“Privacy, Security, and Service: Squaring the circle between multiple influences in Scottish Public Libraries”

By

Karl Thurgood

This dissertation was submitted in part fulfilment of requirements for the degree of MSc Information and Library Studies.

DEPT. OF COMPUTER AND INFORMATION SCIENCES

UNIVERSITY OF STRATHCLYDE

SEPTEMBER 2016

Declaration:

This dissertation is submitted in part fulfilment of the requirements for the degree of MSc at the University of Strathclyde.

I declare that this dissertation embodies the results of my own work and that it has been composed by myself. Following normal academic conventions, I have made due acknowledgement of the work of others.

I declare that I have sought, and received, ethics approval via the Departmental Ethics Committee as appropriate to my research.

I give permission to the University of Strathclyde, Department of Computer and Information Sciences, to provide copies of the dissertation, at cost, to those who may in future request a copy of the dissertation for private study or research.

I give permission to the University of Strathclyde, Department of Computer and Information Sciences, to place a copy of the dissertation in a publicly available archive.

(please tick) Yes [√] No [ ]

I declare that the word count for this dissertation (excluding title page, declaration, abstract, acknowledgements, table of contents, list of illustrations, references and appendices is 19,251

I confirm that I wish this to be assessed as a Type 1 2 3 [✓ 4] 5

Dissertation (please circle)

Signature:

Contents

Abstract:

This study considers the topic of privacy, how this concept is understood within the library profession and how that understanding is reflected within the policies governing the operation of public libraries within Scotland.

Consideration is first given to the historical and theoretical background of thought surrounding privacy, identifying privacy as neither an absolute, nor binary right, but as a qualified right – one whose protection should be balanced against the need to protect others from harm. The study then seeks to formulate a clearer understanding of what privacy is in the context of a public library through the application of discourse analysis to the discourse on privacy of three major professional librarianship bodies – CILIP, IFLA and the ALA, and selected sources from the United Kingdom's Information Commissioner. A broad consensus is noted on the purpose and nature of privacy within the Public Library environment.

In the second stage of the study policy documents relating to privacy from Scotland's 32 public library authorities are studied. A qualitative analysis of these finds that the concept of privacy held by the library profession is only reflected to a limited degree policy, and that little policy reflects the specific nature of the public library context. Public library policy is primarily focused on meeting the requirements of the Data Protection Act, with little consideration being given to the broader elements of privacy or to a rational for it beyond the requirements of the Acts. Little consensus is found on how and what should be communicated to patrons regarding privacy issues.

Recommendations are made for further research and for ways in which the profile of privacy can be raised within the public library sector. Practical recommendations are also made in regard to the adoption of a common baseline for Privacy Statements to ensure that library patrons across Scotland receive at least a minimum consistent degree of information regarding their privacy.

1. Privacy and Libraries:

Where do libraries and librarians stand in regard to privacy? Libraries are, in general, regarded as public spaces which are open to the community in general or a defined subset of it, rather than private spaces. Nevertheless librarians have a long history of considering that maintaining the privacy of library patrons is a matter of importance to the profession. The historical roots of this view may well lie in the tendency for some librarians to view themselves as protectors of intellectual freedom and the freedom to read. S.R. Ranganthan, often held to be the first person to put forward a code of ethics for librarians, held amongst his fundamental principles of librarianship the idea of "every reader his book" – the idea that the right to read and to enquire is a fundamental defining feature of libraries (Gorman, 2015) pp.26-27). Bowers argues that, whilst this freedom to read is a fundamental principle of libraries, people may well be unwilling to engage with a controversial subject if they feel that their community, broader society or their government will know of it and make judgements about them based on that knowledge. Bowers argues it is impossible to exercise the right to read if one feels that one has to self-censor because someone may be watching (Bowers, 2006). Therefore it would follow that protecting the privacy of patrons is a vital aspect of protecting their freedom to read.

The principle professional bodies also consider protection of patron privacy to be a key element of the librarian's role. The American Library Association (ALA) identifies privacy as an essential component of the idea of free speech and thought (American Library Association. Office for Intellectual Freedom, 2010), whilst the International Federation of Library Associations (IFLA) states:- "Library and Information Services should respect and advance privacy both at the level of practices and as a principle" (International Federation of Library Associations, 2015). The United Kingdom's Chartered Institute of Library and Information Professionals guidelines enjoin members that they must respect the confidentiality and privacy of all information users (Chartered Institute of Library and Information Professionals, 2011).

In a practical sense the achievement of this aim has become more complex with the coming of digital technology to libraries. In the past libraries may or may not have kept records of what patrons read or what information they searched for – in some card-based systems the connection between item and reader was explicitly a transient one. The reader's right to read as they saw fit was therefore protected by the very nature of the system. No-one could say who had read what as that information simply did not exist. Modern digital library systems, and digital technologies in general, create records in much more detail and specificity and, as Sturges has observed, such records are inherently easier to retrieve, search and manipulate (Sturges et al., 2003). The complexity of these systems, as Karen Coombs observed, can also make it difficult to determine where user information might actually be located in the system in order to protect it (Coombs, 2005).

Then there is the current trend for using Radio Frequency Identification (RFID) devices within libraries for stock control purposes. Whilst these tags allow easier stock control for librarians, they raise their own concerns. Even without directly exposing a reader's identity or any information, the fact that each RFID has a unique tag number creates the possibility that the tagged book, and the patron in whose possession it is could be tracked by anyone with a suitable reader(American Library Association Office for Intellectual Freedom, 2010). Whilst at the moment these tags contain very little information it is by no means certain that this will remain the case – function creep in the name of efficiency is something that occurs in all walks of life. If so the fact that the RFID's used in libraries do not use any authentication protocols or passwords means that this information would be exposed to anyone with a compatible reader, not just library staff (ibid). The nature of the technology, and the power needed to receive the relatively weak signals, may mean that an "eye in the sky" won't be tracking these RFID. But readers on the ground at a few carefully chosen locations could build up a fairly good picture of the tag's movements – something that could easily be used to compromise the reader's identity or his activities. In academic libraries, which are coming more and more to depend on technological solutions for access control, correlating this data with records of card-operated entrance gates would make this kind of breach much easier. But someone's privacy doesn't need to actually be breached for it to act to reduce their own freedom of enquiry. The mere knowledge that someone might be watching them is often enough for human beings to change their behaviour. The knowledge that someone *could* do this might be enough to make someone reconsider before borrowing controversial material, circumscribing the freedom to read that library professionals are ethically bound to protect.

1.1 US and UK perspectives:

It is notable that the majority of the literature on patron privacy and the “security agenda” originates from the United States, and that there is a relative paucity of material of UK origin. In part this may be a result of the ALA’s long-standing tendency to take a strong public position on the issue of privacy at least as far back as the 1970’s. During this period the Federal Bureau of Investigation operated its Library Awareness Program, involving FBI agents approaching library staff to request that they report on the reading habits of library patrons who were deemed to be “security risks”. This was conducted without warrants or other formal authorisation, merely a visit by an FBI agent requesting that the librarian be a “good American”. It targeted foreign students, visiting professors and other individuals against whom the Bureau had no particular evidence of involvement in espionage – very much as a “fishing expedition”. The ALA took a strong stance opposing the program and the majority of US librarians appear to have refused to cooperate (Bowers, 2006).

The passing of the “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act”, better known as the USAPATRIOT Act, in October 2001 similarly provoked a strong reaction from American librarians, the ALA and individual state library associations. The Madison County Public Library Board, for example, chose to directly address the issue with a statement of their opposition to the Act and an affirmation of their support of the principle of patron privacy and intellectual freedom(Madison Public Library Board, 2004). By 2004 the ALA noted that three states and 210 individual jurisdictions had passed measures of one kind or another indicating that they were uncomfortable with parts of the Act.

Many US librarians also began to take practical steps in the light of the act, choosing to ensure that they did not retain some information in order that they could not be required to disclose it. In one study of 344 public and academic libraries in the state of California for example 78% of respondents indicated that they routinely shredded documents like computer sign-in sheets. Of those who responded, 73% also indicated that they deleted files and logs from computers(Albanese et al., 2003).

The case of the John Doe librarians’ resistance to disclosing usage records of a library computer under the terms of a National Security Letter (NSL) attracted some media attention and publicised the nature of the NSL process. Authorising FBI access to records of all kinds without the need to target specific individuals or to identify if any criminal act is suspected, these also forbid the recipient from disclosing to anyone that such a request has been received (Oder, 2006. Oder, 2007).

The ALA has made very clear statements of their view that this legislation and the security agenda undermines principles of privacy and intellectual freedom (American Library Association. Office for Intellectual Freedom, 2010). Dorothea Salo has gone so far as to describe the digital world as becoming akin to Jeremy Bentham's "Panopticon" – a theoretical prison in which all inmates can be watched at will by authorities from a central point – in which every citizen is an inmate(Salo, 2013).

Whilst there has been considerable discussion both in the literature and in public regarding the impact of the USAPATRIOT Act on US libraries, similar legislation such as the Terrorism Act (2000) in the UK has elicited comparatively less comment from British librarians. Very similar powers to demand borrowing and internet activity records without demonstrating suspicion of wrong-doing, and with only limited oversight, exist in this act, albeit without the "gagging" clauses of USAPATRIOT. But the Terrorism Act has not engendered a similar strength of reaction as its transatlantic cousin. Elspeth Hyams reports a study which found that whilst a number of libraries had received requests for patron's information under this legislation there was a general lack of awareness of the Act's provisions (Hyams, 2007). Hyams argues that whilst a right to privacy still exists in the United Kingdom it remains under threat. Context suggests that if this call was heard it has not necessarily been heeded.

1.2 The natures of privacy:

That said, when we are considering the protection of patron privacy, what is it that we are protecting? In the preceding discussion we have proceeded as if this is a generally understood term for which a common understanding is shared. Closer examination reveals that this is not necessarily the case.

Many different theoretical definitions of privacy in a broad sense exist, with varying natures and scopes. Warren and Brandeis put forward one of the earliest pervasive definitions of privacy in terms of law in an 1890 essay, defining it as a right to be left alone (Wacks, 2010), pp.55).

From this a vision of privacy as defined by the level of accessibility that others have to an individual – with total privacy being defined as total inaccessibility - has been developed by Gavison and others. (Rössler, 2005, pp.7).

By contrast Westin argues that privacy is a matter of the individual's ability to choose what information to share, and with whom(Wacks, 2010) Charles Fried's definition echoes this, stating that Privacy is the control that an individual has about information regarding himself (Rössler, 2005 pp.7).

These formulations have been challenged by Feminist thinkers who argue that traditional definitions of privacy have essentially acted to support the repression of women, by constraining to a "private" domestic sphere out of sight and out of mind of the rest of society, and to obscure ill-treatment and violence (Wacks, 2010) pp. 36) (MacKinnon, 1987, cited in (Wacks, 2010) pp.36), and who have proposed reframing of the concept.

Privacy has also been defined as the right to prevent intrusion in certain locations or dwellings – "locational" or "local privacy" (Wacks, 2010), pp.40.), (Rössler 2005, pp.142.). Or the "right to be left to make your own choices" – privacy defined as personal autonomy (Wacks, 2010), pp.40.)

Daniel Solove, in his paper "Conceptualising Privacy" argues that the difficulty in defining privacy and the nature of its importance has often hindered privacy law from being effective (Solove, 2002).

These many definitions of privacy vary considerably in what they consider privacy to be concerned with. As a result when we discuss "privacy" perhaps the first question that we should be asking ourselves is, what exactly do we mean when we speak about privacy?

1.3: The Research Questions: defining privacy in the library setting:

The primary goal of the present research is, therefore, to address that question – what do we mean by privacy? It is not my goal to propose an expansive definition of the concept, which encompasses every possible situation and environment to which privacy might be applicable. It is rather my intent to examine the existing literature on the nature of privacy and to seek to synthesise from this a definition of what privacy means in a specific context - that of the library.

The first goal of the present research is therefore to seek an answer to the question:-

- "What are the dimensions and nature of privacy, in the context of a public library?"

In the context of the paucity of literature regarding privacy from the UK library sector it is important that we consider the degree to which privacy is embedded at a policy level in Scottish libraries. It is therefore the intention to create, on the basis of the definition of privacy arrived at, a tool which can be used in the analysis of policy documents to determine:-

- "To what degree do the policies of libraries in Scotland reflect the identified nature and dimensions of privacy?"

It is hoped that the answers to these questions can provide some indication of the degree to which there is a consensus on the nature of patron privacy, and the extent to which this expressed in existing policy within the Scottish public library sector.

2: Privacy – an ancient, and polarizing, topic:

Privacy has been a matter that has been much debated throughout human history. Even the ancient Greeks and Romans actively debated the desirability and proper limits of privacy. That debate has remained active for such a length of time perhaps illustrates the importance that the issue holds in human affairs. The debate has become increasingly polarised. On the one hand some argue that people's privacy should be held inviolate, and that it is an absolute, unbreachable entitlement. On the other are those which argue that privacy is easily abused by criminals, terrorists and others seeking to do harm to others in secret, and that "if you have nothing to hide you have nothing to fear".

2.1: What is privacy?

There have been many formulations of privacy advanced over the years. One of the first to be advanced was proposed by Louis Brandeis and Samuel Warren, in a reaction to concerns about the consequences of the rise of instant photography and mass produced newspapers. They argued that implicit in the law was a protection from intrusion for some elements of a person's life – what they called a "right to be left alone" (Warren and Brandeis, 1890). This basic formulation has been influential in much of the later development of the concept of privacy.

