethical approaches, with regards to the capture and retention of data, have proved largely absent from the modern information economy except in a relatively rare set of circumstances[4] (Schneier, 2015, pp. 199-200; Fowler: 2013).

Deborah Caldwell-Stone says that if surveillance is the business model of the Internet as Schneier (2015, p. 49) has claimed, 'then public libraries are well placed to function as an intermediary and a defense against surveillance at least at the individual level' (Deborah Caldwell-Stone cited in Carnegie Trust, 2017).

Feather (2008, p. 189) and Caldwell-Stone both note for example that librarians have applied – and indeed developed – privacy enhancing techniques in their use of technologies such as circulation systems and databases, long before the rise of the Internet (Carnegie Trust, op. cit.).

As Internet technologies have progressed, librarians in the US have proved particularly responsive to the privacy challenges posed by commercial enterprises such as Adobe Digital Editions, whose practices of collecting and transmitting large amounts of unencrypted data[5] about the readers who used their e-book platforms, otherwise went largely unnoticed. The ALA however managed to persuade Adobe to encrypt the data transmissions, ensuring that readers' privacy was adequately protected (Clark, 2014; Dobbs, 2014).

Caldwell-Stone (Carnegie Trust, op. cit.) also remarks that libraries are 'trusted community institutions that offer confidential information services in a non-commercial atmosphere'. Further testaments to the level of trust placed in public libraries are widely reflected in the surveys conducted

[4] Countries such as Germany who have a long memory of the surveillance state for example now have strong privacy regulations which inform data collection practices, known as *datensparsamkeit* (which roughly translates as 'data stinginess') (Goetzmann, 2016).

[5] Adobe sent data about readers' e-book reading habits to its servers in 'plain text' as opposed to using scrambled code.

by the PEW research centre who in 2016 concluded that libraries provided 'a trusted place for people to learn about new technologies.' Moreover 80% of PEW's research respondents agreed that libraries should definitely 'offer programs to teach people, including kids and senior citizens how to use digital tools such as computers, smartphones and apps' (Horrigan, 2016).

In the US in particular, there is considerable evidence to show that pubic library staff are expanding and redefining the territory of digital literacy and inclusion in order to assist members of their communities make informed decisions about their online privacy.

The San José public library in California for example embarked on a project with members of the Teaching Privacy team at the Berkeley-based non-profit International Computer Science Institute, to develop a Virtual Privacy Lab using gaming concepts to teach the basic tenets of threat modelling and help users 'of all ages' become privacy literate (Berman & Worona, 2016).

The activities of the Library Freedom Project (LFP), an organisation founded by former Boston-based public librarian, Alison Macrina, have been paramount in contributing to the understanding of digital mass surveillance as a threat to the commons of knowledge and therefore to the founding principles of public libraries in particular. Following the Snowden revelations, Macrina sought partnerships with fellow librarians, technologists, attorneys and privacy advocates, to raise awareness of both, state and corporate practices which were hostile to online intellectual privacy, as well as free and open source software (FOSS) and technologies which purported to shield users from various forms of online surveillance.

In 2014, Macrina successfully delivered digital privacy classes to members of the local community at the Watertown Free public library in response to growing concerns amid users that their library activities were being monitored (Macrina & Glaser: 2014). Privacy protection tools were

subsequently installed on public library computers to give users more agency over their web browsing and the choice to opt out of online surveillance in public libraries more generally.

This inspired Macrina to engage more widely and publicly with library workers who were sympathetic to privacy concerns and the impacts of mass surveillance on the intellectual freedom and expression of their communities. This in turn resulted in staff training being set up across various states (LILRC, 2016; Macrina, 2014b; Macrina, 2015b) with the aim of empowering public libraries to implement their own local initiatives.

We now know that the LFP mission and stimulus material paid dividends, culminating in privacy events for the general public in libraries particularly across the East coast of the US; from Medway Public Library in Boston, to Portland Public Library in Maine, and Stowe Free Public Library in Vermont, to name just a few examples (Macrina, 2014c; Macrina, 2015a; LFP, 2016).

The LFP website also features guest blogs from public libraries who have independently developed privacy initiatives. These include the Santa Clara City Library in California, whose library staff delivered classes on strong passwords, HTTPS and browser add-ons (Wasterlain, 2015) and the Lebanon Libraries in New Hampshire where library staff installed GNU/Linux computers to provide a more secure online environment for library users (McAndrew, 2015).

Much media coverage was given to a pilot scheme involving the installation of a Tor node known as a 'middle relay' at the Kilton Public Library. The node would enable the library to be the first of its kind to contribute bandwidth to a popular decentralised web browsing tool which ensured all online traffic which passed through it was anonymised thanks to three overall layers of encryption (Koebler, 2015). In mid-2016, the library also became the only public library in the US to operate a Tor 'exit relay' (Associated Press, 2016). This carries considerably more risk due to the fact that 'Tor users

take on the IP addresses of their exit node operators [exposing] those exit node operators to liability for any Tor user's wrongdoing' (Eagle, St. Hilaire, & Sherwood, 2013, p. 8). Whilst the case at Kilton raised some legitimate concerns about the potential for misuse by other Tor users in the network (most notably issues related to obscenity such, as child pornography, and copyright infringement), Macrina argued that in the interests of preserving privacy, enabling free speech and facilitating political reform, 'libraries [could] afford some of the legal exposure that comes with an exit' (Macrina & Fatemi, 2015). The venture ultimately won the support of state representative Keith Ammon, who helped to usher in a bill that was successfully passed into law in 2017, allowing libraries to run privacy software (O'Neill, 2016).

Although the operation of Tor relays is by no means illegal either in the US or the UK, the legal provisions which cover the operation of exit nodes in the US, under Safe Harbor and the DMCA, are much more clearly defined than in the UK, thereby offering substantially better assurances for those operators (Eagle, St. Hilaire, & Sherwood, 2013, pp. 10-11; The Tor Project, 2011).

The rights guaranteed under the US constitution and particularly, the First Amendment also 'provide a lever which librarians can use against the state to defend intellectual privacy' more effectively than in the UK where there is generally speaking no equivalent (Clark, 2016, p. 19). Furthermore, the federal government in the US does not superintend public libraries to the same extent, in spite of the funding they receive (ibid.).

The British government has also publicly opposed the use of encryption technologies on a number of separate occasions related to terrorism incidents (Lomas, 2017; Revell, 2017) which, in the aggregate may have had a naturally discouraging effect on librarians and educators wanting to explore digital privacy initiatives at a grassroots level.

In early 2016 Clark (2016, p. 20) concluded that efforts to defend intellectual privacy within UK public libraries had been lacklustre:

> At present, in contrast to the efforts of library associations and librarians in the US, UK equivalents to the Library Freedom Project have not emerged and there are currently no efforts by CILIP comparable to those of the ALA. […] [I]n the current environment the delivery of such programmes in public libraries managed by local authorities seem unlikely.

In late 2016 however, a public library in Newcastle in the UK moved resolutely towards implementing a digital privacy workshop aimed at sharing good practice with members of the public (Charillon, 2016a). The initiative was believed to be the first of its kind (Haydock, 2016) and is certainly regarded as the first example of a UK public library to explore the intersection between digital inclusion, intellectual privacy and professional library ethics (Charillon, 2016b).

In this respect, the development represented a potential milestone in the study of digital inclusion in UK public libraries, but the secondary data cited above remains limited in some important ways. It is unclear, for example whether public libraries like Newcastle City regarded the provision of digital privacy education as part of their mission to promote informed choices for all or whether it was simply a case of meeting the demands of a particular subsection of the community whose needs and interests were different to those of other groups.

The project's author said that her manager was sympathetic to her proposal to host a cryptoparty, but it is difficult to know to what extent this boosted the project and whether a more adversarial relationship might have impeded such efforts. Other barriers or potential risks were not specified and mentions of particular constraints such as web filtering appear to have referred to hypothetical initiatives.

Lack of documentation, as noted in the literature review concerning the UK at this stage, was likely due to a number of factors including: the undervaluing of intellectual privacy at the level of policy-

making as well as uncertainty with regards to UK law, which had so far favoured mass surveillance arguments and explored measures to ban encryption technologies. Through the inevitable politicisation of concepts such as digital intellectual privacy, public library staff may have instinctively felt that to engage with such initiatives implied taking a side where there might have been a certain expectation to remain 'neutral' (Peachey, 2017, p. 5). Other factors such as local government efficiency savings, resulting in the fracturing and outsourcing of certain library services, would have no doubt also contributed a role (Rust, 2014, Wilson, 2016).

Such questions are central to the premise of this research because they may hold the key to answering broader questions about the perceived roles of public libraries and how far they are prepared to go to uphold certain principles. As such, it was felt that empirical research, in addition to secondary data, was needed to, extrapolate where possible the rationales for implementing digital privacy initiatives in UK public libraries such as Newcastle City, as well as to offer insight into their potential to be replicated more widely.

Research Methods

Introduction

A valuable aspect of this research related to finding out who the frontrunners of digital privacy inclusion were within public libraries in the UK. The literature review concluded that this could not be achieved by commenting on secondary data alone as Anglo-American discourse at the time of writing, was considerably more weighted towards the US where digital privacy initiatives, concerning public libraries, were well documented (Clark, 2016, p. 20).

This presented some obvious challenges when it came to accounting for initiatives, such as pilot schemes, which were conceivably taking place in countries such as the UK but which may not for

instance have achieved the critical mass, or have had access to the professional publicity streams, or systems of peer review required to put them on the map.