Anita Allen (Allen, 1987) and Ruth Gavison extended this idea, characterising privacy as relating to the inaccessibility of an individual, or information about them, with perfect privacy being the unattainable state of total inaccessibility (Gavison, 1980). Such a definition would, taken by itself suggest that the situations in which there could be any expectation of privacy would be few and far between, and would force us to conclude that the very nature of a *public* library would sharply limit the amount of privacy which could exist within it.

By contrast a different strand of thought, exemplified by Alan Westin (Westin 1970, p7), and Charles Fried among others, suggests that privacy is better described as the possession of a degree of control about what information about yourself that you reveal to others. For some this description, too, is incomplete. They suggest that the individual is not the only source of information about themselves. Even if you choose not to reveal something about yourself there may be other ways that this information can be obtained, and that surely this should be encompassed by any definition of privacy (Wacks 2010 pp.41). Spinello developed this notion further, proposing that "informational privacy" concerns the collection, use and onward transmission to a third party of information about an individual. Spinello argues that a right to informational privacy is a "right to control the disclosure of and access to one's personal information" (Allmer, 2011). This "control" idea, and focus on information which is personal to the individual is one which has particular relevance for libraries. A similar approach underpins European and UK data protection legislation, with its controls on the way information about people is gathered, used and shared. The concept of personal information also captures some of what library staff deal with in relation to patrons – whether a home address given to register for a library card or the reference interview yielding knowledge of what information they sought.

This equation of privacy with control has been taken further and extended to cover more than simply information about an individual. In the United States the Supreme Court has found that privacy is implicated in such matters as the right to use or not use contraception (Wacks, 2010 pp.59) or, in Roe vs Wade, to terminate a pregnancy (Wacks, 2010 pp.60) or to make or not make religious observances. What might be called "decisional privacy" (Wacks, 2010 pp.40).

This idea of Decisional Privacy has its echoes in Bernal's argument that privacy is a necessary prerequisite for people to have autonomy – the ability to make meaningful choices about their lives. Bernal argues that privacy is essential in providing a space in which people can make these choices, free from the influence of outside agencies who may wish to direct or manipulate these choices . (Bernal 2014, p.10). Albert Bendich echoes this with his suggestion that US constitutional law has come to see privacy as a protector of the dignity of the individual and their right to the freedom to develop their personality as they see fit (Bendich, 1966).

2.1.1 Legal perspectives on privacy:

In the US two related legal concepts of privacy have developed – one in Constitutional law, stemming primarily from the First Amendment(guaranteeing freedom of speech) and the

Fourth Amendment's prohibition of unreasonable search and seizure, and the other in common law.

The Supreme Court has repeatedly held that: "various guarantees create zones of privacy" (Douglas, quoted in Wacks, 2010 pp.59). This privacy has been held to be more than simply the "right to be let alone" in the sense of isolation or solitude. As we have seen it is considered to encompass the right to make decisions about one's own life and lifestyle without state interference. It is also held that it is possible for acts which are private to occur in a public place. In Katz vs United States for example it was held that the FBI had acted unconstitutionally by placing a bug in a private phone booth to eavesdrop on a suspect's calls without a warrant. The Court identified a phone booth as a place where someone's business might be private even if it was carried out in a public place (Rauhofer, 2008). There are parallels here to the ALA's objection to the Bureau's Library Awareness Program – where FBI agents asked librarians to report on the reading habits of foreign nationals, without warrants or documented suspicion of illegal activity. The ALA strongly protested what they saw as an unjustified and unauthorised intrusion into these individuals' privacy.

The common law approach, remaining largely as summarised in (Prosser, 1960), consists of four basic areas of privacy violation which the law provides for restitution against:-

i) Appropriating someone's identify for one's own benefit
ii) Painting someone in a false light to the public
iii) Disclosing private facts about someone in public
iv) Unreasonably intruding on someone's solitude or seclusion

This formulation has remained at the heart of the US common law understanding of privacy ever since - Richards and Solove describe the influence of Prosser's summary on this area as "profound"(Richards and Solove, 2010)

The US legal conception of privacy corresponds with several of the previously discussed theoretical stances. Ideas of solitude and of control – both of information and of personal life choices – can be seen in common law and Constitutional Jurisprudence. But these are not presented as unbounded and absolute. It is not all intrusions on an individual's solitude that the law offers restitution for. Likewise Katz vs United States indicates that some acts remain private in nature when performed in a public space, but by inference that others do not. This is an important distinction and one to which we will return.

By contrast with the US legal perspective where a distinct right to privacy is held to exist, the view of the common law of the UK is that privacy does not exist as a distinct right. Indeed the case of Malone vs Metropolitan Police Commissioner (1973), concerning telephone taps, stands in distinct contrast in this respect to Katz vs United States.

In the latter it was found that placing a bug in a phone booth without a warrant was illegal and that it violated a reasonable expectation of privacy Katz possessed in the phone booth. By contrast in Malone vs Metropolitan Police Commissioner the court found that it was not possible for telephone taps to be illegal in UK law as no right to privacy existed, and there was therefore nothing for them to breach (Open University, 2016).

It remains the case that no right to privacy per se exists in UK law. This does not mean that there are not protections for privacy itself. Rather than creating a right to privacy, existing law has been developed in order to provide this protection. In this way protections have evolved in a way that the International Court of Justice described as "almost by accident" (Gonzales-Fuster, 2014 p.42). Much of this development has been in the law relating to breach of confidence. Oft-referred to in this respect is Prince Albert vs Strange (1849), here the Royal Family sued a publisher who had obtained copies of etchings which had been done of them at home. The publisher intended to market these for commercial gain and Prince Albert sued to prevent publication. Ruling in favour of the Royal Family, the court held that the law protected their right to choose who would be allowed to see these images (Open University, 2016).

The law relating to confidence has subsequently continued to expand to cover more of what we might consider to be privacy. In Douglas and Others vs Hello! Ltd (2002) the issue related once again to images. Michael Douglas and Catherine Zeta Jones had sold exclusive rights to media coverage of their wedding to OK! magazine. Unauthorised photographs were taken and subsequently sold to Hello!. In the judgement the judge noted that although there did not exist a law of privacy the law of confidence sufficed to provide protection. This judgement established that where there was reason to conclude that a matter was supposed to be private – such as the extensive security measures put in place to prevent photography at the Douglas wedding – then an unjustified intrusion into that privacy could constitute a breach of confidence (Moreham, 2001).

Campbell vs Mirror Group Newspapers Ltd (2002) further developed this. The High Court held that there was a public interest in the Mirror reporting that Naomi Campbell, a model and celebrity who had publically denied taking drugs, was receiving treatment for drug addiction, but that even people in the public eye had a right to a certain degree of privacy. They found no public interest justifying invading that privacy by the publication of the details of the treatment (Reid, 2010).

Confidence requires three things to be the case:-

i) That the information has the necessary quality of confidence

ii) The information must have been in circumstances importing an obligation of confidence – that is the person receiving it must know or have reason to know that the information is private.

Iii) There must have been an unauthorised use of the information which caused some kind of detriment to the person it concerned.
(González-Fuster, 2014)

Confidence is not, however, held absolute in law. There are a number of factors which can cause a piece of information to no longer qualify for protection as a confidence (Open University, 2016):-

i) Information falling into the public domain – that is, accessible without excessive effort by any individual.

ii) Being lacking in value – confidence does not protect information which is trivial or useless

iii) Where it is out-weighed by another public interest which favours disclosure

So whilst UK common law does not admit a specific right of privacy, the law of confidence does provide some protection for what we would recognise as privacy. But this is not an absolute protection, it one is subject to being over-ridden where another public interest is held to be more important.

2.1.2 The European Convention on Human Rights:

The European Convention on Human Rights, to which Britain is a party, also establishes a right to privacy. The Convention's Article 8 states that:- "everyone has the right to respect for his private and family life, his home and correspondence," (Council of Europe, 1968).

The concept of "private and family life" has been interpreted broadly by the European Court of Human Rights. Similarly to the US Supreme Court it has framed this right as also including the right of an individual to live in a way directed by their personal inclinations and beliefs (McGroaty and Finch, 2010, pp.94). Much like Lawrence vs Texas the ECHR has upheld that a right to privacy protects peoples sexual behaviour – Dudgeon vs UK (1983) and ADT vs UK (2000) both held that prosecutions for consensual homosexual activity were a breach of Article 8's right to a private life. In the latter case it was noted that this interference could not be categorised as "necessary in a democratic society" to protect public morality or the rights of others (Open University, 2016). This categorisation is of significance to us, because it establishes that the right to privacy contained in Article 8 is not envisaged as absolute and inviolable.

2.1.3: Limits of privacy: privacy as a qualified right

The right to a private life is classified in the ECHR as what is referred to as a qualified right. Qualified rights differ from those which are defined as Fundamental in that there are viewed as legitimate purposes for which the state can restrict a given qualified right (McGroaty and Finch, 2010 pp.91).

This is not a concept new to the ECHR. Most formulations of rights accept that there are certain limits to the freedom of an individual, if only to prevent the one individual's exercise of their freedom preventing another individuals exercise of theirs. In its narrowest form this principle can be seen in Mill's argument that the only legitimate basis for interfering with an individual's liberty is to prevent them from harming others (Mill, 1985), p72-73). This principle is not unlike the observation often rendered as "your freedom to swing your arm ends where my nose begins"(Chafee, 1919). This is the essence of a qualified right – it is not absolute and unchallengeable. Instead it has limits, and can be restricted in the interests of wider society. The ECHR defines some rights as Fundamental – the right to life, prohibition of slavery and torture and the right not to retroactively be punished for acts which were not criminal at the time they were performed – these are held as being absolute and it is not possible for the state to restrict them(McGroaty and Finch, 2010, pp45).

By contrast, rights such as Article 8's respect for private life may be restricted, so long as this is done in accordance with the ECHR's principles. In all cases any interference with these rights must meet certain criteria(McGroaty and Finch, 2010, pp92):-

a) It needs to be lawful, that is carried out in accordance with the law of the member state concerned.
b) It has to be done for a purpose that the ECHR recognises as legitimate.
c) It must be deemed to be "necessary in a democratic society".
d) It must not be done in a discriminatory manner.

The rights under Article 8 to respect for private and family life, home and correspondence are therefore not absolute, and can be abridged for legitimate purposes (McGroaty and Finch, 2010, pp.91) . These legitimate purposes are defined in the ECHR, and in UK law by the Human Rights Act. These sources identify the following purposes for restriction of the rights under Article 8 which are seen as being legitimate(McGroaty and Finch, 2010, pp.91):-

i) The interests of public safety.
ii) The protection of public order.
iii) The protection of health or morals.
iv) The protection of the rights and freedoms of others.
v) The interests of national security.
vi) The economic well-being of a country.
vii) The prevention of crime.

These criteria were considered in Klass and others vs the Federal Republic of Germany, in regard to the interception of telephone conversations. Klass et al challenged a German federal law which allowed certain agencies to apply for judicial authority to monitor a suspect's telephone conversation. The European Court noted that the existence of such measures by their nature infringes the right to a private life under Article 8. However, the court also observed that this was done in the interests of national security and the protection of the public and national security. As there were sufficient measures in law to prevent abuse of the measures, and to ensure that only the minimum deemed "necessary in a democratic society" was done, the court found that this restriction on the private life was legitimate and that there had been no breach of Article Eight (European Court of Human Rights, 1978). By contrast, when Malone vs Metropolitan Police Commissioner was referred to the Court the results were different. The Court made reference to Klass et al in finding that the arrangements in UK law at the time, where police were issued warrants for telephone taps on the discretion of the Home Secretary, did not provide suitable protections against abuse. The court found that the lack of judicial oversight meant that they could not be seen to be "in accordance with the law" (UK law on this matter was amended following the judgement), and that as a result a breach of Malone's Article 8 rights had taken place (European Court of Human Rights, 1984).

The "right to a private life" under the ECHR then is not an absolute one. It is subject to limits and qualifiers. It can be restricted, not arbitrarily and capriciously, but if it conflicts with other rights and duties, of citizens or the state.

The nature of the right to privacy in US law is less clearly specified. It is often maintained in American discourse that the rights laid out in the Constitution and the Bill of Rights are absolute and that their language is iron-clad (Wilkinson, 2010). That is, for example, that the language of the First Amendment (the right to free speech) means that all speech is protected equally whatever its nature, or that the Constitution permits, or even requires, American citizens to own any kind of firearm that they please.

Wilkinson observes that in practice these rights are far less absolute and all-encompassing than might be thought. The First Amendment does not protect speech which in and of itself violates other laws – such as, for example, child pornography(Wilkinson, 2010). In a similar manner, the Fourth Amendment’s protection from “unreasonable search and seizure” by dint of its language provides protection only from those intrusions which are deemed to be “unreasonable”, leaving the definition of reasonable and unreasonableness for each generation to determine. This argument is at the heart of the previously mentioned “John Doe” Librarian case (Oder, 2006, Oder, 2007). The argument advanced being, in part, that monitoring all users of a particular computer terminal was unreasonable as it targeted all users of the terminal not just a specific individual suspected of wrong-doing. Similarly the ALA had argued previously that the FBI’s Library Awareness Program constituted unreasonable search as it was not authorised by warrant or court, or based on a specific suspicion. (Bowers, 2006).

Wilkinson observes that in practice rights are often restricted by the interests of society as a whole, most commonly in the powers of police and law enforcement organisations to protect society. Wilkinson identifies inherent in this situation a balancing of rights granted to an individual with the interests of wider society(Wilkinson, 2010). It should also be remembered that the Constitution and its Amendments, provide protective rights only insofar as against the state. The right to be free of unreasonable search may apply to the government and its agents entering your house or, perhaps, from reading the contents of your emails but in itself it provides no protection from Google or Facebook. Such protection against private entities comes from the interplay of common law and contract – such as the contract to “sell” elements of one’s privacy embedded in the Facebook sign-up agreement (Milazzo, 2014). So, whilst rights in general, and privacy in particular, are often discussed in absolute terms in the US environment they are - in practice - subject to qualifications and restrictions just as are the UK formulations.

The question of the right to privacy then is not simply a binary matter of its existence of non-existence. Privacy is not an absolute right; it is instead a qualified one which must co-exist with the rights of others and of society in general. The question for libraries therefore becomes how we wish to qualify privacy? Where are we to strike the balance between the privacy of the individual and the rights of others to have security and freedom from crime?

2.2: Privacy and libraries

As we have seen, many theoretical and legal definitions of privacy have been developed, but what does it mean for librarians? What is privacy in the context of public libraries, and why is it important?

The importance of privacy as a concept has a long standing within the profession of librarianship. One of the earliest attempts to establish a code of behaviour for librarians was put forward by S. R. Ranganathan. As part of this he stated: “Every book its reader, and every reader his book” (quoted in Gorman, 2015, pp.26)

Ranganathan advocated a right of freedom of access to books, and by extension to the ideas contained in them. Michael Gorman argues that librarians must, on moral grounds, hold a basic premise that all library patrons have equally the freedom to read, to access information and to think about that information for themselves (Gorman, 2015, pp.111). Gorman also expresses the belief that none of these rights can exist where people know or believe that what they read is monitored and examined by others(Gorman, 2015, pp.185).

Paul Sturges argues that the privacy of what patrons do is a very necessary aspect of the libraries service. Sturges suggests that there are many reasons for its importance – that it allows mental space for people to express their individuality, to define their own needs for themselves as well as the freedom to consider unorthodox or unpopular lines of thought (Sturges et al., 2001)

The codes of ethics of the professional bodies in Librarianship reflect a similar line of thinking. The ALA state that they view the right of privacy as essential to the right to open enquiry and to intellectual freedom. The ALA also expresses the view that respect for the privacy of patrons is therefore an essential element of ethical librarianship. Their code of ethics states that:- “We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted.” (American Library Association, 2008)

This view of the importance of privacy is echoed by the International Federation of Library Associations (IFLA), who argue that privacy is an essential prerequisite of the rights of freedom of access to information and expression laid out in Article 19 of the Universal Declaration of Human Rights, and that libraries therefore have a duty to respect privacy "in principle and practice" (International Federation of Library Associations, 2015). Their code of ethics also calls on librarians to respect and protect the personal privacy of their patrons, and the confidentiality of interactions between staff and users.

As the governing body of librarianship in the United Kingdom CILIP, has expressed in similarly clear terms its belief in the importance of privacy. Their Ethical Principles statement, which establishes the nature of conduct expected from members of the profession, specifically refers to the need to respect the privacy of users of information and the confidentiality of their information use (Chartered Institute of Library and Information Professionals, 2013b) . They also have indicated that Intellectual Freedom is undermined when privacy is not respected, and when people fear reprisal for accessing certain information or for expressing their ideas(Chartered Institute of Library and Information Professionals, 2015) .

A consensus can be seen therefore in the librarianship profession as to the meaning of privacy in the library context, and as to why it matters. There is an agreement that patrons should be able to access information and to use it without being scrutinised, that the nature and content of their interactions with library staff should be considered to be in confidence. There is also a broad agreement that without respect for the privacy of their enquiry the patron's Intellectual Freedom becomes circumscribed, and that therefore patrons must be free to enquire without wondering who might be watching what information they access. Privacy therefore matters to libraries because without it the goal of providing free and equal access to information becomes impossible to achieve.

Michael Gorman adds a further, practical, consideration to this discussion. He argues that the relationship between libraries and their communities is one that is predicated on trust and that this trust is eroded where patrons believe that the library will not preserve the confidentiality of their enquiries and their business(Gorman, 2015, pp191)

Clearly there are many different theoretical approaches to privacy and understandings of what is meant by it. But it seems equally clear that privacy is of relevance to librarians both as an ethical principle, and as an important requirement for achieving the goal of providing free and equal access to information. How then is this reflected in the policies which govern how public libraries operate? Surprisingly little investigation has been done into this matter. Whilst there has been some consideration of the topic this has tended to be in the context of academic libraries (Sturges et al., 2001) (Coombs, 2005), or has concentrated solely on issues relating to electronic information or internet use (Sturges et al., 2003) (Gallagher et al., 2015). The question of how privacy is embodied at the policy level in public libraries has meanwhile gone unanswered.

It is therefore my proposal to investigate how the policies of public libraries in Scotland consider privacy and what elements of the conceptualisations of the professional bodies are reflected in them.

3: Methodology:

3.1 Quantitative or qualitative:

It was decided to approach this research from a qualitative standpoint rather than quantitative. It was felt that this would be the more effective approach to take due to the nature of the research goal. Due to the observed nature of privacy as an element of the social world subject to varying definitions it was felt that quantitative research, the paradigm of which is to view social reality as an objectively existent phenomenon with measurable and quantifiable characteristics was less suited to the goals of the study. The deductive, theory-testing outlook of quantitative research also seemed an inappropriate tool in the absence of existing data from which to derive an initial theory to test. It was therefore felt that qualitative methods, based on a more inductive approach and whose paradigm views social reality as an emergent, and changeable, property was more suited to the purposes of the study (Bryman, 2016, pp.21).

3.2: Data sources:

The data sources used in this study were all public documents. They consisted of three groups of documents. The first group were those related to privacy sourced from the major professional bodies relating to public librarianship in the English-speaking world – the ALA, CILIP and IFLA. CILIP was chosen for inclusion as, being the professional body with responsibility for Librarianship within the UK, its conception of privacy in the library environment had direct relevance for Scottish libraries. The ALA was included as it was felt that there was a degree of cross-fertilization between the US and UK contexts, and as a result it was possible that ALA's view of privacy might have also have come to be reflected within Scottish library policy. IFLA were included in this group to represent the broader, international perspective on privacy. A search for documents relating to privacy was carried out of each body's website. This produced an initial pool of documents which was then assessed to screen out those not relevant to the study such as login pages referencing website privacy policies, book reviews etc. The remaining pool contained a variety of documents – including ethical codes, statements of principles, and press releases – which appeared to have bearing on their view of privacy.

The second group of documents was comprised of those sourced from the Office of the Information Commissioner. As the body responsible for overseeing the operation of the Data Protection Act within the UK it was considered that they could be taken to represent the legal constraints within which any policy developed for public libraries required to operate. It was therefore felt that their view of privacy could provide valuable context for this study. Documents relating to this were sourced from the Commissioner's website in a similar manner as above. A complete list of documents from CILIP, the ALA, IFLA and the Information Commissioner which were used is reproduced as Appendix 1.

The third and final group of documents were the policies relating to the public libraries themselves. As public libraries are public services, and thus fall under the jurisdiction of the Freedom of Information Act, FOI requests were made in order to obtain these. A request was sent to each of the thirty-two Public Library Authorities in Scotland. The requests were worded so as to be relatively non-prescriptive. Rather than request Privacy Policies per se the authorities were asked:- "I write to request, under the terms of the Freedom of Information Act, that you send to me, by email, copies of the policies on privacy which apply to your libraries." This wording was chosen so as to attempt to not prejudge the authorities' view of privacy and to leave the question open enough for each of them to respond to it according to their own understanding.

FOI requests were chosen as a mechanism for two reasons. They were deemed to be the most effective method of obtaining these documents, and previous studies carried out at the researcher's institution had obtained a good response rate using this method (Gallagher et al., 2015, Brown and McMenemy, 2013)

3.2.1: Criteria for inclusion:

All of the documents examined were pre-existing publically available documents. They were therefore viewed, for several reasons, as being suitable subjects for study. They had not been produced for the purposes of the research, representing communications addressed to the general public rather than to the researcher. They were relevant to the topic of the research, being identified as relevant to the topic of privacy.

In assessing the quality of the documents to confirm they were suitable for inclusion in the study regard was also had to the four criteria suggested by Scott (Scott, 1990) in (Bryman, 2016, pp.546)). The first criteria is *authenticity*, the question whether the evidence is genuine and its provenance known. As all of the documents used were sourced directly either from the official websites of the organisations studied, or from the organisations through the formal method of an FOI request it was felt that their authenticity would be high. The criteria of Meaning, the clarity and comprehensibility of the information, was also relevant, and in the most part was met as the documents had clear relations to the topic under study (ibid).

Scott also suggests that the *credibility* of documents should be considered – whether they are free from error and distortion (ibid) . In the case of this study the intent was to use the documents to identify the concepts of privacy which were embodied in the various library authorities' policies. It was considered that it was unlikely that the documents produced and submitted by the authorities themselves would deliberately misrepresent these ideas. Whether they reflected the actual practices of the organisations is a separate question. It has been observed that documents in themselves do not necessarily reflect the actual day-to-day reality of the way organisations operate. ((Atkinson and Coffey, 2011) in (Bryman, 2016) pp.561) argue that documents form a reality separate from that of day-to-day practice, something they call "documentary reality". This was not considered to represent a difficulty in the current study, as its subject was policy rather than practice. Whilst an examination of the degree to which the reality of everyday practice matched that of the documentary reality of policy might perhaps be illuminating it was beyond the remit of this study. As a result it was considered that the credibility of the documents would be sufficient for them to be valid subjects of study.

The final criteria which Scott suggests should be considered is Representativeness(Scott, 1990) in (Bryman, 2016, pp.546). By this he means whether the evidence used is typical of a document of its kind, or if the extent to which it is atypical is known. In this case the topic of interest was the similarities and differences between the ideas of privacy expressed by library authorities and professional bodies – in some regards making that very aspect of representativeness a part of the research question. As the nature of the concepts held by the various groups whose documents were studied were not known in advance it is acknowledged that there were difficulties applying the criteria of representativeness to determine inclusion of documents, but that this was not felt to be problematic given the nature of the study.

3.2.2: Geographical scope:

Scotland was chosen as the geographical scope of the research. This decision was taken for several reasons. Firstly Scotland is divided into 32 local authority areas, representing a large enough sample to produce sufficient data but also small enough not to produce too much data to be effectively analysed. It also represents a single legal jurisdiction, meaning that all of the authorities surveyed could be presumed to be subject to the same external influences in this regard. Scotland is also the researcher's location. As a result, examining the topic in a Scottish context has a high relevance for the researcher.

3.2.3: Anonymisation of data

Although no data on specific individuals was used in this study, it was still considered appropriate on ethical grounds to anonymise the contributing library authorities in the discussion of results. This was done to ensure that the focus of the discussion remains on the representations of privacy in the broader context of Scottish public library policies, rather than becoming side-tracked into discussion of the policy of particular library authorities or of specific documents.

3.2.4 Discourse Analysis:

The methodology which was chosen for this study was based in Discourse Analysis. There were a number of elements which made this seem to be a suitable methodology for the research. Discourse Analysis originates at least in part of the works of European philosophers, such as Michael Foucault. It takes as its starting point Foucault's concept of "discourse" as the idea that the way an object or idea is talked about and depicted acts to frame it. Effectively these elements, the discourse, around something become the object or idea that is perceived. The version of the thing which comes to exist in the social world is constructed by the way it is described. (Bryman, 2016. pp.531)

Discourse analysis then argues that there is no single external reality waiting to be discovered, and that instead there is a constructionist process of creating reality. It argues that the process of discourse entails selecting a particular version of something from many possible versions in order to build-up a particular definition of reality. Scott describes the purpose of discourse as “establishing one version of the world in the face of competing versions” ((Gill, 2000) in(Bryman, 2016, pp.534))

Discourse analysis is often performed on spoken communication, but it is more flexible than techniques such as Conversational Analysis and can be productively employed on text documents and multimedia sources such as television news broadcasts.

The fact that many different definitions of the nature and purpose of privacy exist suggests that any given professional body or library authority will have selected a particular vision of it, and that it is this that their discourse, what they have said about it, will embody. As described by Findlay, discourse analysis “studies the way in which objects or ideas are spoken about” (1987 cited in (Frohmann, 1994)) . This suggested that it might be a productive technique to employ in this context.

Discourse Analysis should be differentiated from the technique of Critical Discourse Analysis which has evolved from it. Whilst sharing the techniques of Discourse Analysis, Critical Discourse Analysis takes further the approach of Foucault in studying the way that social relationships and social power are made manifest in discourse. It treats the process of discourse as an exercise of power to establish a particular reality within a given social group and attempts to trace the power relationships and methods involved in this (Bryman, 2016). The current study is not primarily concerned with identifying the power relationships between library authorities, librarians, and library users in regard to privacy. The study is rather aimed at exploring what idea of privacy public library policy constructs, and how this reflects those constructed by the professional bodies. Whilst, therefore, it was decided that discourse analysis was a promising technique to apply in this case, it was decided not to apply Critical Discourse Analysis as its main concerns differed from those of the study.