The literature review succeeded however in shedding light on the work of Aude Charillon in Newcastle Libraries (Charillon, 2016b), in addition to providing a useful framework with which to discuss new forces emerging in the field of digital inclusion that incorporated intellectual privacy. It was also this framework that was used to foster exchanges with public librarians and others, in an attempt to bring to light similar initiatives and practices worthy of study in the UK.

Providing that other initiatives were indeed being developed within the UK, it followed that this research should report on the character of those initiatives and explore their stated goals. As outlined in chapter 1 of this research, these accounts held the potential to reveal common motivations or strategic challenges which could provide a means of speculating more widely on the capacities for public libraries to deliver digital inclusion programs that were more orientated towards intellectual privacy.

Research Strategy

The first concern of this research was to identify a particular phenomenon in the UK based on models observed in the literature review i.e. US public libraries that provided online privacy training to the public as part of a digital inclusion narrative.

Because the nature and study of the phenomenon of digital privacy in public libraries was still considered to be in its infancy however (Charillon, ibid.; Clark, op. cit), a survey approach which used quantitative techniques such as sampling to make inferences about a larger population, was likely to be highly unsuitable to a UK context where the true population size was unknown to begin with.

This research therefore focused on qualitative case studies as the most effective and appropriate means of gathering in-depth information about a very specific set of practices which, based on the

available knowledge, was judged likely to be of relevance to only a small minority of public libraries across the UK (Clark, 2016: 20).

As this was a relatively novel area of research, it was also anticipated that the research strategy would incorporate elements of the exploratory and descriptive approaches to case study research, rather than strive to provide a generic explanation for the relationships between digital privacy initiatives and digital inclusion within UK public libraries.

Whilst a descriptive framework was necessary in order to understand the operational detail of privacy initiatives in the UK and answer the research objectives related to known risks and barriers, an exploratory analysis was also essential. Supported by the literature review, this aimed to go beyond purely descriptive elements in order to approach questions about the feasibility of wider replication and a more rigorous emphasis on privacy as a core library value.

Furthermore, an exploratory approach was desired to inform the direction and nature of future research questions regarding the progress of digital privacy in UK public libraries.

Data Collection

In order to answer the primary research aim (who are the frontrunners of digital privacy education in UK public libraries?), it was necessary to produce carefully defined criteria, in order to identify and then determine the eligibility of candidates to be approached more formally to participate in the case studies (Yin, 2009,np. 91). This process aimed to finesse the data collection plan 'with respect to both the content of the data and the procedures to be followed' (Yin, 2009, p. 92).

The criteria for candidate participation in this research are outlined below with justifications for each criterion further down:

- Past or present digital privacy initiatives needed to be facilitated, at least in part, by a member of public library staff (i.e. Library Managers, Librarians, Library Assistants, Library Volunteers or Library Trainees);
- The library staff member(s) needed to be based in a UK public library;
- Participating public libraries needed to meet the 'local authority' definition as described in the Public Libraries and Museums Act 1964 and not merely constitute a library that was openly accessible to the public;
- Digital privacy initiatives needed to be delivered within the confines of that public library or another venue or space which was connected with the library in question;
- Digital privacy initiatives needed to constitute practices which in some way deviated from the routine activities associated with the public library in question;
- Digital privacy initiatives needed to constitute exchanges between public library staff and members of the public rather than simply staff training opportunities.

By defining the parameters of the multiple case studies in this way, it became possible to focus on the role of the target group (public library staff based in the UK) involved in implementing digital privacy initiatives for the public, as opposed to the roles of third party groups[6]. Secondary research showed that this latter group was invested in tackling similar issues but often had values and agendas that were wholly different to those of the public library profession (Clark, 2016, p. 17).

The screening criteria were also designed to exclude certain open access libraries (for example the Médiathèque of the French Institute in London), which are held to different standards and benefit

[6] See 'Barclays Digital Eagles' in Clark, 2016, p. 17.

from different funding models. This allowed for a shrewder analysis of the types of risks and challenges that directly affected local authority libraries (Rust, 2014, Wilson, 2016).

The fact that digital privacy initiatives in this research were strictly limited to public library spaces was also significant because it served to highlight risks or challenges associated with the image and perception of public libraries as 'neutral' or 'safe spaces' (Peachey, 2017, p. 5).

The condition that specified that digital privacy initiatives differ in some way from the service norm was also useful because it automatically discounted baseline practices, such as the configuration of public computers that support restoration software[7]. These more often than not reflected long established policies on user privacy and confidentiality rather than the concerted efforts of individually engaged members of library staff.

The final condition, which framed the digital privacy initiative as an exchange between user and public library worker, was important because it focused on a community-grassroots approach rather than a top-down strategic approach to digital inclusion which usually has broader aims and does not typically[8] account for intellectual privacy concerns to the same extent (Clark, 2016, p. 17; Learn My Way).

The process of candidate selection initially relied on what was revealed in the findings of the literature review, which highlighted Aude Charillon from Newcastle City public library as a prime candidate for this research. The criteria above however were instrumental in appealing for additional responses from candidates across the UK.

[7] I.e. to clear a user's computer activity once they have completed their session.
[8] The Library Freedom Project staff training schemes in the US have so far shown to be the exception which proves the rule.

Despite the narrow eligibility criteria, the approaches for identifying candidates, by necessity of the research (which concerned the territory of the UK), needed to extend nationally rather than just locally. Reaching out to respondents was therefore undertaken through:

- A variety of access arrangements (Yin, 2009, p. 91) to national discussion groups and mailing lists such as the Jiscmail email list for the Radical Librarian Collective (http://www.jiscmail.ac.uk/RLC-DISCUSS);
- Engaging with special interest groups that were active on social media such as the Multimedia Information and Technology Group (MmIT) of CILIP, representatives of Public Library News (PLN) and the Library Freedom Project[9] (LFP);
- Contributing to public discussion boards within blogs and forums of like-minded groups such as the Open Rights Group (ORG) which also owned regional branches;
- Keeping abreast of events organised by leading professionals, such as Phil Bradley and Paul Pedley, as well as organisations such as CILIP and the Carnegie Trust;
- Performing advanced Twitter searches using Boolean techniques to find real-time evidence of digital inclusion activities in UK libraries that focused on privacy.

Once the selection criteria and approaches were defined, it became possible to examine how they could be used to help develop relevant lines of enquiry and a case study structure to support the individual research objectives outlined in the introduction. These were summarised as follows:

A. What are the rationales for implementing digital privacy initiatives in public libraries?

[9] Whilst the LFP are a US organization, their following on social media include professionals and groups based in the UK.

B. Could other public libraries realistically work public awareness programs about digital privacy into their existing service strategies?

C. What risks or barriers are likely to be indicative of the sorts of problems public libraries in the UK face in terms of implementation?

D. Do such activities have the potential to be replicated on a wider scale?

In order to ensure that the research output was reliable however, the research objectives above, which explored broader theoretical questions about the state of digital privacy initiatives in the UK, needed to be recalibrated for the purposes of each case, to maximise objectivity and specificity where possible (Biggam, 2015, pp. 174-175). This would theoretically render the research output less reliant on the personal biases and conjectures of respondents whilst retaining the validity of in-depth, first-hand accounts that often shed light on these broader questions (Bell: 2005, p. 6; Biggam, 2015, p. 155).

Given the fairly novel nature of this research, it was essential to give the respondent the possibility to expand on questions relating to their initiatives without interposing unscripted questions that could unfairly influence their answers. A semi-structured interview (for e.g. in person or via Skype) is arguably more discursive and potentially risky. Therefore, a more rigid interview structure, using pre-arranged emailed questions was adopted to achieve balance (Biggam, 2015, pp. 174-176).

In summary, a hybrid approach was deemed desirable for the purposes of this research. This combined the positive attributes of personal interviews (the respondent is known, there is scope for open-ended questions and the possibility for factual as well as analytical responses) with those of written questions (that cannot be changed as per need and preference, as they are written in an appropriate sequence) (Surbhi, 2016).

The final draft of written questions put to the respondents who participated in this research, can be viewed in appendix A.

Framework for Data Analysis

Prior to describing the findings, it is relevant to comment briefly on the case study respondents and outline the process of collecting their responses. This is discussed in the next chapter and is necessary to contextualise the second stage of comprehensive analysis. It also provides opportunities to highlight unusual discrepancies or unexpected findings made in the data collection process which are then clarified later on. Respondents' answers to the questions submitted (see appendix A) are then grouped under the headings of the individual research objectives described in the methodology.

The figure below shows how questions were accommodated under the relevant theme and the manner in which they were to be analysed. Theme A, for example relates to the *specific* rationales of the libraries featured in the multiple case study and were not intended to make inferences about the attitudes or rationales of public libraries outside of this study. For this reason, a uniquely descriptive analysis was attributed, in contrast to areas which had the potential to be analysed more exploratively.