The technique of discourse analysis has not yet achieved widespread penetration of library and information science research. Although it has been employed in some studies it remains a relatively new and underutilized technique. The technique does offer some advantages. Fairclough, discussing the application of the technique to texts, argues that “texts constitute a major source of evidence for grounding claims about social structures, relations and processes”. He also observes that in many cases social scientists dealing with large scale interests – such as class – are often basing their analysis on texts rather than the phenomenon itself, whether or not they acknowledge this (Fairclough, 1992).

The current studies application of this technique to privacy then extends the penetration of the technique in LIS research and to a topic it has yet to be used to investigate.

3.3 Coding:

The initial coding was done through an analysis of the documents obtained from CILIP, IFLA, the ALA and the Information Commissioner. It was decided not to establish an a priori coding scheme, but rather to allow coding to emerge from an analysis of the documents. This was due to the very broad range of theoretical formulations of privacy which we have discussed previously. It was felt that to establish a coding scheme in advance would encounter difficulties in covering the entire range of possible standpoints and might have the potential to bias subsequent analysis.

A process was therefore adopted of analysing each of these documents and identifying elements within them that were felt to be relevant to privacy - whether in terms of being elements of what the organisation expressed privacy to consist of, or things for which they felt privacy was a prerequisite. The software package Nvivo was used to assist in this process. Nvivo allows the application of coding to specific sections of text in documents by a process of assigning nodes to them. Nodes are groupings of sections of a text or texts which relate to a particular idea, subject or theme. A given section of text can have a node or nodes applied to it, reflecting the ideas embodied in it. These nodes can then be used to retrieve all sections of a text or texts which relate to a particular idea or ideas.

3.3.1: Initial coding:

An initial set of codes therefore evolved through the process of studying these documents. This was an iterative process. Codes developed as a result of studying a given document or documents for a particular organisation were used in coding future documents. New codes developed from these documents were then used in a subsequent pass through earlier documents. This was continued until a stable set of codes resulted. Not all of these codes were present in documents from all of the organisations, representing that there were some differences between them in their discussion of privacy. There were however definite points of commonality between organisations. (See 5.1 for further discussion).

The final set of codes which resulted from this iterative process consisted of twenty-one codes. On further examination it was felt that two of these reflected concepts which could be regarded as subordinate elements of a third. These were therefore coded within Nvivo as sub-nodes of that node.

The twenty one codes and sub-codes were:-

- *Right to freedom of access/ open enquiry* – the right to access information, to enquire and to engage with and consider ideas without hinderance.
- *Freedom from scrutiny/surveillance*
- *Confidentiality*
- *Unrestricted and equal* – the principle that everyone should have the freedom to access information without being treated differently simply because they belong to a particular group.
- *Right to be informed* – The right of patrons to know what information is being obtained and retained about them
- *Right to choose* – The ability of patrons to choose not to use those services which require them to disclose information, or to have that information destroyed or deleted at a later date when they have stopped using the service
- *Right to know* – Refers to the right of patrons to expect libraries to be able to provide help and advice to them in regards to how to protect their privacy.

- *Legally bound* – The recognition that a patron's information will be protected as required by law, and that it will only be disclosed as part of a properly legally authorised process.
- *Fundamentality* – Recognition of privacy as a fundamental right.
- *Responsibility of everyone*
- *Reciprocity* - referring to library patron's having a duty to respect the privacy of other patrons
- *Actively protecting* – defining the practical measures that will be taken to protect the privacy of patrons.
- *Limited collection* – Referring to the collection of only enough information for service provision, and no more
- *Anonymity* – the right not to have to give a name in order to access information or services.
- *Intellectual freedom* – which had two sub-ordinate codes
    - *Freedom of expression*
    - *Freedom of ideas*
- *Personal/personally identifiable data*
- *Autonomy*
- *Proportionality* – The idea that methods and degree of surveillance used should be in proportion to the harm that they sort to prevent.
- *Bodily privacy* – the right to control access to an individual's physical body, only observed in the case of documents from the Information Commissioner.

3.3.2: Coding of library authority documents:

The objective of this study was to determine the degree to which public library policy in Scotland reflected the dimensions of privacy that had been identified as relevant in the context of public libraries. Discourse analysis presupposes that the version of an idea or object that exists in social reality is constructed from the way it is spoken about.

The coding's which had been derived from study of the documents produced by CILIP, IFLA, the ALA and the Information Commissioner can therefore be taken as being representative of what they believe privacy is in the context of a library. Therefore it was proposed to study the documents sourced from Scottish library authorities to identify the extent to which these dimensions were found in the version of privacy which was constructed by the discourse of the library authorities.

These documents were therefore subjected to a similar analysis as the professional body documents had been, but in this case the set of codes which had been derived from the latter were used in the assigning of nodes in Nvivo. This having been done it was possible to carry out searches of the corpus of documents in order to retrieve instances of the various identified dimensions of privacy. This allowed the extent of the reflection of these elements in public library policy to be recorded and the degree of reflection of the various constructs of privacy from the professional bodies to be examined.

5.0 Professional bodies, the Information Commissioner, and privacy

Two related sets of data emerged from this study. The first had regard to the conceptualisations of privacy of the bodies which represent librarianship as a profession, and that of the Information Commissioner who has legal responsibility for some aspects of what we might term informational privacy. These representations were then used as the basis of an assessment of how these concepts were represented in Scottish Public Library policy

5.1 The Professional organisations and privacy:

Examination of documents from IFLA, CILIP and the ALA revealed that there were distinct and well-defined concepts of privacy held by the various professional organisations. It was also observed that there was a considerable degree of commonality between the views held by the three organisations. Of the 21 identified elements, nine could be considered to be shared by all three bodies. These elements were:-

- *Freedom of Enquiry/ freedom of access to information*
- *Confidentiality* of the interaction between library staff and patron.
- The patron's *Right to be informed* of what information would be held by the library. The ALA's assertion that "Lack of privacy and confidentiality has a chilling effect on users' choices", closely mirrors CILIP's view that "People must be free to access and use information and to express their ideas without fear of reprisal."(Chartered Institute of Library and Information Professionals, 2015)
- The patron's *Right to choose* to not use a service which requires them to give out personal information, or to choose to have that data destroyed when they chose to cease to use the service
- The *Right to know* how to protect their privacy – that is, an expectation that it was the role of the librarian to advise patrons on how they can protect their privacy and to provide assistance to them in this task. IFLA's Statement of Privacy in the Library Environment calls specifically for education in the protection of the privacy and personal data to be included as part of information literacy training for library users. The ALA similarly states that "Librarians must educate their users through a variety of

learning methods that provide the information and tools adults and minors need to protect their privacy and the confidentiality of their own PII. [Personally Identifiable Information]"(American Library Association, 1991)

- The concept that privacy was *legally bound* - That the law both acted, and required librarians, to protect the privacy of patrons but also to establish qualifications to that right and to define circumstances under which librarians might be legally expected or required to divulge information. There was a recognition that privacy did not provide protection for acts which were themselves illegal. There was also, for all three organisations, an understanding expressed that any surveillance of patrons information use should be based on a suspicion of wrongdoing by a specific individual and a rejection of the ethical legitimacy of blanket surveillance or reporting. All three professional bodies also saw the requirement to operate within the law as being a reciprocal one. That any surveillance should only be done through a formal, legal process which established both a specific individual to be targeted and the existence of a particular suspicion of wrongdoing on that person's part. CILIP observe that: "They [librarians] will be subject to other Acts [than the Data Protection Acts] that give the police and security agencies rights to demand access to personal data within specific contexts…", and advise their members that it is important that their libraries are legally compliant. In the same guidance however CILIP also remind members that they should also have regard to the ethical principles of their profession, and specifically to the statements in their ethical code in regard to respect for user confidentiality and privacy(Chartered Institute of Library and Information Professionals, 2016) . They have also advised members that they have a duty to balance "within the law" both the need to respect the confidentiality of patrons and the public good(Chartered Institute of Library and Information Professionals, 2013a). IFLA also express the view that privacy cannot be absolute. They observe that it is not possible to completely avoid government access to government agencies having access to library user's data or to their communications activities (such as Internet searches). They stated that it is therefore necessary for library services to ensure that this is based in "legitimate principles" and "necessary and proportionate to legitimate aims", pointing to the "International Principles on the Application of Human Rights to Communications Surveillance" as a good basis for defining the ideas of legitimacy and proportionality (International Federation of Library Associations, 2015). IFLA also suggest, not just in relation to privacy but more broadly in the spectrum of information law, that their members should be prepared to offer critique of existing law, and to take part in the improvement of both the drafting and implementation of relevant law.

- That patron privacy was to be a*ctively protected***.** CILIP's Code of Professional Practice indicates members are expected to:- "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." (Chartered Institute of Library and Information Professionals, 2013a). Similarly , the third principle of the ALA's code of ethics states that members "protect each library user's right to privacy and confidentiality"(American Library Association, 2008)
- Each of the three organisations also made explicit statements that all groups should have, in principle, u*nrestricted and equal* access to information and that any monitoring of information usage which was targeted at particular social groups as a whole was an unequal breach of their privacy which would undermine this principle.
- Although only CILIP explicitly identified privacy as an essential prerequisite of *intellectual freedom*, it could be argued that the ALA's expressed commitment to privacy as a requirement for *freedom of ideas* and *freedom of expression* are, in essence, elements of the same concept. IFLA also indicated that they considered privacy to be essential for *freedom of expression*.
- That there should be *limited collection* of information about individuals. CILIP argue that the best way to preserve patrons' privacy is simply to not have the information in the first place. The ALA and IFLA take a similar position, arguing that libraries should only be regularly asking for the information they actually need to fulfil the libraries mission, and no more.

Of the remaining identified privacy-related elements, which were not shared by all three bodies, three were observed to be shared by two:-

- Both the ALA and IFLA explicitly indicated that they felt that information users in general should be *free from scrutiny or surveillance* of their use of information.

- *Fundamentality* – both the ALA and IFLA made explicit statements that they considered privacy to be a fundamental right of all patrons
- Both the ALA and CILIP made specific reference to the need to protect and prevent the disclosure of data which could be used to identify a specific individual. The ALA referred to this as *"personally identifiable data"* whilst CILIP identified this as ***"**personal data**"***, the same term as used in the UK Data Protection Acts.

There were, however, some concepts which emerged only in the context of a single body:-

- *Responsibility of everyone* – the proposition that all staff within a library, professional and non-professional had a responsibility to ensure the privacy of patrons was explicitly mentioned only by the ALA
- *Reciprocity* which was identified from the ALA's concept of privacy - The idea that patrons had a responsibility and duty to respect and observe the privacy of other patrons. Neither CILIP nor IFLA made mention of this concept, nor did they address expectations of patron conduct or perceived duties of patrons.
- The concept of *proportionality* was only explicitly addressed in documents sourced from IFLA. They identified this as the principle that any surveillance should be directly proportional to the nature and extent of an existing suspicion of wrong-doing by individuals.
- Only CILIP made any mention of the concept of *autonomy*, identifying privacy as an element of the autonomy of individual patrons.

These privacy elements, and the bodies in whose discourse they were found are summarized in Table 1 below:-

Table 1: Summary table of privacy elements across professional bodies.

Elements of Privacy	Professional Body		
	ALA	CILIP	IFLA
Right to Freedom of Access/ Open Enquiry	√	√	√
Freedom from Scrutiny/Surveillance	√		√
Confidentiality	√	√	√
Unrestricted and Equal	√	√	√
Right to be informed	√	√)	√
Right to choose	√	√	√
Right to know	√	√	√
Legally Bound	√	√	√
Fundamentality	√		√
Responsibility of everyone	√		
Reciprocity	√		
Freedom of Expression	√		√
Actively Protecting	√	√	√
Limited Collection		√	√
Anonymity		√	
Intellectual Freedom		√	
Personal/personally identifiable Data	√	√	
Autonomy		√	
Proportionality			√
Freedom of ideas	√		

5.2 The Information Commissioner and privacy:

Whilst the professional librarianship bodies had a remit which encompassed the world of information generally, the Information Commissioner's role, as established in UK law, is concerned with the protection of what is defined as personal data. This is information which, either by itself or in combination with other information about an individual might serve to identify them. It was expected then that the Commissioner's role would focus primarily on what might be described as "informational privacy". This was indeed found to be the case, it was observed that there was a distinct subset of privacy elements which were held in common between the Information Commissioner and all of the professional bodies:-

- The individual's *right to be informed* of what information was collected about them.
- Their *right to choose* to have information destroyed or deleted when they ceased to use a service, and to make an informed choice whether or not to use a service based on how it would affect their personal information
- The individual's *right to know* how to protect their privacy
- That the protection and disclosure of individual's personal data was *legally bound*
- That personal data should be *actively protected* and kept secure.

In addition to these elements common across all four bodies, it was also found that there were also a number of elements which, whilst not shared by all three professional organisations, did emerge from both the Information Commissioner's discourse on privacy and that of the majority of professional bodies:-

- The idea that some information was p*ersonal/personally identifiable data,* fundamental to the information commissioners role, was one that they shared with the ALA and CILIP
- That, in principle, individuals should have *freedom from scrutiny/surveillance***,** also expressed by IFLA and the ALA
- *Limited collection* – expressed also by CILIP and IFLA.

There were also two privacy elements which had been identified in CILIP's discourse which also recurred in that of the Commissioner.