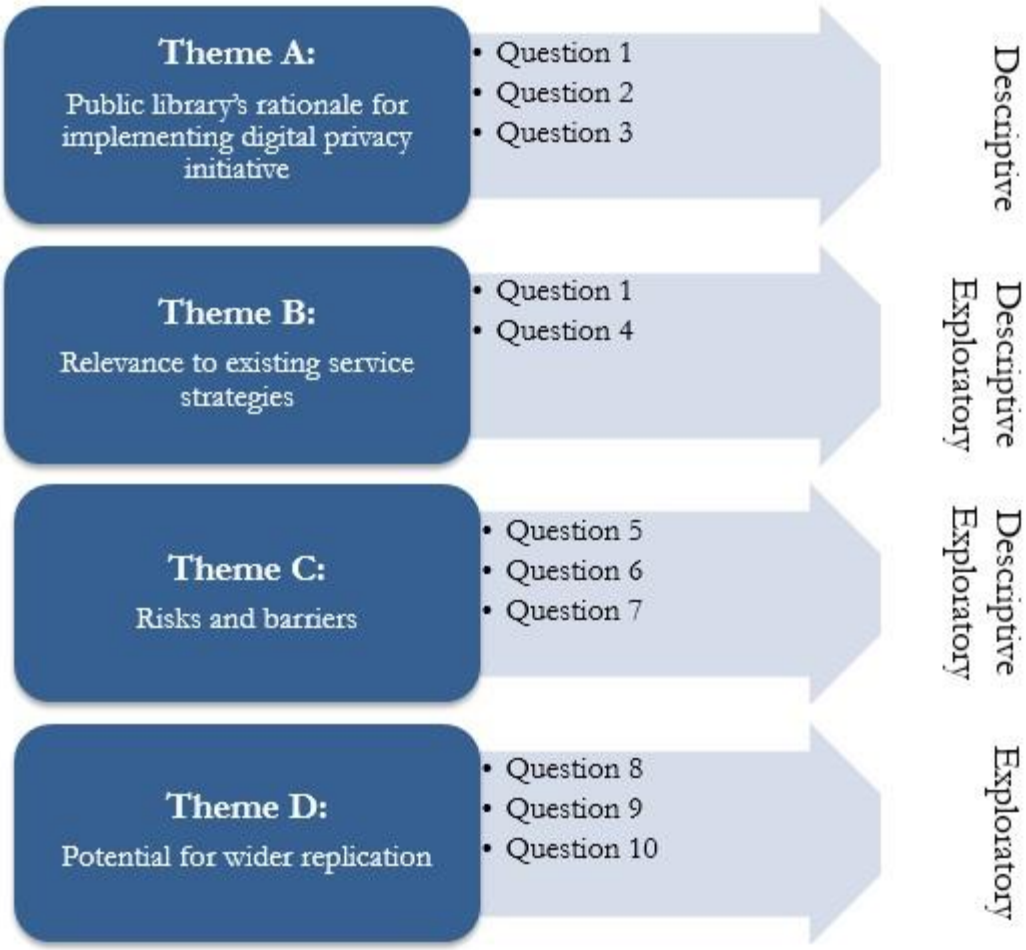

Figure 1. Thematic headings corresponding to the individual research objectives

This allowed for a more rigorous cross-referencing of data results whilst drawing on aspects of the literature review findings, such as legal and online definitions of privacy, which could have impacted on *rationale, existing policies, risks and barriers* as well as *wider replication* (Biggam, 2015, p. 193).

It is important therefore to see the thematic headings (above) and the key concepts of the literature review as interrelated as they were both crucial in addressing the overall research aim and individual objectives.

Two different analytical approaches were also undertaken (represented in the chart below) to indicate how far the empirical data should be interpreted when it came to addressing the individual research objectives. Again, both of these approaches could be seen as mutually supportive but were intended to act as an aid when it came to extrapolating the data.

Figure 2 shows a graphic interpretation of the framework which was used to unpack the empirical data from the case studies based around the dual process of summarising and analysing.

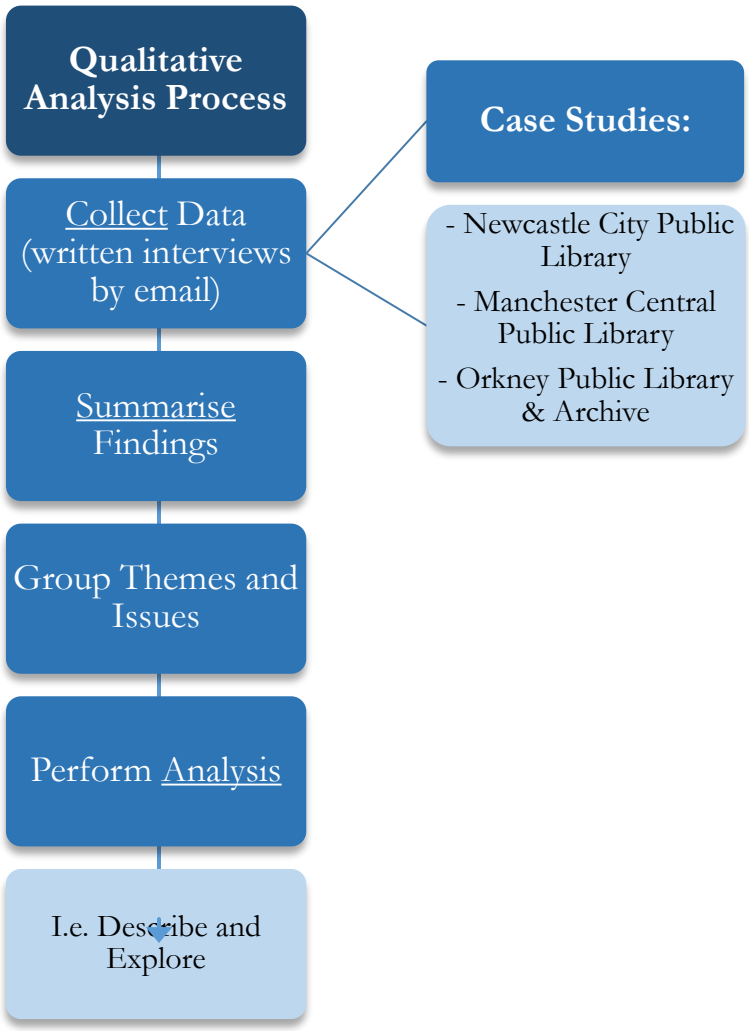

Figure 2. Qualitative data analysis process

Limitations and Potential Problems

The research faced several problems but not all of these were crucial to the validity of the findings. A main concern reverberated back to the overall research aim which asked: which public library services are involved in putting forward (or have previously implemented) online privacy initiatives in the UK? The literature review established that few efforts had been made to advance an understanding of this phenomenon. The lack of rich and substantive data, therefore, presented a significant challenge. On the other hand, obtaining even limited information represented progress.

In terms of the methodology, the choice to use written questions rather than conduct personal interviews (in person or via Skype) ran the risk of a low response rate due to the fact that respondents are typically deterred by the rigidity of pre-structured questions (Surbhi, 2016), in addition to what they often conceive to be 'too many questions' (Biggam, 2015, pp. 155, 176). Responding to open questions, which require a degree of depth was also potentially inhibitory in contrast with survey methods that simplify the process through multiple choice or yes/no responses (Biggam, 2015, pp.155, 162; Surbhi, 2016).

One of the significant risks of using open-ended written questions was the challenge it presented to respondents who might have had problems engaging with complex ideas or literacy. This had the potential to render the research invalid because such a barrier could have undermined the capacity for qualitative, in-depth responses as well as contravened the principles of equal opportunities (although a rudimentary pre-screening of candidates usually anticipates this).

Even if exceptional measures could have been taken to accommodate the responses by other means, such as by adopting a personal interview (oral) approach, this could equally have had ramifications for the way the data were collectively analysed. Personal interviews for instance 'are

usually more expansive than those obtained through other means' and sometimes result in case study results which appear incongruous or more unwieldy than others (Biggam, 2015, p. 154).

Open questions, whether they are written and submitted by email or posed face to face are particularly vulnerable to bias and social-environmental factors. Biggam (2015, p. 175-176) for instance says that 'respondents might be tempted to give you an 'answer' that either shows themselves in a good light or which they think will please you'. Both undermine data reliability.

Wiles (2013, p. 34) also cautions about the consequences of not being sufficiently forthcoming with respondents about research which requires their consent. This can result in situations where respondents commit to the initial terms of participation or even carry on through to the full cycle of the project only to backtrack because they were unaware of the way 'data would be recorded, how anonymity and confidentiality would be managed or how the study would be disseminated'.

Much research is likely to be hampered by one of more of the problems described above, any of which could compromise one's findings. In this instance, the major issues were the paucity of available UK data and the problem of recruiting appropriate and interested participants. Nevertheless, useful information was obtained – albeit on a limited scale – and the respondents also flagged up other individuals and further potential avenues of enquiry. This may help raise awareness of future possibilities.

Findings

Case Study Results

This section reveals the results of the multiple case study research in which written interview-style questions were sent to respondents representing three different public library services spread across the UK. As per the previous chapter on research methods, a qualitative approach was adopted in

order to gain a deeper understanding of the digital privacy initiatives being implemented and in doing so, establish a descriptive and exploratory framework for analysis.

Attention is given here to a 'first impressions' overview of the data and to how the choice of strategy impacted on key stages of the research.

The empirical research was carried out between June and July 2017 and identified three candidates who had been involved in delivering original digital privacy initiatives for the benefit of users in their libraries. They were: Sue Lawson, a Library Service Development Coordinator from Manchester Central Public Library, Aude Charillon, a Library and Information Officer from Newcastle City Public Library and Karen Walker, the Principal Librarian for Orkney Public Library and Archive (see appendix B for full details on the written questions and responses of participants).

Charillon's work - which was highlighted in the literature review chapter and is widely believed to be the first account of a public library in the UK to host a cryptoparty (a type of decentralised initiative aimed at teaching digital privacy principles and techniques to the general public) - was considered a logical point of departure for this research and so it was through her that initial enquiries were made. This successfully brought to the fore the work of Lawson in Manchester who, like Charillon, had been keen to explore partnerships with organisations such as the Open Rights Group (ORG) in order to deliver cryptoparties for the users in her library. Finally, Walker was contacted via the official Orkney Library and Archive website after it was discovered through Twitter that the Kirkwall branch had hosted a digital privacy and security workshop in partnership with Scottish PEN (see appendix C).