- The idea that privacy is necessary in order for people to exercise *autonomy* over their own lives.
- The principle that people should be able to maintain their *anonymity*. CILIP addressed this explicitly in the context of digital information, arguing that Librarians and information professionals supported and educated information users in how to maintain their anonymity when accessing information. The Commissioner, meanwhile, indicated that over-collection of data harmed the right of individuals to be anonymous – "An important aspect of privacy protection is sustaining the right to interact with organisations without declaring one's identity."

There were, then, a subset of privacy elements which were observed to be shared between the Commissioner's view and those of the various professional bodies. It was also observed that there were a number of elements present in the latters' discussion of privacy which did not appear in that of the Commissioner:-

- The Right of *freedom of enquiry/freedom of access* to information in a general sense.
- The concept of *unrestricted and equal access* to information.
- Privacy as a perquisite for *intellectual freedom, freedom of expression* or *freedom of ideas*.
- *Confidentiality* – in the context of the reference enquiry and of the individual's information use.
- An explicit statement that the privacy of a service's users was the *responsibility of everyone* who worked for it.
- The ALA's concept of *reciprocity*
- The *fundamentality* of a right of privacy.
- The *proportionality* of surveillance measures.

Two additional elements were identified from the Information Commissioner's documents:-

- *Bodily privacy*: related to the individual's ability to control access to their own body in the context of blood, urine and other samples, and also to control the observation of those parts of their body society generally considers to be private**.**

- *Location and tracking*: The Commissioner identified measures that could be used to identify the location of an individual, or to track their movements, as a risk to their privacy – especially in those cases where these measures made a record of those movements.

Bodily privacy which was felt not to be relevant to the library policy environment, and *location and tracking* did not appear in the views of any of the librarianship bodies.

Table 2 below extends Table 1 to include the privacy elements identified as part of the Information Commissioner's conceptualisation, along with those of the professional bodies.

Table 2: Summary table of privacy elements across professional bodies

Elements of Privacy	Professional Body			Information Commissioner’s Office
	ALA (Prevalence)	CILIP (Prevalence)	IFLA (Prevalence)	
Right to Freedom of Access/ Open Enquiry	√	√	√	
Freedom from Scrutiny/Surveillance	√		√	√
Confidentiality	√	√	√	
Unrestricted and Equal	√	√	√	
Right to be informed	√	√	√	√
Right to choose	√	√	√	√
Right to know	√	√	√	√
Legally Bound	√	√	√	√
Fundamentality	√		√	
Responsibility of everyone	√			
Reciprocity	√			
Freedom of Expression	√		√	
Actively Protecting	√	√	√	√
Limited Collection	√	√	√	√
Anonymity		√	√	√
Intellectual Freedom	√	√	√	
Personal/personally identifiable Data	√	√		√
Autonomy		√		√
Proportionality			√	
Freedom of ideas	√			
Bodily Privacy				√
Location Privacy				√

5.3: Summarising the professional views of privacy:

As has been observed there are distinct similarities between the elements of privacy identified in documents from the three professional organisations. Looking at the appearance of these elements in their discourse a number of areas of consensus can be seen to emerge.

5.3.1 The purpose of privacy in libraries:

All three of the professional bodies can be seen to demonstrate a strong convergence in terms of the reasons that the privacy of library patrons matter. All of them hold that patrons have a right to freely access information and to make enquiries into matters of interest or concern to them. The privacy and confidential nature of these enquiries are seen as vital guarantees of this freedom

5.3.2 The nature of privacy in libraries:

Likewise, a consensus exists that part of that privacy is that what passes between patron and librarian in regard to their information needs and the information that they consult should remain confidential. This also extends to a general agreement that libraries should not be asking for information that isn't absolutely needed.

CILIP and IFLA made mention of facilitating the anonymity of patrons. In a statement on digital privacy CILIP observed that librarians have become more involved in educating users in ways of protecting their privacy and anonymously accessing information. IFLA's Statement on "Libraries and Intellectual Freedom", asserts library users have rights to both privacy and anonymity.

5.3.3 Qualified privacy:

All of the professional bodies agreed that the right to privacy was not absolute, all recognising that there were situations where there was a requirement in law where the privacy of individual library users might have to be breached.

The ALA showed signs of accepting that privacy could not necessarily be completely inviolate. The language with which they addressed this showed some distinct differences to that of CILIP or IFLA however. The ALA's "Policy concerning Confidentiality of Personally Identifiable Information about Library Users" argues that government interest in the library use of individuals equates a person's reading habits with their future behaviour, and describes this as being both "dangerous" and "fallacious". Whilst their description of libraries as "impartial resources" that provide information to all is not dissimilar to the views of CILIP and IFLA their position on defending this is framed in rather more uncompromising terms. They state that they oppose "any use of governmental prerogatives that lead to the intimidation of individuals or groups and discourages them from exercising the right of free expression" and that the ALA "encourages resistance to such abuse of governmental power".

The tenor of ALA's discourse here appears to represent a much more absolutist approach than is apparent in CILIP and IFLA's tone. Whilst CILIP and IFLA appear to portray the qualified nature of privacy as something to be negotiated, societally agreed, explained and carefully weighed, ALA's discourse appears more to view it as an "unfortunate necessity". Their choice of language and tone seems to portray a steadily encroachment by government and the law into an area in need of defence. Whilst sharing the other bodies views that privacy is necessary for intellectual freedom the ALA strike a more confrontational tone in their discussion of this principle.

It is possible that this is a result of ALA's ongoing involvement in campaigning against various measures from the Library Awareness Program to the USAPATRIOT Act, or from a more openly polarised public debate in the United States about surveillance and privacy, or from a generally more individualistic attitude in American society. It is outside the scope of the current research to attempt to determine how this difference has evolved, but the fact that it exists emerges clearly from the examination of the ALA's treatment of privacy.

5.3.4 Privacy and library users:

The theme of educating library users regarding privacy could be seen in all three bodies' discussion of privacy.

There was likewise a strong consensus between all three organisations in stating their belief that users had the right to know what information was being collected about them, and to have incorrect information corrected, as well being able to make informed choices about whether or not to use a particular service based on its privacy implications.

There is then, a clear consensus not only that libraries should "do" privacy, but that it is a necessary prerequisite of a fundamental aspect of the library mission. Equally that privacy is not an absolute right, but that it is subject to qualifications in terms of the law, and the good of wider society (if seemingly somewhat reluctantly on the part of the ALA). There is also a strong degree of consensus of what this should mean in terms of how libraries interact with users. Comparison of the positions of the professional bodies with that of the Information Commissioner identified distinct similarities in this latter regard.

5.3.5 The Information Commissioner's view of privacy:

As previously observed, there was a subset of privacy elements on which there was a consensus between the Information Commissioner's view of privacy and that of the professional bodies. These primarily centred around the collection, use and protection of people's personal information. That this should be the case is unsurprising, given that the Commissioner has a specific remit to administer the UK's main law concerning personal data – the Data Protection Act. That the Commissioner's documents were seen to espouse the principles of giving people knowledge of what personal information was collected about them and control of how it was used is perhaps unsurprising. Neither is their espousal of the importance of collecting only the minimum data on individuals needed to provide a service, or of taking active steps to protect that data once it was collected. Similarly a strong emphasis on requesting and disclosing data only within the bounds of what was legally permitted was observed. This also fed into a position that as far as was possible people should be free from surveillance of their activities or their physical location.

It was notable that the Commissioner, similarly to CILIP and IFLA, appeared to hold the view that people should have the opportunity to be anonymous. The Commissioner's observation that it was a matter of concern that people's anonymity was threatened by the insistence on collecting names where the real goal was establishing an entitlement to a service paralleled IFLA's assertion of a right to anonymity for information users (Information Commissioner's Office, 2014).

The Commissioner also appeared to advance the individual's *right to know* how to protect their privacy quite strongly. Indeed, the Privacy Toolkit was specifically aimed at educating people as to how they could protect their privacy.

Whilst much of the practical elements of the Information Commissioner's expressed concept of privacy showed a strong commonality with those of the professional librarianship bodies, the rationale for why privacy mattered differed. The discourse of the professional organisations concentrated on the importance of privacy as a protector of open enquiry and intellectual freedom. By contrast the Information Commissioner's office expressed the view that privacy, and the protection of people's personal information mattered because of the value of the personal information itself, and the damage that could be done by information which was incorrect, or not properly protected.

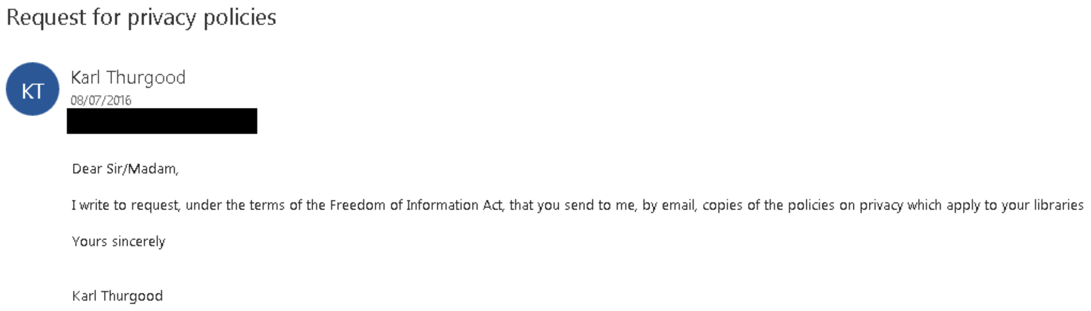
5.3.6: Terms of reference of the Information Commissioner:

As we have seen previously, there is no single definition of what privacy is, so it should not be too unexpected that there are similarly divergent viewpoints on why it matters. The lack of discussion by the information commissioner of privacy as a prerequisite of intellectual freedom should not be seen then as an omission. Rather it reflects the way that the Commissioner's concept of privacy is shaped by the context in which it is framed. Whilst the librarianship bodies view privacy from the perspective of their missions, the Commissioner's mission is – as established in statute – very specifically and concretely framed as overseeing the protection of personal data. This then will both direct the way they view privacy, and establish the boundaries in which they consider it. Not being empowered to consider issues of intellectual freedom and open enquiry, it is unsurprising that the Commissioner's discussion of privacy does not extend to those areas.

6: Library authorities and privacy:

Freedom of Information requests were sent to all 32 Library Authorities in Scotland, asking them to provide the policy documents which related to privacy within their libraries. The email used to make these requests is reproduced in Figure 1 below.

Figure 1: email request for privacy related documents.



Request for privacy policies

KT

Karl Thurgood
08/07/2016
[redacted]

Dear Sir/Madam,

I write to request, under the terms of the Freedom of Information Act, that you send to me, by email, copies of the policies on privacy which apply to your libraries

Yours sincerely

Karl Thurgood

These were then analysed using a coding scheme which utilised the privacy elements identified in the first phase.

6.1 Response rate of library authorities:

Responses were received from 26 of the 32 library authorities in Scotland. This represented a response rate of 81.25%

6.2: Range of responses from authorities:

A wide variability in the responses from different authorities was observed. This was apparent both in terms of what was sent, and the number of documents which were sent in response to the query. Whilst the majority of responses consisted of between one and four documents, some were significantly larger. The largest number of documents received was from Authority 2, which included twenty distinct documents, or links to documents, in its response. Of these, nine were found to be membership forms for various services operated through the library, presumably due to their included data protection statement. A further five were privacy/data policies of other organisations and providers of services, such as

Twitter and Facebook. Although included in the total of documents received, these were not subject to analysis as they were outside the control of both the authority and its libraries. In total, eighty four documents were received from the twenty five responding library authorities.

Table 3, below, shows the breakdown in response rates by authority (N/R indicates at non-responding authority):-

Table 3: number of documents received by authority number

Authority Number	Number of documents received
1	1
2	20
3	N/R
4	3
5	1
6	4
7	1
8	5
9	5
10	9
11	1
12	2
13	N/R
14	2
15	1
16	3
17	4
18	1
19	1
20	N/R
21	1
22	1
23	6
24	N/R
25	N/R
26	1
27	1
28	N/R
29	4
30	2
31	2
32	2

There was a similar variety observed in the nature of the documents comprising responses. Whilst the most commonly submitted type of documents were those identified as Data Protection statements many other types of documents were also sent. These included, but were not limited to membership application forms, web site “cookie” statements and records management policies. For example, whilst Authority 26 sent only an Acceptable Use Policy (AUP) for their publically accessible computer systems, Authority 29 sent an AUP along with their Information Security Policy, Information Strategy and Privacy Policy. By contrast, Authority 7 responded solely by means of a letter stating that they observed the Data Protection Act in regard to information given to them as part of a membership process, and that all browsing data and history was cleared when a user logged out from a browsing session.

The table below, Table 4, shows the types of documents, and number of authorities which sent each document type:-

Table 4: Document types by number of authorities submitting

Document Type	Number of authorities sending
Data Protection Policies	14
Privacy Policy	2
Letter Confirming authority follows Data Protection Act	1
Website Privacy Statements/Terms and Conditions	6
AUP/ Acceptable Use Guidelines	10
Cookies Statement	2
Information Security Policy	2
Library and Information Service Management Rules	1
Freedom of Information Policies	2
Membership forms	3
Clear Desk Policy	1
Social Media Guidance/ Policy Governing the use of communications systems	2
Records/ Archive Management Policies	2
Information Strategy	2
Customer Charter	2
Membership Booklet	2
CCTV Code of Practice	1
Accessible Information Policy	1
Details of remote data-hosting facility	1

Of the two submissions identified above as privacy policies, on closer examination, one proved to be primarily concerned with implementing the requirements of the Data Protection Act and as a result was similar in content to those identified by other authorities as Data Protection Policies.