All respondents initially agreed to answer the questions submitted by email (see appendix A), however special arrangements via Skype were eventually agreed on in Charillon's case, to mitigate her limited availability as well as provide further clarification on the written questions where she felt it was

needed. Her responses were recorded and transcribed (and can be viewed in appendix B). This allowed her to elaborate on the questions but made her answers more discursive as a result. Conversely, Walker provided very cursory answers to the questions submitted, leaving several questions blank. It is not easy to determine from this whether further clarification was also needed in her case or whether the capacity to which she contributed to the initiative with Scottish PEN was simply more limited.

Although necessarily limited, the data obtained are nevertheless illuminating and shed light on issues pertinent to the overall aim of this research. In retrospect, an alternate method of data collection, such as using personal interviews via Skype, might have produced better qualitative responses (although it is hardly without its own problems, including risks of technical issues and a stronger vulnerability to bias, as the methodology indicates).

The responses first of all showed that each of the three libraries had collaborated with an outside organisation to offer cryptoparties amongst other digital privacy initiatives for the users of their libraries.

According to Charillon, Newcastle hosted two cryptoparty events in 2016 in association with the local branch of the ORG, an organisation which exists in the UK to preserve and promote rights in the digital age. Lawson, who references Charillon's work as 'a great template for UK libraries to follow', similarly organised a raft of events in early 2017, as part of her 'Get Smart Data Day' at Manchester Central Library which included an array of guest speakers as well as a cryptoparty coordinated by the Manchester branch of the ORG. According to Walker, a previous collaboration between Orkney libraries and the free speech non-profit Scottish PEN (referred to as the 'Many Voices' project), lead to further collaborative opportunities. In 2017, ta digital privacy workshop for the public at their Stromness branch as well as a staff-orientated workshop in Kirkwall.

Interestingly, the responses revealed that the initiatives implemented in all three libraries had to some degree been inspired by the activities of Alison Macrina and the Library Freedom Project in the US. In response to question 1 for example, Charillon says that 'the Library Freedom Project, […] is something that really blew my mind in a way and I thought, "Yes, we should really be doing these sort of things"'. Lawson also cites Macrina as a key influence, stating: 'I heard about Alison Macrae's [*sic*] work and read more when the Librarians Privacy Project won a Knight Foundation award'. Whilst a link between Orkney Libraries and the LFP is never made by Walker, a page on the Scottish PEN's website (referring to a workshop organised by Nik Williams, who Charillon incidentally alludes to in question 8) makes it clear that the workshops were developed under the auspices of the LFP (Scottish PEN, N.D.).

Exploratory Analysis of Empirical Data against Literature Review Findings

In this section, the empirical data is grouped under thematic headings in order to tackle the individual research objectives head on. Each theme examines the case study responses (see appendix B) and where relevant, refers more widely to the literature review to advance an integrative and exploratory analysis of the findings.

Rationale for implementing digital privacy initiative.

Throughout their responses, Charillon and Lawson talk freely about their personal and profession sensitivities to intellectual privacy issues, particularly at the level of library ethics. Where Charillon describes herself as a self-styled digital skills librarian, using the advantage of her position at Newcastle City Public Library to engage in digital training opportunities, Lawson is an 'early adopter' where the environment of Manchester Central Public Library provides ample opportunities to experiment with resources and implement initiatives of benefit to her users.

It is comparatively less easy to draw conclusions about Walker's motivations with regards to digital privacy. The partnership between the Orkney Public Library service and Scottish PEN for example predates the delivery of the digital privacy workshops and so it is entirely possible that the project evolved as part of a more congenial arrangement between the two organisations.

Walker makes clear, however, that the project was jointly organised and that 'Libraries for Privacy' workshops were aimed at library staff and the public. Although the precise nature of her role or views on the project are not made explicit, the partnership with the staunchly pro intellectual freedom and privacy non-profit, arguably reveals something about where the sympathies of the service as a whole, lie.

In response to question 3, which explores the intentions of the digital privacy initiative, Walker identifies improved 'user awareness' as the main goal of public engagement, stressing the importance of knowledge of particular browsers and the principle of strong passwords. Again, further details are lacking about the degree to which public libraries should facilitate such initiatives but the overall rationale appears to be that libraries have a duty of care to their users.

The sentiment is shared by Charillon and Lawson who library staff have ethical responsibilities to assist users to make informed choices about their online experiences. According to Charillon this requires 'giving them the whole spectrum of information available'. This is deftly evidenced in Lawson's work where her concerns about e-book vendors spying on users' reading habits inspired her to share tips on how to remove DRM with library users at MCPL.

Such arguments give new meaning to the term digital inclusion, by incorporating what many may perceive to be the more 'fringe' aspects of online learning but which are, for all intents and purposes, no less important 'as markers of a digitally integrated life' (Gangadharan: 2012). This is

reflected in Lawson's rationale to 'put open data and online privacy on the public library agenda' in order to highlight the various ways that residents could protect their privacy and encourage such practices to become more widely accepted.

Cryptoparties also presented opportunities for NCPL to meet specific user demands about digital privacy. This appealed to Charillon, particularly as they took place in an ethically principled non-commercial atmosphere allowing her to earn the trust of library newcomers which may have proved harder to do otherwise. As a librarian and a 'trusted person' with responsibilities 'to facilitate access to information' and learning, Charillon was ideally positioned to recognise the value of the initiatives she organised and this comes across in her rationale.

Relevance to existing service strategies.

When asked whether the digital privacy initiatives entered into the scope of the libraries' key service objectives, responses were somewhat guarded. Walker for example does not answer the question directly but implies in another area that the 'Libraries for Privacy' workshops with Scottish PEN were consistent with their other practices including encouraging 'all library users to log out of anything they may log on to using our Public PCs as they are shared machines'. A specific impetus behind OPLA's collaboration (as discussed in the findings) is not evident, other than as an opportunity for continued engagement with local groups.

Lawson says that the 'Get Smart Data Day' initiatives did not reflect strategic service objectives at MCPL but that they had been signed off as positive developments by her manager and head of service whom were sympathetic to arguments about online privacy. Rather than shoehorning the initiatives into pre-existing schemes, Lawson justified the projects by drawing attention to intellectual privacy as a kind of trademark of library ethics that could be freed up and shared more openly with the public.

This is consistent with other transferals of cultural practice within librarianship where skills that were once considered the preserve of information professions - such as searches using indices, encyclopaedias and directories - have been gradually passed on to the layperson in the form of information literacy (Feather, 2008, p. 185). As with critical approaches to online search and retrieval, privacy-enhancing techniques have long been evidenced in librarians' use of technologies (Carnegie Trust, 2017), making them in some ways the ideal purveyors of digital privacy skills. This point is echoed by Charillon (2016b) who says 'I feel that teaching library users how to protect their privacy and providing them with the tools to do so is simply the next step for improving digital skills, and it fits with our role as librarians'.

Lawson was however concerned that 'there might be a kneejerk reaction to holding a Cryptoparty' and describes how she 'combined the open data sessions and online privacy sessions into one event - so it sounded less 'radical''.

This contrasts starkly with the tone of events in the US, where the ALA professional body lends legitimacy to bold initiatives such as 'Let's Encrypt' as well as 'Choose Privacy Week', a 'week-long event that promotes the importance of individual privacy rights' and 'celebrates librarians' unique role in protecting privacy in the library and in society as a whole' (ALA, 2016; Caldwell-Stone 2015).

Even if US libraries are not superintended to the same extent by the federal government compared with the UK (Clark, 2016, p. 19), professional bodies such as CILIP could use their reputation to advance privacy campaigns (similar to 'Facts Matter'). These might give more agency and much needed validity to the work of individuals in local authority libraries where digital privacy may be considered counter-cultural or a low strategic priority.

It is unclear whether Lawson had also considered framing her initiatives as digital inclusion projects, particularly given the ways in which digital inclusion has become standardised over the last few years. **(Wilson, 2016).** By making the 'Get Smart Data day' an independent project and by speaking about its successes afterwards, Lawson clearly attempts to set a new agenda for public libraries rather than retrofit digital privacy into older library programmes.

Charillon's first cryptoparty at NCPL, which was looked at briefly in the literature review, is framed as a personal venture. She reminds us that she organised it outside of working hours, as a member of the ORG and not strictly in her capacity as a librarian observing key service objectives (Charillon, 2016b). Had she been challenged, she concedes that her response would have been more formal ('"It is a new path to explore future digital skills activities"').

These two positions reveal the extent to which worthwhile initiatives often rely on the reputation of 'early adopters' with strong community ties, to influence higher levels of decision-making, rather than the reverse.

The second cryptoparty is a case in point where Charillon describes it as 'more open in [that] Newcastle Libraries supported [it], and I did the second one [in] my work time'. She is also much clearer about her rationale to incorporate key characteristics of the cryptoparties into the library's existing digital inclusion activities. Interestingly, the events succeeded in responding to key service objectives in a way that had not been anticipated. Charillon for example says that the cryptoparties attracted 'slightly different audiences to the library' who came away with a possibly changed perception of the service.

Lawson, Charillon and Walker additionally succeeded in building mutually supportive relationships with local partners such as Scottish PEN and the ORG whose ethics were arguably more aligned than those of the commercial third parties observed by Clark (2016, p. 17) in the literature review.

Risks and barriers.

In the absence of long-term service strategies that acknowledge privacy (as discussed above), support and open dialogue between lower tier staff and middle management has proved desirable and arguably essential to overcoming the potential pitfalls and barriers of organising digital privacy initiatives in public libraries.

Charillon and Lawson highlight the support they received from their managers, who on both accounts were sympathetic to privacy issues. Lawson also acknowledges that she works in a fairly 'progressive environment' and shares Clark's (2016, p. 19) ambivalence about the capacity for all public library authorities to reproduce such initiatives.

Working in 'a large city centre library with Wi-Fi and a good number of laptops to loan [and] a large meeting space' for example are not universal across libraries weathering a tough economic climate (Rust, 2014).

Similar advantages apply for Charillon who works in a large library with access to event rooms free of charge. She remarks that it would be difficult to run similar initiatives in smaller branches (even within Newcastle) because of the attendant problems such as shorter opening times.

As far as the data shows, this does not appear to have been the case with OPLA whose Stromness branch is open part time and serves a far smaller population. Walker does not mention any risks or barriers and says that 'planning was fairly straightforward – Scottish PEN and our media sites were used'.

Future potential barriers for MCPL, according to Lawson, could relate to the venue space itself, which is often in extremely high demand and usually only available to hire at a cost. Many of Lawson's guest speakers were also paid which again potentially limits the scope for events at smaller or more rural

libraries (ibid.). In the lead up to the 'Get Smart Data day' Lawson is forthcoming about her awareness of the risks:

> I was concerned about the potential for misunderstanding or linking learning about Tor to the Dark net or encryption to terrorism or hacking. I was worried that a member of the public may complain to a councillor and they might make the wrong assumptions. If a councillor complains, senior council officers tend to acquiesce.

Charillon agrees that councils often come across as 'very risk-averse' but says that the cryptoparties at NCPL 'just weren't high-profile enough to attract that kind of comment'.

An interesting dilemma that Charillon touches on however relates to the reputation of the public library as a 'neutral space' **(Peachey, 2017: 5)** and the potential for digital privacy initiatives to undermine this position, particularly if they are perceived to be 'pushing back against current legislation'.

In the US, similar challenges were levelled against the Kilton public library which installed a Tor exit relay causing traffic from around the network to be linked to the library's IP address. Despite pressure from the Department of Home Security (DHS), the local board voted unanimously to keep the exit node turned on and a law was subsequently passed in New Hampshire to protect future decisions of this kind (Glaser and Macrina: 2015; O'Neill, 2016).

Unlike the US where the first amendment enjoys unusual protections (Richards, 2015, p. 10) and a coordinated effort to oppose Section 215 of the Patriot Act (known as the 'library provision') was successfully overseen (ALA, 2017), UK privacy legislation has comparatively less clout. Uncertainty abounds about how similar ventures would fare in light of the IPA and counter terrorist strategies such as Prevent, which also apply to public libraries (CILIP, 2012, pp. 1-4).

Although Charillon does not currently envisage introducing Tor relays to NCPL, it is not an initiative that she thinks should be ruled out by 'forward-thinking' public libraries in the UK **(Charillon:**

2016b). She also believes that misunderstandings can be avoided by taking steps to be as transparent about the practices of the library, wherever possible.

Lawson says that an important way to mitigate risks of grievance is 'to be prepared for any questions or challenges before you embark on any similar activities'. This is again reinforced by Charillon who highlights the counter argument to public library neutrality claims, emphasising that '[l]ibraries *have* to take a stand for privacy *in order* to stay neutral'.

Technical issues are described by Charillon and Lawson as factors which are not inherently risky but which require forethought and planning.

At MCPL for example the Wi-Fi didn't support tools such as the Tor browser because of the way it had been systematically configured to block VPNs and proxies. Web filtering, which is common to public libraries (Payne, 2016), is also identified as a barrier to demonstrating certain tools. Charillon says that NCPL was fortunate in that it had comparatively less restrictions in this regard, allowing participants to connect to the Wi-Fi and download the Tor browser bundle without issue.

She continues to stress that the initiatives she helped to run were highly approachable, partly due to the low-risk nature of the activities which presented no legal barriers and partly because they were consistent with other learning initiatives they had implemented (as discussed above with digital inclusion schemes).

Nevertheless, two library services in England had, according to Charillon, declined to offer cryptoparties when they were approached, citing financial woes and general impracticality as service barriers.

Potential for wider replication.

In spite of the barriers and risks associated with organising digital privacy initiatives, the three public libraries which form this multiple case study, have either discussed plans to implement digital privacy initiatives in the near future or have links with organisations who are preparing to expand their projects further across libraries in the UK.

Lawson for example says that MCPL is 'planning another event for the autumn' and Charillon says that a third cryptoparty is anticipated at NCPL later in the year. Whilst OPLA have currently no further plans to run 'Libraries for Privacy workshops', their partners, Scottish PEN have embarked on a wider campaign. This will provide initiatives for public and academic library staff (including I.T. personnel) across Scotland, including the Glasgow Women's Library, the Edinburgh Central library and the AK Bell public library in Perth (Williams, 2016; Scottish PEN, N.D.).

The proclivity for replication, according to Lawson and Charillon, relies a great deal on such training schemes being made available to front-line staff as well as building rapport with I.T departments (as alluded in the findings section) to find common ground. Such efforts appear to underpin behind the majority of Scottish PEN's workshops, which, as noted in the chapter on findings, have been modelled on the tried and tested training strategies of the Library Freedom Project in the US.

The LFP has additionally called attention to the dynamism that can result from engaged members of staff who are also prepared to provide in-house expertise for projects requiring a degree of systems knowledge. In the case of Kilton public library in New Hampshire, Internet Librarian Chuck McAndrew was able to run all of the computers on the network using GNU/Linux distributions as well as assist in the installation of a Tor relay (McAndrew, 2015). Involvement at this level has the added value

of understanding the practicability of certain initiatives (prior to implementation) based on general familiarity with the library's network setup and in turn, cut down on costs (McAndrew & Macrina, 2015).

The cross-pollination of initiatives we are beginning to see may be further aided by the arrival of new legislation in the UK such as the General Data Protection Regulation (GDPR). Where deficient laws as we have seen in the literature review, have to some extent enabled corporate surveillance and profiling in particular, to flourish (ICO, 2017a:, pp. 3-6; Pedley, 2017a), the GDPR, as Charillon points out, could persuade many organisations including public library authorities to review their policies on privacy and transparency and in doing so, invite a culture which is more tolerant towards the use of privacy-enhancing technology. The GDPR, which comes into force in May 2018, could also be incorporated into digital inclusion courses such as 'Learn My Way' (which have previously offered primers on the DPA and the FOIA (Learn My Way, 2017)) and in doing so provide a natural springboard for online intellectual privacy activities. This is acknowledged in Charillon's action points where she plans to consolidate the latter into the curriculum for her 'Silver Surfers' group.

Lawson similarly reflects on the potential for online privacy to be incorporated into the SCL's 'Digital Offer', a component of six key areas of concern to public library services including health, reading and culture (Drakard, 2016). These are used to provide targeted training to the library workforce, again making it clear that good practice can be cascaded to staff in order to help forge stronger relationships between intellectual privacy and library ethics.

Elevating intellectual privacy to the level of professional awareness as seen through schemes such as 'Choose Privacy Week' in the US (ALA, 2016), is clearly another important step to supporting dynamic initiatives.

In terms of practicality, Charillon and Lawson suggest that large flagship libraries are better suited to accommodate initiatives such as cryptoparties but Walker indicates that even comparatively smaller, part-time branches such as Stromness can support small-scale initiatives, using PowerPoint presentations that encourage audience participation.

The use of creative commons leaflets to disseminate information on privacy tools (a method used by organisers of the first NCPL cryptoparty) is another effective contingency for smaller libraries and communities who may lack the means to demonstrate certain tools or relay information that is relatively diffuse in nature.

Public libraries could also include input from law professionals or paralegals (another type of 'trusted person') to quell any public concerns and provide further clarification on the legal implications of certain technologies. This format was adopted in Alison Macrina's earlier work with Kade Crockford from the Massachusetts branch of the ACLU (Macrina, 2014b; Macrina, 2015b) as well as Charillon's work with Northumbria law graduate, Alex Haydock (Haydock, 2016).

English PEN, Scottish PEN, Liberty and the ORG (which have several regional branches across the country) are all examples of organisations that can offer human rights perspectives on digital privacy and may be open to collaborating on related initiatives with public libraries.

Failing that, public libraries could simply host informal debates on intellectual privacy issues in the interests of their local communities. Involving the community from the start was a lesson which had been underappreciated by McAndrew after Kilton residents rallied to support the reinstatement of the Tor relay which had been temporarily disabled following interventions by the DHS (McAndrew & Macrina, 2016).

Conclusions

Summary of Findings and Resulting Conclusions

The overall aim of this research was to advance an understanding of digital privacy initiatives being implemented in public libraries, particularly in relation to the UK where research is underdeveloped for a number of reasons.

Firstly, the literature showed that whilst privacy is primarily defined through social norms and principles which are enshrined in UK law, privacy itself is not strongly supported in practice. Furthermore it revealed that the most important decisions regarding digital privacy are unlikely to be resolved through legislation alone.

Secondly, the capacity for every Internet user to have digital privacy relies on overcoming many of the same challenges raised by digital inclusion provision. These include *access* (to unmonitored services and technology), *skills* (relating to information security), *motivation* (knowing why digital privacy is valuable) and *trust* (knowing how to determine reliability of online contacts and services). The literature reveals that some government and private sector-lead schemes offer few assurances in this regard and prepare users for worlds where cyber criminals represent the only conceivable threats to their wellbeing.