It can be seen from this that very few authorities had a privacy policy for their libraries which was identified as such. Indeed, it was the case that very few of the documents received were specific to the library context. Most were those of the overall authority –

whether this was a local authority or a community trust or other arms-length organisation, covering all the services which they provided.

Of those documents submitted the ones which were specific to the library context were membership forms, two membership booklets, the Acceptable Use Policies, and a Service Management Rules document.

6.3: Coding of privacy concepts in library authority documents:

As indicated above, coding was carried out of the documents from the library authorities in Nvivo to identify the privacy elements which were expressed in the documents, using the privacy elements previously identified.

The results of this coding, by library authority, is summarised in Table 5. (Authorities who did not respond have been omitted from the table)

Table 5: Privacy Elements in Library Authority documents.

Authority Number	Privacy Element												
	Right to Freedom of Access/ Access to information	Freedom from Scrutiny/ Surveillance	Confidentiality	Unrestricted And equal	Right to be Informed	Right to Choose	Right to know	Legally bound	Fundamentality	Responsibility of everyone	Reciprocity	Freedom of Expression	Actively Protecting
1													
2					√			√			√		
4					√			√		√			√
5					√	√		√					√
6	√		√		√		√	√		√		√	√
7								√					
8			√		√		√	√		√			√
9			√		√	√		√		√			√
10			√		√	√		√			√		
11					√	√		√					√
12					√			√					
14					√		√	√					√
15					√	√		√					√
16					√	√		√					
17			√		√								
18					√	√		√		√			
19					√			√					
21					√	√		√					√
22					√			√			√		
23			√		√			√		√			√
26					√		√				√		
27					√	√		√					
29			√		√		√	√		√			√
30					√			√					
31					√	√		√		√			√
32	√				√	√	√	√					√
No. held by	2	0	7	0	23	11	6	22	0	8	4	1	13

Authority Number	Privacy Element							No. of Privacy Elements expressed by each authority
	Limited Collection	Anonymity	Intellectual Freedom	Personal/ Personally Identifiable Data	Autonomy	Proportionality	Freedom of Ideas	
1				√				1
2				√				4
4	√			√				6
5				√				5
6								8
7				√				2
8	√			√				8
9				√				7
10				√				6
11				√				5
12				√				3
14	√							5
15								4
16				√				4
17				√				3
18	√			√				6
19				√				3
21	√			√				6
22								3
23	√			√				7
26								3
27	√			√				5
29	√			√				8
30				√				3
31	√			√				7
32				√				7
No. authorities held by	9	0	0	20	0	0	0	

6.4 Privacy in public library policies:

Looking at the documents provided by the various library authorities, whilst individual differences between authorities existed there was a discernible pattern in the privacy elements most commonly expressed in policy. It was also apparent that whilst there were similarities between their expressed conceptualisations of privacy and those of the professional bodies, this was not as strong as with that of the Information Commissioner. There were also a number of other notable features observed not only in what was discussed in the context of privacy, but in the way that the authorities chose to discuss it.

6.4.1: Privacy elements in library policy:

As shown in Table 4 above, although none of the privacy elements were observed in the submissions from all the authorities there was a group of identified privacy elements which were observed in more than half of the authorities. These were the idea that some information should be considered to be *personal* or capable of identifying an individual person – (found in the case of 20 of 26 authorities (77%)), the individual's *right to be informed* of what information related to them was being collected (23 of 26 (88%)) , and the idea that privacy was *legally bound* (22 of 26 authorities (84%)), and that privacy should be *actively protected* (13 of 26 authorities (50%)) These elements were ones that were shared with both the professional organisations, and with the Information Commissioner.

A definition of what constituted personal information was not offered by all authorities. Where a definition was offered it followed closely the form given within the Data Protection Act of personal information being that by which "an individual can be identified from or which together with other information in the possession of or likely to come into the possession of the data controller could serve to identify an individual".

Two distinct interpretations of the *right to be informed* were observed amongst the authorities. One group discussed this idea only in terms of the subject access requests provided for under the Data Protection Act, essentially holding that they only needed to tell people what information had been gathered about them *if* they directly asked for it. This school of thought is exemplified by Authority 30’s Data Protection statement which states: “The Data Protection Act allows you to find out what information the Council holds about you on computer and some paper records. This is called the ‘right of subject access’. You can see the information that the Council holds about you by making a ‘subject access request’ ”. Authority 23 arguably took this further observing not only that people only needed to be told when they asked that information was gathered about them, but that the provisions of the Act did not prevent them from holding information about an individual that the individual did not know about, provided that it was notified to the Information Commissioner.

By contrast the other group of authorities held that people should be informed what information was being gathered about them and what it would be used for at the time it was gathered. Authority 14’s Privacy and Personal Information Statement advises:-

“We keep a limited amount of personal information about our customers. This is restricted to:-

- Name - required
- Address- required
- Age – if provided
- Gender – if provided
- Language – if provided
- Telephone numbers – if provided
- E-mail addresses – if provided”

going on to detail the information about patrons’ library use kept by their Integrated Library System.

In a similar fashion Authority 10’s Data Protection Policy indicated that individuals must be made aware of what would be done with the personal information that the Council gathered about them at the point where the Council acquired it. Their policy also indicated that all forms where data was gathered should have a Data Protection Statement that explained why the Council was gathering the information, what would be done with it and whether, and with whom it might be shared.

The idea that privacy operates within legal bounds, that there are both legal requirements to protect individuals privacy as well as situations where there exist legal authority or requirements to breach that privacy, was found to be present in the majority of responses. 22 of 26 (85%) of responses contained some discussion of legal bounds. The most common, found in all 22 cases, was a statement that the personal data provided to the authority would only be used or processed in accordance with the law. These statements varied in character from Authority 15's observation that: "…if you choose to book tickets or workshops, register to be kept up to date with our events or provide your personal data in any other form, we will only process your data in accordance with the relevant legislation", to more detailed statements such as Authority 23's:-

"This Policy and Code of Practice sets out how the Council ensures it complies with the 1998 [Data Protection] Act to ensure that personal information about people is:

- Processed in accordance with the 1998 Act
- Collected and used fairly
- Stored safely and securely
- Not disclosed to any third part unlawfully."

In all 22 cases which discussed the idea of privacy as a legal responsibility the emphasis, explicitly or implicitly was on the Data Protection Act and the authorities' duty to abide by this as the primary source of this responsibility. Whilst these 22 authorities clearly noted that they had a legal duty to protect the personal data of individuals, there was less unanimity where it came to the other aspect of legal bounds which was identified by the professional bodies. There was less emphasis seen in the submissions from the library authorities of an importance being placed on the existence of a clear legal process and legal authority for individual disclosure requests by law enforcement and security agencies. The majority of authorities did include a statement confirming that they would disclose information "where legally obliged to do so", and in some cases "where permitted to do so".

There were differences in emphasis observed between different authorities on this – some emphasising that the law required certain information to be disclosed, and others giving a stronger emphasis on the disclosure of information being something that the law allows them to do.

For example, Authority 22’s Library Membership booklet states that patron’s use of the internet will be monitored and that these records may be passed to the police or other agencies “as permitted by law”. Authority 21’s Privacy Statement indicates that they are required to protect public funds and as a result: “It [the authority] may share information provided to it with other bodies responsible for auditing or administering public funds, in order to prevent and detect fraud. By contrast Authority 14’s website Privacy Statement indicates that they may “be legally obliged” to share information if it “could be used to prevent or detect a crime”. This latter formulation suggests a view of the presumption being against disclosure as a matter of course, whereas Authority 21’s position tends towards certain disclosures of information being made as a matter of routine.

In general there was less emphasis found in the authorities’ discussion of the importance that the Professional Bodies had placed on disclosure to Police or security organisations being targeted and by means of a specific legal process. The majority of authorities simply stated that they would disclose information that might help to detect or prevent crime, but with few exceptions did not elaborate on how this was done. The only exceptions observed to this were Authorities 23 and 31.

Authority 31’s Data Protection Procedure outlined that requests for information in relation to detection and protection of crime should be made in writing and that an audit trail of the request and the information disclosed should be maintained. Authority 23 were the only one to express a concurrence, in their Data Protection Policy and Code of Practice, with the professional bodies view that any disclosures should be in regard to particular individuals. They also indicated in their CCTV Code of Practice that in this context that they expected all requests from Law Enforcement agencies to be made in writing.

The remainder of the 22 authorities that discussed this topic merely stated that they would make disclosures to police or security agencies as “permitted” or “required” by law, but did not express anything comparable to the expectations of the professional bodies of how these should be regulated.

The only other privacy element which was observed in large numbers in the responses from library authorities was that of *actively protecting* privacy. Whilst all of the respondents made some mention of protecting personal data, only in 13 (50%) authorities was reference made of measures to do so which were felt to qualify as active protection of this data. This discussion varied in scope and strength considerably.

Authority 7 notes in their Acceptable Use Policy that the Internet History and Cache on individual computers is cleared on the user logging out protecting their confidentiality. This represents only a very weak degree of protection given the same documents implication elsewhere that the authority’s system maintains a log of all sites visited which can be accessed by staff.

By contrast Authorities 7 and 29 maintained authority-wide Information Security policies, and 7 and 10 Information Management Strategies, which established very detailed regimes for maintaining the security of “personal data” in a wide variety of situations and contexts. The majority of cases of active protection fell somewhere in between these two extremes in thoroughness. Once again, the rationale given for protecting this data was often traced back to the Data Protection Act, with several authorities referencing the Acts requirement that personal data is “held securely”. In the case of Authority 7 and 10 a “proprietorial” interest was noted, with Authority 10 observing in its Information Management Strategy that information held by the Council, including personal information regarding the users of its services, was an asset held by the Council, in the same sense as its buildings and equipment. The protection that these particular strategies gave to individuals against misuse of their information seemed in many ways a side-effect rather than a primary goal. It was clear in most cases for the Data Protection Act to serve as the primary rationale for active protection of data, with most authorities describing their measures to protect “personal information”, and focusing on information held electronically or in paper filing systems.

Only 9 of the 26 authorities (35%) expressed a commitment to the principle of *limited collection* of information. These 9 authorities stated that they sought to collect only the minimum information needed to provide a given service, whilst the remaining responding authorities indicated in various ways their commitment to the Data Protection Act's stipulation that information collection should not be excessive.

Only 8 of the 26 (31%) authorities explicitly identified that the protection of privacy or the personal information of users as the *responsibility of everyone* who might come into contact with the users or their data. A few of the remaining authorities identified ensuring compliance with the Data Protection Act as the responsibility of specific members of staff. The remainder merely stating that the authority in general was committed to complying with the Act, or "relevant legislation" concerning the processing of personal data.

In terms of service users *right to know* how to protect their privacy the pattern that appeared was, like *limited collection*, of an element not expressed by the majority of authorities. Only 6 of the 26 authorities (23%) made any references to ways in which individuals could preserve their privacy. As well as being a relatively uncommonly expressed element, it was found that it was one which was relatively weakly expressed where it was found. In all 6 cases this element was expressed only in connection with online privacy.

In two of these it related solely or primarily to minors – Authority 31's Terms of Use Policy advising that they provided information for children and parents on safe internet use, and Authority 29's encouragement to parents and guardians to advise their children to be careful about interacting online with strangers and not to give out personal information such as their address online.

Both Authorities 26 and 32 advised that: "Broadcasting personal or private details over the network may lead to the receiving of unwanted mail or unwanted attention."

Whilst authority 6 advised that people not pass their personal details to websites they are not sure are safe, they do not indicate how this determination should be made.

Only three authorities provided any practical guidance, and two of these related solely to the authorities own websites. Authority 32 stated that they would inform users what information is collected on the authority's websites by means of cookies, and how to switch these off. This, however, only applies to those used directly by the authority and not those used by providers of embedded content on various pages. Authority 4 provided similar guidance but also links to information on how to manage cookies generally on various web-browsers.

Of all the responses, only Authority 14 provided any broader advice regarding protection of privacy online. Their Privacy and Personal Information document advised that it was possible for sites on the internet to gather information on users of library computers, and that the "private browsing" mode offered by some web browsers only covers information on the computer a patron is using. They were the only authority in the sample who advised of the existence of "anonymous" web-browsers – citing DuckDuckGo and Ixquick as examples. They also indicated that library staff were able to provide further advice on this topic. Whilst relating solely to online privacy this represented by far the strongest example of the *right to know* observed in Scottish public library policy.

Seven of the authorities (27%) discussed *confidentiality* but this was observed to be in a more limited sense than that which had been implied by CILIP and ALA. In these authorities responses confidentiality was seen to be treated as synonymous with the protection of information covered by the Data Protection Act, rather than the broader sense implied by the professional bodies which extends not just to information that could identify an individual but also to the nature of the information sought and/or used by an individual. In the case of one authority the concept of confidentiality was encountered only in the context of reinforcing that information regarding other employees of the authority should also be considered personal data and protected as per the Act.

Only one authority, Authority 10, was observed to mention the possibility of *anonymity*, and this was not in the context of users, but of a warning that internet access allowed patrons "access to" people whose identity could not be verified. This was the only mention of anonymity encountered in the responses, and was notable for presenting the idea in a solely negative light.