Public librarians have passed many of the skills that were once considered unique to their profession on to the communities they serve. Being guided by ethical stewardship of information rather than shareholder values also makes them trusted intermediaries. The literature indicates that public librarians in the US are well-versed in intellectual privacy issues and are ideally placed to provide privacy skills training for many of the reasons described above.

Although limited, the empirical research suggests that public libraries in the UK have a strong case for engaging in digital privacy initiatives. Current knowledge shows that there is no official mandate to provide such skills but that digital privacy training for the public is consistent with many existing programmes and reflects the natural progression of library practice and ethics. Risks and barriers are part and parcel of any new proposed initiative and parallels with digital inclusion activities should not be viewed as panaceas. Interestingly many of the perceived risks, such as complaints or challenges from the council or press (even domestic security), relate back to poor public understanding around digital privacy which some may argue does more to support such initiatives than it does to ultimately deter them. Few of the risks or barriers identified in the case studies are described as insuperable however. In spite of a wide range of potential issues, evidence from the literature and the case studies suggests that an equally wide number of solutions are exploitable depending on the means of the library and the scale of the project.

Recommendations

This study has identified three potentially influential public libraries delivering digital privacy initiatives in the UK. Providing that similar initiatives become more widely accepted in the future (as this research anticipates), particularly with the introduction of GDPR legislation, quantitative research concerned with the impacts of specific digital privacy projects within public libraries could represent the next logical step for a UK-wide study.

Community feedback to library-lead privacy workshops, in the form of surveys for example, could be used to extrapolate valuable data used to incentivise policy-makers and major public library stakeholders to take more action. One possibility is to focus on organisations such as Scottish PEN who

provide skills training in different areas of Scotland and were identified in the practical research as a potential successor to the Library Freedom Project in the UK.

Increased participation in such programmes on the part of public libraries in the UK, could additionally increase the scope of cross-cultural research between the US and the UK but also other countries around the globe.

References

Acquisti, A., & Grossklags, J. (2006). What Can Behavioral Economics Teach Us About Privacy? Retrieved 29 March 2017, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.442.2852&rep=rep1&type=pdf

American Library Association. (2006, July 7). Privacy [Text]. Retrieved 19 August 2016, from http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy

American Library Association. (2016, March 21). Choose Privacy Week 2016: Raising Privacy Awareness in Your Library and in Your Community [Text]. Retrieved 20 August 2017, from http://www.ala.org/advocacy/intfreedom/webinar/privacy2016

American Library Association. (2017, December 29). USA PATRIOT Act [Text]. Retrieved 22 August 2017, from http://www.ala.org/advocacy/advleg/federallegislation/theusapatriotact

Associated Press. (2016, June 26). Browse free or die? New Hampshire library is at privacy fore. *Daily Mail Online*. Retrieved 14 August 2017, from http://www.dailymail.co.uk/wires/ap/article-3660721/Browse-free-die-New-Hampshire-library-privacy-fore.html

Astor, M. (2017, July 25). Your Roomba May Be Mapping Your Home, Collecting Data That Could Be Shared. *The New York Times*. Retrieved from https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html

Barron, S., Regnault, C., & Sanders, K. (2017). Library Privacy. *NY Delegate Pack: Reading Materials*, 22–24.

Bell, J. (2005). *Doing Your Research Project: A Guide for First-Time Researchers in Education, Health and Social Science*. Maidenhead: Open University Press.

Bercovici, J. (n.d.). What Mark Zuckerberg Doesn't Get About Facebook | Inc.com. Retrieved 16 November 2016, from https://www.inc.com/jeff-bercovici/mark-zuckerberg-denial.html

Berman, E., & Worona, J. (2016, January 4). California Library Creates Online Privacy Tool. Retrieved 9 April 2017, from https://americanlibrariesmagazine.org/2016/01/04/library-creates-online-privacy-tool/

Biggam, J. (2015). *Succeeding with your Master's Dissertation* (3rd ed.). Maidenhead: Open University Press.

Bradley, P. (2016, March 7). UK Government Spying law moves forward. Retrieved 15 March 2017, from http://philbradley.typepad.com/phil_bradleys_weblog/2016/03/uk-government-spying-law-moves-forward.html

Burgess, M. (2017, July 25). The Internet of Things is a data farm, Roomba won't be its only profiteer. Retrieved 26 July 2017, from http://www.wired.co.uk/article/roomba-data-sell-internet-of-things

Busby, M. (2017, August 31). Revealed: how gambling industry targets poor people and ex-gamblers. Retrieved 31 August 2017, from http://www.theguardian.com/society/2017/aug/31/gambling-industry-third-party-companies-online-casinos

Cabinet Office. (2014). Government Digital Inclusion Strategy - GOV.UK. Retrieved 18 July 2016, from https://www.gov.uk/government/publications/government-digital-inclusion-strategy/government-digital-inclusion-strategy#challenges

Caldwell-Stone, D. (2015, December 29). Encryption and Patron Privacy [Text]. Retrieved 20 August 2017, from http://www.ala.org/advocacy/privacy/encryption

Carnegie Trust. (2017, May 10). Privacy in a Digital Age - Carnegie UK Trust Seminar on Future of Public Libraries | Carnegie Council for Ethics in International Affairs. Retrieved 14 June 2017, from https://www.carnegiecouncil.org/studio/multimedia/20170510-privacy-in-a-digital-age

Chakrabarti, S. (2014). *On Liberty*. London: Allen Lane.

Charillon, A. (2016a, March 18). Excited that we have a firm plan to organise a cryptoparty in Newcastle in May, with ORG North East + hosted by Newcastle Libraries! [Tweet]. Retrieved 23 May 2016, from https://twitter.com/Audesome/status/710778831720808449

Charillon, A. (2016b, June 13). CryptoParty Newcastle and user privacy in libraries - informed. Retrieved 15 May 2017, from http://theinformed.org.uk/2016/06/cryptoparty/

Chesha, C. (2014). Blog posts for cristian-chesha from manchester-open-rights-group-meetup-24-feb-2014 | The Pirate Party. Retrieved 19 February 2015, from https://www.pirateparty.org.uk/blogs/cristian-chesha/manchester-open-rights-group-meetup-24-feb-2014

Cheshire, T. (2017, August 7). How much dirt do social networks have on you? Retrieved 8 August 2017, from https://news.sky.com/story/how-much-dirt-do-social-networks-have-on-you-10977974

CILIP. (2012). The Prevent Strategy: What it means for library and information professionals. Retrieved 2 April 2017, from

https://archive.cilip.org.uk/sites/default/files/documents/Prevent%20strategy%20briefing%20Jan%202012.pdf

CILIP. (2014). Digital Inclusion. Retrieved 22 May 2016, from https://www.cilip.org.uk/advocacy-campaigns-awards/advocacy-campaigns/electionwatch-2015/digital-inclusion

CILIP. (2015). Libraries and privacy in the digital age. Retrieved 14 March 2015, from http://www.cilip.org.uk/events/libraries-privacy-digital-age

CILIP. (2017). Existing ethical framework. Retrieved 14 June 2017, from https://www.cilip.org.uk/research/topics/ethics-review/existing-ethical-framework

CIPFA. (2012). Library Stats, UK, 11/12. Retrieved 15 May 2016, from https://docs.google.com/spreadsheets/d/1b7xaami4N_6VBNsfcoFzW9r9-35epsbc5sPHl7Eiw6Q/edit?usp=embed_facebook

Clark, I. (2016). The digital divide in the post-Snowden era. *Journal of Radical Librarianship*, *2*. Retrieved from https://journal.radicallibrarianship.org/index.php/journal/article/view/12

Clark, L. (2014, October 13). Adobe responds to ALA on egregious data breach; some action expected by week of Oct. 20 [Text]. https://doi.org/http://www.ala.org/news/press-releases/2014/10/adobe-responds-ala-egregious-data-breach-some-action-expected-week-oct-20

Communications Market, The. (2016, September 30). The Communications Market Report 2015. Retrieved 26 October 2016, from https://www.ofcom.org.uk/research-and-data/multi-sector-research/cmr/cmr15

Conservative and Unionst Party, The. (2017). The Conservative Party Manifesto 2017. Retrieved 17 June 2017, from https://www.conservatives.com/manifesto

Cryptoparty. (n.d.). guiding_principles [CryptoParty.]. Retrieved 10 January 2015, from https://www.cryptoparty.in/guiding_principles

Department for Business, Innovation & Skills. (2012, December). The 2011 Skills for Life Survey: A Survey of Literacy, Numeracy and ICT Levels in England. Retrieved 19 January 2016, from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/36000/12-p168-2011-skills-for-life-survey.pdf

DiMaggio, P., Hargittai, E., Celeste, C., & Shafter, S. (2004). Social Inequality. In *Digital Inequality: From unequal access to differentiated use: a literature review and agenda for research on digital equality* (pp. 355–400). New York: Russell Sage Foundation.

DiMaggio, P., Hargittai, E., Neuman, W. R., & Robinson, J. P. (2001). Social Implications of the Internet. *Annual Review of Sociology*, *27*(1), 307–336. https://doi.org/10.1146/annurev.soc.27.1.307

Dobbs, A. (2014, October 13). ADE in the Library eBook Data Lifecycle – LITA Blog. Retrieved 13 August 2017, from http://litablog.org/2014/10/ade-in-the-library-ebook-data-lifecycle /

Drakard, H. (2016). Workforce Development E-learning Modules. Retrieved 27 August 2017, from http://goscl.com/training/

DuckDuckGo. (2017, March 24). Keep your personal data private with these privacy tips for Android. Retrieved 24 April 2017, from https://spreadprivacy.com/android-privacy-tips/

Eagle, S. C., St. Hilaire, A., & Sherwood, K. (2013). *Tor Exit Nodes Legal and Policy Considerations* (The Technology Law and Public Policy Clinic). University of Washington School of Law. Retrieved from https://www.law.uw.edu/academics/experiential-learning/clinics/technology-law/

Electronic Frontier Foundation, The. (2014, September 13). Want a security starter pack? Retrieved 9 May 2016, from https://ssd.eff.org/en/playlist/want-security-starter-pack

Fatemi, N. (2015, July 28). Tor Exit Nodes in Libraries - Pilot (phase one) | Tor Blog. Retrieved 19 August 2016, from https://blog.torproject.org/tor-exit-nodes-libraries-pilot-phase-one

Feather, J. (2008). *The Information Society: A study of continuity and change* (5th ed.). London: Facet.

Gangadharan, S. P. (2012). Digital inclusion and data profiling. *First Monday*, *17*(5). https://doi.org/10.5210/fm.v17i5.3821

Get Safe Online. (N.D.). Privacy. Retrieved 12 June 2015, from https://www.getsafeonline.org/protecting-yourself/privacy/

Glaser, A., Macrina, A., & Shamas, N. (2015, September 16). How a Small New Hampshire Library Fought Government Fearmongering. *Slate*. Retrieved from http://www.slate.com/blogs/future_tense/2015/09/16/how_new_hampshire_s_lebanon_libraries_fought_back_against_dhs_fearmongering.html

Goetzmann, J.-F. (2016, October 6). The German approach to privacy in technology: Datensparsamkeit. Retrieved 12 August 2017, from https://medium.com/@jefago/the-german-approach-to-privacy-in-technology-datensparsamkeit-393d2514c04d

Goldacre, B. (2017, May 13). XP isn't the only version of Windows hit by this attack but this decision surely worsened the odds for the NHS. https://twitter.com/VegSoft/status/863300755813478401 … [Tweet]. Retrieved 13 May 2017, from https://twitter.com/bengoldacre/status/863301880864178176

GOV.UK. (n.d.). Digital Service Standard - Service Manual - GOV.UK. Retrieved 16 May 2016, from https://www.gov.uk/service-manual/service-standard

Green Party, The. (2015). For the Common Good: Full 2015 General Election Manifesto. Retrieved 16 March 2017, from

https://www.greenparty.org.uk/assets/files/manifesto/Green_Party_2015_General_Election_Manifesto_Searchable.pdf

Greenberg, A. (2015, September 14). Mapping How Tor's Anonymity Network Spread Around the World. Retrieved 22 May 2016, from https://www.wired.com/2015/09/mapping-tors-anonymity-network-spread-around-world/

Greenberg, A. (2016, January 17). Here's What Tor's Data Looks Like as It Flows Around the World. Retrieved 22 May 2017, from https://www.wired.com/2016/01/heres-what-tors-data-looks-like-as-it-flows-around-the-world/

Greene, J. K. (2014). Before Snowden: privacy in an earlier digital age. *International Journal of Philosophy and Theology*, *2*(1).

Griffin, A. (2015, May 21). Most people just write rubbish in online forms, because they hate companies so much. Retrieved 22 May 2016, from http://www.independent.co.uk/life-style/gadgets-and-tech/news/most-people-lie-in-online-forms-because-they-dont-trust-companies-study-finds-10267687.html

Hargittai, E. (2002). Second-Level Digital Divide: Differences in People's Online Skills. *First Monday*, *7*(4). https://doi.org/10.5210/fm.v7i4.942

Harris, T. (2016, May 19). How Technology Hijacks People's Minds—from a Magician and Google's Design Ethicist – Tristan Harris. Retrieved 20 July 2016, from http://www.tristanharris.com/2016/05/how-technology-hijacks-peoples-minds%e2%80%8a-%e2%80%8afrom-a-magician-and-googles-design-ethicist/

Haydock, A. (2016, May 30). What we learned from hosting our CryptoParty. Retrieved 26 July 2016, from https://medium.com/@alexhaydock/what-we-learned-from-hosting-our-cryptoparty-3950c9721f3e

Horrigan, J. B. (2016, September 9). Libraries 2016. Retrieved 13 August 2017, from http://www.pewinternet.org/2016/09/09/libraries-2016/

IBM. (2015). IBM Finds More Attacks Originating from the TOR Network. Retrieved 20 July 2016, from http://i1-news.softpedia-static.com/images/news2/ibm-finds-more-and-more-attacks-originating-from-the-tor-network-490041-2.jpg

IFLA. (2013). *Riding the Waves or Caught in the Tide? Navigating the Evolving Information Environment: Insights from the IFLA Trend Report*. Retrieved from https://trends.ifla.org/files/trends/assets/insights-from-the-ifla-trend-report_v3.pdf

Information Commissioner's Office. (2017a). Feedback request – profiling and automated decision-making. Retrieved 30 April 2017, from https://ico.org.uk/media/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf

Information Commissioner's Office. (2017b). Guide to the General Data Protection Regulation (GDPR). Retrieved 27 May 2017, from https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Kelion, L. (2017, March 27). WhatsApp's privacy protections questioned after terror attack - BBC News. Retrieved 28 March 2017, from http://www.bbc.co.uk/news/technology-39405178

King, E., & Lock, D. (2016, December 1). Eric King and Daniella Lock: Investigatory Powers Bill: Key Changes Made by the Lords. Retrieved 16 March 2017, from

https://ukconstitutionallaw.org/2016/12/01/eric-king-and-daniella-lock-investigatory-powers-bill-key-changes-made-by-the-lords/

Koebler, J. (2015, September 17). A Dozen Libraries Want to Host Tor Nodes to Protest Government Fearmongering. Retrieved 23 May 2017, from https://motherboard.vice.com/en_us/article/539np8/a-dozen-libraries-want-to-host-tor-nodes-to-protest-government-fearmongering

Kovacs, E. (2015, August 25). Tor Increasingly Used by Malicious Actors: IBM | SecurityWeek.Com. Retrieved 28 March 2017, from https://www.securityweek.com/tor-increasingly-used-malicious-actors-ibm

Lamana, T. J. (2016, June 26). We keep talking about how libraries are heralds of privacy, but we are TERRIBLE AT IT. #alaac16 #alattt [Tweet]. Retrieved 12 May 2017, from https://twitter.com/paraVestibulum/status/747116391505879040

Law Teacher. (N.D.). Invasion of Privacy is not an acknowledged Tort in the UK. Retrieved 14 May 2016, from https://www.lawteacher.net/free-law-essays/constitutional-law/invasion-of-privacy-is-not-law-essays.php

Learn My Way. (2017). Subjects | Learn My Way. Retrieved 11 June 2017, from https://www.learnmyway.com/subjects

legislation.gov.uk. (n.d.). Human Rights Act 1998 [Text]. Retrieved 27 November 2014, from http://www.legislation.gov.uk/ukpga/1998/42/contents

LFP. (2016, October 25). taught a great privacy class this evening at the lovely Stowe Free Library in Vermontpic.twitter.com/IBNkOvPyC7 [Tweet]. Retrieved 23 May 2016, from https://twitter.com/libraryfreedom/status/790712032785989632

Liberty. (2010, August 31). Article 8 Right to a private and family life [Text]. Retrieved 5 May 2016, from https://www.liberty-human-rights.org.uk/human-rights/what-are-human-rights/human-rights-act/article-8-right-private-and-family-life

LILRC. (2016, April 18). Recap & Resources from Privacy Toolkit for Librarians Workshop. Retrieved 23 May 2017, from https://lilrcevents.org/2016/04/18/lfp/

Lomas, N. (2017, June 5). We want to limit use of e2e encryption, confirms UK minister | TechCrunch. Retrieved 6 June 2017, from https://techcrunch.com/2017/06/05/we-want-to-limit-use-of-e2e-encryption-confirms-uk-minister/

MacAskill, E., Borger, J., Hopkins, N., Davies, N., & Ball, J. (2013, June 21). GCHQ taps fibre-optic cables for secret access to world's communications. Retrieved 2 June 2016, from http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

Macrina, A. (2014a). Libraries at the forefront of the digital privacy movement. Retrieved 19 May 2015, from http://www.cilip.org.uk/blog/libraries-forefront-digital-privacy-movement

Macrina, A. (2014b, September 19). Helloooo Massachusetts librarians, I'll be teaching a privacy workshop w/ @onekade at the Milton Public Library, September 24th at 1 pm. [Tweet]. Retrieved 23 June 2016, from https://twitter.com/flexlibris/status/512989765260824576

Macrina, A. (2014c, November 6). Just had one of the best privacy workshops we've ever taught at Medway Public Library. Super engaged group who asked amazing questions. [Tweet]. Retrieved 23 June 2016, from https://twitter.com/flexlibris/status/530484614071328770

Macrina, A. (2015a, September 30). Tomorrow I'm doing a privacy class for teens at Portland Public Library in Maine and bringing a stack of these jointspic.twitter.com/998qJ5C7KC [Tweet]. Retrieved 23 June 2016, from https://twitter.com/flexlibris/status/649030645239390209

Macrina, A. (2015b, October 29). Today @onekade and I did a training at the Barrington Public Library in Rhode Island. Before my talk, one of the librarians came up to me... [Tweet]. Retrieved 19 May 2015, from https://twitter.com/flexlibris/status/659784056150884352

Macrina, A., & Fatemi, N. (2015, July 28). Tor exit relays in libraries: a new LFP project – Library Freedom Project. Retrieved 15 August 2017, from https://libraryfreedomproject.org/torexitpilotphase1/

Macrina, A., & Glaser, A. (2014, September 13). Radical Librarianship: how ninja librarians are ensuring patrons' electronic privacy / Boing Boing. Retrieved 1 October 2014, from https://boingboing.net/2014/09/13/radical-librarianship-how-nin.html

Mai, J.-E. (2016). Big data privacy: The datafication of personal information. *The Information Society*, *32*(3), 192–199. https://doi.org/10.1080/01972243.2016.1153010

Markesinis, B., O'Cinneide, C., Fedtke, J., & Hunter-Henin, M. (2004). Concerns and ideas about the developing English law of privacy (and how knowledge of foreign law might be of help). *AM J COMP LAW*, *52*(1), 133–208. Retrieved from http://discovery.ucl.ac.uk/184252/

McAndrew, C. (2015, August 14). Guest post: How I set up GNU/Linux at my library – Library Freedom Project. Retrieved 14 July 2017, from https://libraryfreedomproject.org/gnulinuxinthelibrary/

McAndrew, C., & Macrina, A. (2015, December 1). Wrapping up our Tor exits pilot, and what's next for this initiative – Library Freedom Project. Retrieved 17 August 2017, from https://libraryfreedomproject.org/torexitspilotwrapup/

McCandless, D. (2017). World's Biggest Data Breaches & Hacks. Retrieved 15 March 2017, from http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Morozov, E. (2014). *To save everything, click here: the folly of technological solutionism*. New York: Public Affairs.