In the case of only four authorities (15%) was the principle of *reciprocity*, that there was a duty on library users to respect each other's privacy, observed. In all these instances it related specifically to Internet and computer use. It was observed in the Acceptable Use policies of Authority 10 which stated that users "must respect the privacy of others" and Authority 26 which enjoined that "Library Users must respect the privacy of other users, and refrain from attempting to view or read material being used by others". Similarly, the Library Membership booklet of Authority 22 lists amongst the things which computer users must not do "invade the privacy of others".

Freedom of ideas was only found to be addressed in one case, and then only implicitly and by way of noting its qualification. Authority 26 noted in its Acceptable Use policy that they believed that "the best interests of adult service users" were served by not using filtering software, but nevertheless advised that they did employ filtering to prevent access to "illegal and highly offensive sites".

The remaining elements of privacy which had been identified in the initial phase of this study – *freedom from surveillance/scrutiny*, *unrestricted and equal access*, the *fundamentality* of a right of privacy, *intellectual freedom*, *autonomy,* and *proportionality* – were not observed in any of the responses

A number of authorities provided Acceptable Use Policies, or similar documents, amongst their responses. It was noted that in none of these cases was a positive privacy of internet access for users of public access computers outlined. All, even Authority 14 -who had provided advice regarding keeping browsing activities private from other web-sites – indicated that the Internet activity of all users was logged, or monitored to varying degrees and extents. This policy of blanket surveillance of all users arguably represents a diametrically opposite view to that taken by all of the professional bodies, representing a pre-emptive "in case" approach which contrasts sharply with the professional view that such surveillance should only occur where there are pre-existing grounds for suspicion of illegal activity.

Only two authorities made mention any mention of a concept of *freedom of access to information*. In the cases of both Authority 6 and Authority 32 this was only found in their

Acceptable Use Policies in the context of internet access. It was also in this context that Authority 6 noted a commitment to *freedom of expression* – the only such mention found in this study. Whilst Authority 32 indicated their support for *freedom of access to information* they went on to observe that this was open to “misuse and abuse” and that their AUP had been produced to “safeguard the interests of the Council and the community”

6.5 Privacy in library authority policy: In summary.

As previously observed, only a minority of the documents identified by library authorities as relating to privacy within their libraries were identified as specific to the library context. Primarily they related to the broader context of the authority, whether this was a community trust or a local authority.

It is also the case that the majority of the policies in place were set out primarily in the context of the protection of personal data, in the sense identified by the Data Protection Act. Indeed, one authority provided only a letter indicating that they complied with the Data Protection Act in dealing with personal data given to them when taking out membership of their libraries. It is perhaps unsurprising then that a significant proportion of the documents submitted in response to the FOI query were identified specifically as Data Protection policies or statements. This focus on the requirements of the Act can also be seen to be reflected in the distribution of privacy elements across the different authorities’ policy backgrounds.

Only four elements were found to be expressed by more than half of the authorities surveyed. These elements – *personal/personally identifiable information*, *actively protecting*, *right to be informed* and *legally bound* – were elements which were also found in the privacy constructions of all three of the professional bodies, and the Information Commissioner. In these respects policy of library authorities reflected the conceptualisation of privacy held by the library and information management profession. It was noteworthy, however that all of these elements were identified by the library authorities in terms which, explicitly or implicitly, were positioned in terms of the concept of “personal data” expressed within the Data Protection Act.

Conversely a much larger number of the privacy elements were observed in only a minority of authorities. *Confidentiality*, again in terms of “personal data”, people’s *right to know* how to protect their privacy, that regard for people’s privacy was a *responsibility of everyone* involved in service delivery and the principle of *limited collection* of data were identified in less than half of the authorities which responded. Many other elements of privacy identified in the professional bodies’ conceptualisation were either observed rarely or not at all. Many of these latter elements were those connected to the purpose of privacy in the library environment. Elements related to privacies role in safeguarding *freedom of access to information*, *intellectual freedom* and the *right to enquire* were notable by their absence from the library authorities’ discussion of privacy.

Overall then, the concept of privacy which emerged from an analysis of the policy of public library authorities only reflected to a limited degree that of the professional bodies. That there is a stronger degree of resemblance to that of the Information Commissioner is noteworthy, given the latter’s role in enforcement and oversight of the operation of the Data Protection Act which was often referred to in authority policy . Even here, the correspondence is not complete. The Information Commissioner advanced the element of only collecting the absolute minimum of information necessary to operate a service, something observed in less than half the authorities. The suggestion of the Commissioner that people should be entitled to confirm their entitlement to use a service whilst retaining anonymity was also not reflected by any of the authorities.

7: Conclusions and recommendations

7.1: Conclusions:

The response rate achieved from Library Authorities in this study allows us to be fairly confident in drawing conclusions regarding the current status of privacy in Scottish public library policy. Distinct trends emerge in how privacy is represented and addressed within the policy of Library authorities in Scotland. It is also possible for us to make recommendations for how the position of privacy in Scottish public libraries might be enhanced.

7.1.1: Recommendations for further research.

Studies of Library Authorities within other geographical areas within the United Kingdom could be carried out to determine whether public library policy in these areas, also within the jurisdiction of CILIP, show similar patterns in their consideration of privacy. It is possible that academic library policy, having developed in a different context to that of public libraries may demonstrate differences in its treatment of privacy and it might also prove informative to extend the consideration of the topic to this context.

The particular patterns observed in this study may at least partly result from the history of the treatment of privacy in UK law and society. It is possible that similar studies in European nations where the history of privacy within the civil law differs may reveal differences in the way privacy is treated in public library policy even in the presence of shared influences such as European Union law and the ECHR. Similarly, given the very different legislative background, and more widespread public discourse on privacy, not to mention the ALA’s high profile in engagement on the issue, it seems probable that a similar study carried out of public library policy within the United States would reveal a different pattern of results.

7.1.2: Privacy, the professional conceptualisation and its reflection in Scottish public library policy.

Analysis of the privacy conceptualisations of IFLA, CILIP and the ALA demonstrate a significant degree of agreement regarding privacy within the English-speaking library profession, and suggest that this consensus may well extend to the profession more broadly. At a professional level, librarianship in the English-speaking world appears to hold a clear and consistent view of privacy, one rooted firmly in their ethical codes. They view privacy as being of fundamental importance, and as an under-pinning of the principle that the profession is ethically bound to ensure that access to information remains as free and open as possible. The codes of professional conduct and ethics of all three professional organisations commit their members to protect the privacy of their patrons as a vital prerequisite for affording them intellectual freedom – the right to enquire and to consider ideas freely – an essential requirement for properly engaging in a modern democratic society. There is likewise considerable commonality across the ethical codes as to the elements which constitute privacy, as well as those which constitute its purpose. All three bodies concur that privacy is a qualified right – that there is no right to privacy in doing things which are illegal or which are harmful of others – but that privacy should be qualified to the minimum degree necessary to ensure safety. In short that any surveillance of what a people reads, what they think and the ideas that they choose to think about should be based on a reasonable suspicion of wrong-doing, rather than a pre-emptive watching of everyone in case they should do something wrong.

A set of core elements can be identified in the discourse of all three professional bodies, and of the UK's Information Commissioner, which represent the essentials of a definition of privacy applicable to the context of Public Libraries.

If the profession of librarianship holds this conceptualisation of the nature and importance of privacy, to what extent and in what way is this reflected in the policies which are in operation within Scottish public libraries?

From the results of this study it seems overwhelming to be the case that the answer to this must be, to a very limited degree and in a far from coherent fashion. The wide range, and volume of documents, received from library authorities demonstrates a wide variation in understanding of what privacy is and how it should be treated. There is little consistency between library authorities in either the number, or title of documents which they see as relevant to the concept of privacy. In the light of this one questions how library patrons are to know where they need to look to find out how use of the library will affect their privacy.

Only rarely is policy made which addresses the specific context of the public library. In the vast majority of cases policy is made at the level of an overarching leisure trust or local authority, in a way which is intended to apply not simply to one service, but to apply to anything from Housing and Social Work departments to swimming pools and gymnasiums. Swimming pools are not libraries, however, and vice versa. It is not surprising that policy which is intended to cover a local swimming pools membership information does not mention intellectual freedom, however that same omission means that this same policy is silent on concerns which should be of great importance to libraries, and to library professionals.

Examining the detail of these policies also suggest at best a partial understanding of, and commitment to privacy. The overwhelming majority of policy appears to have as its primary concern satisfying the legislative requirements of the Data Protection Acts. Thus the protection of personal data is seen as a means towards ensuring the authorities legislative compliance, rather than any broader goal. Indeed, the use of "obliged to" and "required by" in many cases suggests a tone of reluctant compliance with the law, rather than a commitment to doing something because it is the right thing to do.

In many cases the impression is given indeed that compliance with the law means that privacy is abolished entirely. The prevalence within AUP's and similar documents of statements confirming that the internet activity of all patrons is logged and monitored strongly resembles a statement that in this context no privacy is permitted.

Overall, it would appear that the impression to be garnered from public library policy is that privacy is synonymous with Data Protection, and that the primary reason for "doing privacy" is that the law says that it must be done. Privacy, however, is a broader concept than the definition of personal information proposed by the Data Protection Acts. Something implicitly argued even by the office charged with overseeing compliance with the acts. The Information Commissioner themselves argues after all that even whilst requiring people to establish their identity in order to receive a service remains compliant with the letter of the Acts, that people should be afforded the right to maintain their anonymity wherever possible.

In policy terms then in Scottish public libraries privacy could be classified as being treated as an afterthought, cast into a limited mould directed at avoiding legal entanglements rather than promoted as a positive goal. By contrast privacy is held to be of great value by CILIP and by the standards of ethics and professional conduct that librarians should uphold. If, as CILIP maintain: "…without respect for our privacy our intellectual freedom will be undermined" (CILIP 2015), then surely the protection and promotion of privacy should be central to the mission of public libraries. After all, what are Ranganathan's second – "Every book its reader" – and third laws – "Every reader his book." – if not statements of the role of public libraries in allowing the opportunity for intellectual freedom (Gorman, 2015 ,p26)? If these statements – arguably foundation stones of principled and systematic formulations of what libraries are for – require that privacy be respected to be possible, then surely privacy too should be at the heart of the mission of public libraries.

7.1.3 Recommendations for the public library sector in Scotland:

Privacy is too central to the mission of libraries to be left to linger on the side-lines as it seems that it currently does in Scottish public library policy. There is also little likelihood that its importance, either in terms of public debate and concern or in the face of developing technologies such as RFID stock management and the need to balance their benefits against the potential for abuse by bad actors of all sorts (ALA, 2010), will decrease in the foreseeable future. Privacy should, therefore, occupy a more prominent position than it currently does in Scottish public libraries. It does not, however, have to be this way. There are things that can be done, on an individual library level as well as on a wider, professional level to bring privacy back to the position of importance that it should occupy on the policy stage.

Firstly, a positive case for privacy should be put. This should go beyond the current "there are risks to the organisation if it doesn't abide by the data protection act" to emphasise the positive benefits of privacy. A case should be made for freedom of expression, and for intellectual freedom as a means of ensuring a vibrant and active democratic society. Rather than the protection of privacy being an "obligation" imposed by weight of law it should be "sold" as a positive thing to do in its own right, and the mark of genuine engagement with the community.

At the same time it is important that a nuanced case for the qualification of privacy is made. Not, though, on the polarised terms of “if people can’t be watched then they might do bad things”. Rather on the basis that whilst there must be a presumption of the right of people to their privacy there must similarly be a right, where there is reasonable suspicion in an individual case that this right is being misused in ways that might harm others, to breach this privacy in order to protect them from harm.

This, however, is not something that individual libraries can be expected to do - both because they lack the leverage to move larger authorities unaided, but also because it would be both inappropriate and unprofessional for them to take a position of public disagreement with their authorities. As the professional body for public librarianship in Scotland this is a role which CILIP could play. CILIP’s existing statements on privacy are a solid basis for building a positive, progressive qualified privacy for public libraries. It is not, however, sufficient for CILIP and the profession to hold these principles in isolation. As the voice of the profession CILIP should be making the case, to local authorities, trusts, to central government and to the public for a reasoned, qualified view of privacy.

There are also things that can be done on the individual library and library authority level to improve the treatment and status of privacy in public libraries. Firstly it needs to be acknowledged that Data Protection is only a portion of what privacy actually encompasses, and that compliance with the letter of the law should be a starting point for discussions about policy, not necessarily an end to the discussion.

Secondly, it is recommended that consideration be given to the fact that the library context is very different to that of say a gym, or sports-club and that policy which may be suitable to those environments may not be sufficient in the case of the library, just as it is to a social work office or a solicitor's. Whilst some elements of policy may be able to cover all of an authority's services, it may be necessary to supplement these with policies specific to individual contexts such as a policy on privacy in libraries which picks up where the authorities Data Protection policy ends.

Of immediate benefit would be a consistency of explanation of privacy and privacy impacts on library use, one consistent across library authorities and user-friendly enough for all library users to understand. Public libraries should have a Privacy Statement or Privacy

Policy, which identifies what information they collect, why they collect it and what is done with it. The statement drawn up by Authority 14 stands as a good example of this kind of statement. If this kind of policy statement existed in all authorities it would make this information equally accessible to all service users across Scotland. This would be both fairer, and more likely to engender trust between authorities and their users than the current situation, where in some areas it is necessary to use a formal subject access request process to determine something that in another area users are told up front.

Library authorities could also take the position that whilst they reserve the right to monitor the internet activity of users where they believe there is reason to believe wrongdoing is taking place, they will not do so as a matter of course. This is not only a gesture of trust which may resonate positively with otherwise sceptical elements of their user communities, but is also in line with the Information Commissioner's view that any surveillance should be limited, targeted and based on specific suspicions.

It is also a more practical solution in many respects. Monitoring and recording the internet activity of all the computers of a library in an area with a high level of digital deprivation will generate extremely large quantities of data, most of which will be of little relevance or use to any future criminal or security investigation. Given the storage, security and handling of this quantity of data poses challenges in its own respect, especially in the current conditions of austerity. Is it not therefore more parsimonious, as well as less intrusive to limit the volume of this data by using these resources only when necessary, rather than on an overly cautious, "just in case" basis?

Libraries could also adopt the principle of *limited collection* – looking at the information about an individual that they retain and taking the decision to only retain what they actually need in order to supply a service. Does their ILS retain the borrowing history of individual readers and does this actually provide any useful service. If not, they could decide to set the system to discard this information. As CILIP observe – the best way to ensure people's privacy is simply to not collect the information to begin with (CILIP 2011 p.8)

Public libraries could be seen as caught between two sides of an ever more polarised debate, between those who believe that the right to privacy must be an inviolate, absolute right on the one hand and those arguing that those who want to hide what they are doing must be up to no good. I would suggest that whilst this may initially seem an invidious and unenviable position to be in, it provides an opportunity for public libraries, and the library profession as a whole to make a nuanced contribution to the debate and to exemplify a nuanced understanding of the nature of privacy as a right qualified by the responsibility to safeguard both the rights of the individual and the broader society.

Bibliography

Albanese, A., DiMattia, S. & Oder, N. (2003) 'Meese seconds Ashcroft's attack: ex-AG's criticism countered by ALA; new anti-Patriot Act bills'. *Library Journal,* 128 (18), pp.17+.

Allen, A.L. (1987) 'Taking liberties: privacy, private choice, and social contract theory. (Symposium: Feminist Moral, Social, and Legal Theory)'. *University of Cincinnati Law Review,* 56 (2), pp.461-491.

Allmer, T. (2011) 'A critical contribution to theoretical foundations of privacy studies'. *Journal of Information, Communication and Ethics in Society,* 9 (2), pp.83-101.

American Library Association (1991) *Policy concerning Confidentiality of Personally Identifiable Information about Library Users*. Available: http://www.ala.org/advocacy/intfreedom/statementspols/otherpolicies/policyconcerning (Accessed: 15 May).

American Library Association (2008) *Code of Ethics of the American Library Association*. Available: http://www.ala.org/advocacy/proethics/codeofethics/codeethics (Accessed: 20 May).

American Library Association Office for Intellectual Freedom (2010) *Privacy and freedom of information in 21st-century libraries [internet resource].* Chicago, IL: Chicago, IL : ALA TechSource.

American Library Association. Office for Intellectual Freedom (2010) *Privacy and freedom of information in 21st-century libraries [internet resource].* Chicago, IL: Chicago, IL : ALA TechSource.

Atkinson, P. & Coffey, A. (2011) '*Analysing Documentary Realities'*. In*:* Silverman, D. (ed.) *Qualitative Research: Issues of Theory, Method and Practice.* 3rd end edn. London: Sage, pp.

Bowers, S.L. (2006) 'Privacy and Library Records'. *The Journal of Academic Librarianship,* 32 (4), pp.377-383.

Brown, G. & McMenemy, D. (2013) 'The implementation of internet filtering in Scottish public libraries'. *Aslib Proceedings,* 65 (2), pp.182-202.

Bryman, A. (2016) *Social research methods.* 5th ed.. edn. Oxford: Oxford : Oxford University Press.

Chafee, Z.J. (1919) 'Freedom of Speech in Wartime'. *Harvard Law Review,* 32 pp.932 - 957.

Chartered Institute of Library and Information Professionals (2011) '*User Privacy in Libraries: Guidelines for the Reflective Practitioner'*. London: Chartered Institute of Library and Information Professionals.

Chartered Institute of Library and Information Professionals (2013a) *Code of Professional Practice*. Available: http://www.cilip.org.uk/about/ethics/code-professional-practice (Accessed: 15 May).

Chartered Institute of Library and Information Professionals (2013b) *Ethical Principles*. Available: http://www.cilip.org.uk/about/ethics/ethical-principles (Accessed: 20 May).

Chartered Institute of Library and Information Professionals (2015) *Respecting Privacy*. Available: http://www.cilip.org.uk/advocacy-campaigns-awards/advocacy-campaigns/intellectual-freedom/respecting-privacy (Accessed: 15 May).

Chartered Institute of Library and Information Professionals (2016) *Protecting the privacy of information and library service users.* Available: http://www.cilip.org.uk/productsservices/onsite-training/course-subjects/library-information-management/protecting-privacy-library-information-service-users.

Coombs, K.A. (2005) 'Protecting USER PRIVACY in the Age of DIGITAL LIBRARIES'. *Computers in Libraries,* 25 (6), pp.16-20.

Council of Europe (1968) *The European convention on human rights.* Strasbourg: Strasbourg, Council of Europe, Directorate of Information.

European Court of Human Rights (1978) '*Klass and others v Federal Republic of Germany'*. The Hague.

European Court of Human Rights (1984) '*Malone v United Kingdom'*.

Fairclough, N. (1992) 'Discourse and Text: Linguistic and Intertextual Analysis within Discourse Analysis'. *Discourse & Society,* 3 (2), pp.193-217.

Frohmann, B. (1994) 'Discourse analysis as a research method in library and information science'. *Library & Information Science Research,* 16 (2), pp.119-138.

Gallagher, C., McMenemy, D. & Poulter, A. (2015) 'Management of acceptable use of computing facilities in the public library: avoiding a panoptic gaze?'. *Journal of Documentation,* 71 (3), pp.572-590.

Gavison, R. (1980) 'Privacy and the limits of law

'. *Yale Law Journal,* 89 (3), pp.421 - 427.

Gill, R. (2000) '*Discourse Analysis'*. In*:* Bauer, M.W. & Gaskell, G. (eds.) *Qualitative Researching with Text, Image and Sound*

London: Sage, pp.

González-Fuster, G. (2014) *The emergence of personal data protection as a fundamental right of the EU [internet resource].* Cham: Cham : Springer.

Gorman, M. (2015) *Our enduring values revisited : librarianship in an ever-changing world.* Chicago : ALA Editions, an imprint of the American Library Association.

Hyams, E. (2007) 'Preserving users' privacy in spite of surveillance'. *Library + Information Update,* 6 (10), pp.26-28.

Information Commissioner's Office (2014) '*Privacy Impact Assessment Handbook Version 2.0'*. Wilmslom, Cheshire: Information Commissioner's Office.

International Federation of Library Associations (2015) *IFLA Statement on Privacy in the Library Environment*. Available: http://www.ifla.org/files/assets/hq/news/documents/ifla-statement-on-privacy-in-the-library-environment.pdf.

Madison Public Library Board (2004) *USA Patriot Act: Board Resolution on the USA Patriot Act and Related Measures that Infringe on the Rights of Library Users*. Available: http://www.madisonpubliclibrary.org/policies/usa-patriot-act (Accessed: 19/03/2016).

McGroaty, J. & Finch, V. (2010) *Human Rights Law Essentials.* Edinburgh University Press.

Milazzo, M., J. (2014) 'Facebook, Privacy and Reasonable Notice: The Public Policy Problems with Facebook's Current Sign-up Process and How To Remedy the Legal Issues'. *Cornell Journal of Law and Public Policy,* 23 (3), pp.661 - 690.

Mill, J.S. (1985) *Utilitarianism ; On Liberty ; Essay on Bentham.* London: London : Fontana.

Moreham, N. (2001) 'Douglas and others vs Hello! Ltd - the Protection of Privacy in English Private Law'. *The Modern Law Review,* 64 (5), pp.767 - 774.

Oder, N. (2006) '"John Doe" case dropped'. *Library Journal,* 131 (13), pp.16.

Oder, N. (2007) 'Criticism over patriot act use: still, Justice Department says library controversy caused hesitation'. *Library Journal,* 132 (6), pp.14+.

Open University (2016) *Privacy Rights and the Law*. Available: http://www.open.edu/openlearn/people-politics-law/the-law/privacy-rights-and-the-law/content-section-2.2.

Prosser, W. (1960) 'Privacy'. *California Law Review,* 48 (3), pp.383 - 423.

Rauhofer, J. (2008) 'Privacy is dead, get over it! Information Privacy and the dream of a risk-free society'. *Information and Communications Technology Law,* 17 (3), pp.185 - 197.

Reid, E. (2010) *Personality, confidentiality and privacy in Scots law.* Edinburgh: Edinburgh : Thomson/W. Green.

Richards, N.M. & Solove, D.J. (2010) 'Prossers Privacy Law: A Mixed Legacy'. *California Law Review,* 98 (6), pp.1887 - 1924.

Rössler, B. (2005) *The value of privacy.* Cambridge, UK: Cambridge, UK : Polity.

Salo, D. (2013) 'Breaking the panopticon'. *Library Journal,* 138 (19), pp.14.

Scott, J. (1990) *A matter of record : documentary sources in social research.* Cambridge: Cambridge : Polity.

Solove, D.J. (2002) 'Conceptualizing Privacy'. *California Law Review,* 90 (4), pp.1087-1155.

Sturges, P., Davies, E., Dearnley, J., Iliffe, U., Oppenheim, C. & Hardy, R. (2003) 'User privacy in the digital library environment: an investigation of policies and preparedness'. *Library Management,* 24 (1/2), pp.44-50.

Sturges, P., Teng, V. & Iliffe, U. (2001) 'User privacy in the digital library environment: a matter of concern for information professionals'. *Library Management,* 22 (8/9), pp.364-370.

Wacks, R. (2010) *Privacy : a very short introduction.* Oxford ; New York: Oxford ; New York : Oxford University Press.

Warren, S.D. & Brandeis, L.D. (1890) 'The Right to Privacy'. *Harvard Law Review,* 4 (5), pp.193-220.

Wilkinson, J.H.I. (2010) 'Dual lives of rights:The Rhetoric and practice of rights in America'. *California Law Review,* 98 (2), pp.277 - 326.

Appendix 1: Professional Body Documents Used Within Analysis

American Library Association:

Privacy: An Interpretation of the Library Bill of Rights (http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy)

Resolution on Radio Frequency Identification (RFID) Technology and Privacy Principles (http://www.ala.org/advocacy/intfreedom/statementspols/otherpolicies/rfidguidelines)

Privacy Policy (http://www.ala.org)

Code of Ethics of the American Library Association (http://www.ala.org/advocacy/proethics/codeofethics/codeethics)

Library Bill of Rights (http://www.ala.org/advocacy/intfreedom/librarybill)

Library Privacy Guidelines for E-book Lending and Digital Content Vendors (http://www.ala.org/advocacy/library-privacy-guidelines-e-book-lending-and-digital-content-vendors)

Policy Concerning Confidentiality of Personally Identifiable Information about Library Users Questions and Answers on Privacy and Confidentiality (http://www.ala.org/advocacy/intfreedom/statementspols/otherpolicies/policyconcerning)

Chartered Institute of Library and Information Professionals:

Code of Professional Practice (http://www.cilip.org.uk/about/ethics/code-professional-practice)

Ethical Principles (http://www.cilip.org.uk/about/ethics/ethical-principles)

Privacy Statement (http://www.cilip.org.uk/privacy-statement)

User Privacy in Libraries: A Guide for the Reflective Practitioner (http://www.cilip.org.uk/archived-policy-statements/user-privacy-libraries-guidelines-reflective-practitioner)

Respecting Privacy (http://www.cilip.org.uk/advocacy-campaigns-awards/advocacy-campaigns/intellectual-freedom/respecting-privacy)

The Role of CILIP and Our Members (http://www.cilip.org.uk/advocacy-campaigns-awards/advocacy-campaigns/intellectual-freedom/role-cilip-our-members)

International Federation of Library Associations:

Ethics and Information Ethical principles of the library and information professionals (http://www.ifla.org/node/6496)

FAIFE Mission (http://www.ifla.org/faife/mission)

Internet Manifesto 2014 (http://www.ifla.org/publications/node/224)

Principles on Public Access in Libraries (http://www.ifla.org/node/10781)

The Glasgow Declaration on Libraries , Information Services and Intellectual Freedom (http://www.ifla.org/publications/the-glasgow-declaration-on-libraries--information-services-and-intellectual-freedom)

Code of Ethics for Librarians and other Information Workers (full version) (http://www.ifla.org/news/ifla-code-of-ethics-for-librarians-and-other-information-workers-full-version)

IFLA Data Protection Policy (http://www.ifla.org/data-protection-policy)

IFLA Licensing Principles (2001) (http://www.ifla.org/publications/ifla-licensing-principles-2001)

IFLA Statement on the Right to be Forgotten (2016) (http://www.ifla.org/publications/node/10320)

IFLA Statement on Privacy in the Library Environment (http://www.ifla.org/publications/node/10056)

IFLA Principles for Library eLending (http://www.ifla.org/elending/principles)

Social Media, Children and Young Adults @ the Library – Safety, Privacy and Online Behaviour (http://www.ifla.org/publications/node/9961)

Information Commissioner:

Privacy Impact Assessment Handbook version 2.0

Personal Information Toolkit