Mossberger, K., Tolbert, C., & McNeal, R. (2008). *Digital citizenship: The Internet, society, and participation*. Cambridge, Mass.: MIT Press.

Mozilla. (2017, March 9). Hackers, Trackers and Snoops: Our Privacy Survey Results. Retrieved 13 March 2017, from https://medium.com/mozilla-internet-citizen/hackers-trackers-and-snoops-our-privacy-survey-results-1bfa0a728bd5#.j844ubv38

Newsletter on Intellectual Freedom. (2014). ALA backs legislation to limit NSA. *Newsletter on Intellectual Freedom*, *63*, 3–35.

O'Neill, P. H. (2016, February 18). New Hampshire bill allows public libraries to run Tor in the face of federal challenges. Retrieved 4 July 2017, from https://www.dailydot.com/layer8/new-hampshire-tor-library-legislation/

Online Centres Network. (2017, January 3). New centre survey is live - but what are we learning? | Online Centres Network. Retrieved 10 July 2017, from https://www.onlinecentresnetwork.org/news-and-activity/news/new-centre-survey-live-what-are-we-learning

Payne, D. (2016). New research maps the extent of web filtering in public libraries. Retrieved 26 June 2017, from https://www.cilip.org.uk/blog/new-research-maps-extent-web-filtering-public-libraries

Payton, T. M., & Claypoole, T. (2015). *Privacy in the Age of Big Data: Recognising threats, defending your rights and protecting your family*. Rowman & Littlefield.

Peachey, J. (2017). Shining a Light: The Future of Public Libraries Across the UK and Ireland. Retrieved 20 August 2017, from https://www.carnegieuktrust.org.uk/carnegieuktrust/wp-content/uploads/sites/64/2017/04/Policy-Report-Shining-a-Light.pdf

Pedley, P. (2011). *Essential law for Information Professionals* (3rd ed.). London: Facet.

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

Pedley, P. (2016). CILIP: the library and information association. Retrieved 15 January 2017, from https://www.cilip.org.uk/blog/privacy-library-user

Pedley, P. (2017a). Musings on a definition of 'privacy''. Retrieved 16 July 2017, from https://libraryprivacyblog.wordpress.com/2017/07/10/musings-on-a-definition-of-privacy/

Pedley, P. (2017b, August 4). Enquiry about data protection laws.

Perry, M. (2010, June 30). Tips for Running an Exit Node | Tor Blog. Retrieved 11 May 2017, from https://blog.torproject.org/tips-running-exit-node

Pirate Party, The. (2015). Think Different? Vote Different: Our Manifesto for the General Election. Retrieved 16 March 2017, from https://www.pirateparty.org.uk/sites/default/files/library/NationalManifesto.pdf

Privacy International. (N.D.). What is Data Protection? Retrieved 22 March 2016, from https://www.privacyinternational.org/node/44

Revell, T. (2017, June 5). Theresa May's repeated calls to ban encryption still won't work. Retrieved 6 June 2017, from https://www.newscientist.com/article/2133644-theresa-mays-repeated-calls-to-ban-encryption-still-wont-work/

Richards, N. (2015a). *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*. Oxford: Oxford University Press.

Richards, N. (2015b). How encryption protects our intellectual privacy (and why you should care). Retrieved 29 April 2015, from http://www.wired.co.uk/article/encryption-intellectual-privacy

Rust, E. (2014, June 23). When the UK goes 'digital by default', who will be left behind? | Technology | The Guardian. Retrieved 10 March 2016, from https://www.theguardian.com/technology/2014/jun/23/when-the-uk-goes-digital-by-default-who-will-be-left-behind

Scheff, S. (2014, November 21). Online Safety: What Does It Mean To You? Retrieved 10 June 2017, from https://www.huffingtonpost.com/sue-scheff/online-safety-what-does-i_b_6179918.html

Schneier, B. (2006, March 6). The Future of Privacy - Schneier on Security. Retrieved 2 August 2016, from https://www.schneier.com/blog/archives/2006/03/the_future_of_p.html

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

Scottish PEN. (N.D.). Libraries for Privacy: Digital Security Workshop. Retrieved 20 August 2017, from https://scottishpen.org/event/libraries-privacy-digital-security-workshop/

Segev, E. (2010). *Google and the Digital Divide*. Oxford: Chandos Publishing.

Simonite, T. (2015, November 3). Is Google's Lackluster Support for Encryption a Human Rights Issue? Retrieved 20 January 2016, from https://www.technologyreview.com/s/543161/why-google-trailing-apple-on-encryption-support-is-a-human-rights-issue/

Smith, B. (2017, May 14). The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack. Retrieved 14 May 2017, from https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/

Snowden, E. (2017, May 14). Extraordinary: Microsoft officially confirms @NSAGov developed the flaw that brought down hospitals this weekend.https://blogs.microsoft.com/on-the-

issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/ … [Tweet]. Retrieved 14 May 2017, from https://twitter.com/Snowden/status/863872972553166848

Soghoian, C. (2016). *Your smartphone is a civil rights issue*. Retrieved from https://www.ted.com/talks/christopher_soghoian_your_smartphone_is_a_civil_rights_issue

Surbhi, S. (2016, September 6). Difference Between Questionnaire and Interview (with Comparison Chart). Retrieved 7 August 2017, from https://keydifferences.com/difference-between-questionnaire-and-interview.html

Temperton, J. (2015, September 18). AVG can sell your browsing and search history to advertisers. Retrieved 9 February 2017, from http://www.wired.co.uk/article/avg-privacy-policy-browser-search-data

The Tor Project. (2011). Response template for Tor relay operator to ISP. Retrieved 11 July 2017, from https://www.torproject.org/eff/tor-dmca-response.html

Thomas, K. (1966). *Early Public Libraries: a history of public libraries in Great Britain before 1850*. London: London Library Association.

Trottier, D. (2012). *Social Media As Surveillance: Rethinking visibility in a converging world.* Oxon: Routledge.

TRUSTe, & NCSA. (2016). 2016 TRUSTe/NCSA Consumer Privacy Infographic - GB Edition. Retrieved 14 March 2017, from https://www.trustarc.com/resources/privacy-research/ncsa-consumer-privacy-index-gb/

Virtual Privacy Lab. (2015, October 1). Virtual Privacy Lab. Retrieved 9 April 2017, from https://www.sjpl.org/privacy

Wade, M. (2017, May 10). Privacy in a Digital Age - Carnegie UK Trust Seminar on Future of Public Libraries | Carnegie Council for Ethics in International Affairs. Retrieved 14 June 2017, from https://www.carnegiecouncil.org/studio/multimedia/20170510-privacy-in-a-digital-age

Wasterlain, J. (2015, July 23). Guest post: one librarian's privacy class success story – Library Freedom Project. Retrieved 14 July 2017, from https://libraryfreedomproject.org/privacyclasssuccess/

Webb, J. (2009). *Dictionary of Law*. London: Penguin Books.

Wiles, R. (2013). *What Are Qualitative Research Ethics?* London: Bloomsbury.

Williams, C. (2013, April 2). Google faces privacy investigation over merging search, Gmail and YouTube data - Telegraph. Retrieved 1 April 2016, from https://www.telegraph.co.uk/technology/google/9966704/Google-faces-privacy-investigation-over-merging-search-Gmail-and-YouTube-data.html

Williams, N. (2016, November 24). Scottish PEN Archives. Retrieved 1 April 2016, from http://theinformed.org.uk/tag/scottish-pen/

Wilson, L. (2016, September 22). Taking digital inclusion in libraries to the next level - Libraries Taskforce. Retrieved 9 April 2017, from https://librariestaskforce.blog.gov.uk/2016/09/22/taking-digital-inclusion-in-libraries-to-the-next-level/

wtwu. (2009, March 19). Passion and Dalliance blog: Why you need balls of steel to operate a Tor exit node - Spy Blog - SpyBlog.org.uk. Retrieved 16 July 2017, from http://spyblog.org.uk/blog/2009/03/passion-and-dalliance-blog-why-you-need-balls-of-steel-to-operate-a-tor-exit-nod.html

Wu, T. (2012). *The Master Switch: The Rise and Fall of Information Empires*. Toronto: Borzoi Books.

Yin, R. K. (2009). *Case Study Research: Design and Methods* (4th ed.). Toronto: Sage Books.