

“You don’t come to the library to look at porn and stuff like that”: Filtering software in public libraries

Louise Cooke, Rachel Spacey, Claire Creaser, Adrienne Muir

Abstract

Should public libraries filter the content of internet services offered to their users? We discuss this question in the light of findings from the AHRC-funded MAIPLE project, which has been investigating measures taken by UK Public Library Services to manage public internet provision in their libraries. Initial findings suggest that filtering software is extensively used, and that librarians and users alike are mostly content with this solution. It could be argued that this position is at odds with our professional and ethical duties towards clients to provide uninhibited access to information and ideas. However, we recognise the social norms and realities in which services must operate and go on to discuss clear and transparent policies and procedures that public libraries might adopt to mitigate the potential for misuse of their internet facilities.

1 Introduction

Following the success of the People’s Network project in the UK, proposed in 1997 and launched in 2000, the provision of internet access for library users has become one of the key functions of public libraries and is provided by every UK Public Library Service (PLS). According to statistics from the Chartered Institute of Public Finance and Accountancy (CIPFA), there were 42,914 workstations with internet and/or library catalogue access in UK public libraries in 2012/13 (CIPFA, 2013). However, the management of content access in UK public libraries has been given relatively little attention in the academic or practitioner press and PLS have been left to find their own way of preventing illegal and/or

Authors

Louise Cooke is a Senior Lecturer and Director of Postgraduate Programmes in Information Management at Loughborough University.

Email: l.cooke@lboro.ac.uk

Rachel Spacey is Research Associate at LISU (Library and Information Statistics Unit) at Loughborough University.

Claire Creaser is Director of LISU, Loughborough University, and a Chartered Statistician.

Adrienne Muir is a Senior Lecturer in Publishing at Loughborough University.

Received 12 March 2014

Accepted 18 May 2014

inappropriate use of such services. Currently there appears to be little standardisation, guidance or transparency about measures being taken to prevent misuse. In particular, there has been no clear evidence as to what extent the use of filtering software as a solution to this dilemma has been taken up, although observation seemed to indicate that it has become a well-accepted response. This is a matter of some importance given that librarianship is a profession with a strong ethical commitment to freedom of access to information, and, according to the International Federation of Library Associations and Institutions (IFLA) *Code of Ethics for Librarians and Information Workers*:

Librarians and other information workers reject the denial and restriction of access to information and ideas most particularly through censorship whether by states, governments, or religious or civil society institutions.

(IFLA, 2012, S1, para.2).

This apparent contradiction was one of the key motivations that led to the *Managing Access to the Internet in Public Libraries* (MAIPLE) project (LISU, 2012). MAIPLE is a two-year project funded by the UK Arts & Humanities Research Council (AHRC), with the overarching aim to identify and quantify measures being taken in UK public libraries to regulate and to manage access to internet content. This includes regulation via technical means such as the implementation of filtering software, and via organisational measures such as the adoption of Acceptable Use Policies (AUPs) and the provision of user education.

A secondary motivation, other than an ethical objection to the restriction of access to information in public libraries, was the oft-cited inaccuracy of filters as a content restriction measure, leading to under- and over-blocking that has the potential to distort the information landscape. These issues have been discussed extensively in both academic and popular literature (e.g. Simpson, 2008; Stol *et al.*, 2009; Ybarra *et al.*, 2009; Hope, 2013; Jivanda, 2013), but to date the technical inaccuracies of the software solution do not appear to have been resolved. Indeed, given the cultural and contextual difficulties of determining what constitutes offensive content, it is questionable whether a technical solution could ever satisfactorily resolve this dilemma.

The purpose of this paper is not to present the findings of the MAIPLE project in detail: these have already been reported elsewhere at least with regard to the quantitative aspects of the study (see Spacey *et al.* 2014a); although a brief overview of some key aspects will be presented here in order to provide some context. Instead, this article will consider how public libraries can utilise filtering as a content control mechanism in a transparent and open way, providing users with the opportunities to have some say in its implementation.

2 Background context

The research strategy for the MAIPLE project included a comprehensive international literature review, in order to be able to learn and to draw from practice within and beyond the UK. The full review can be read in Spacey *et al.* (2014b), but for the purposes of this paper a more concise overview of key literature in the field will be given.

In the USA, the use of filters as a means to manage access to internet content in public libraries has been well-documented as have the arguments of both the pro- and anti- filtering lobbies. Legislation has shaped the content control landscape with the signing into law of the *Children's Internet Protection Act* (CIPA) in 2000. If they are to be eligible for federal subsidies towards the cost of internet access, schools and libraries must employ a technology protection measure (TPM) to protect children against visual depictions of child pornography, obscenity and harmful material. TPMs may include filtering software and site blocking. The constitutionality of the CIPA was challenged by the American Library Association, a vehement opponent of what it perceives to be internet censorship but in 2003, the Supreme Court declared CIPA constitutional. Adult users, however, may request that TPMs are disabled to permit the unblocking of a particular site(s).

Opposition to the use of filtering has been on ethical grounds and its use as a means to censor and infringe constitutional freedoms which the American people hold dear: "all filters block access to critical constitutionally protected speech about many subjects people need to know" (Kranich, 2001, 481). While some librarians may agree to the use of filtering per se they may have little direct say or involvement in what is actually blocked as decision making may be managed by IT colleagues, a reliance on the filtering software used or the Internet Service Provider (ISP):

While it has been pointed out that librarians have always selected material for library stock and have therefore acted, to an extent, as a filter, filtering software removes selection decisions from librarians and places it in the hands of non-library trained third parties or computer automation.

(Hamilton, 2004, 163)

Filters have also been criticised for their technological limitations including under-blocking – "when content is not blocked that should be restricted" and over-blocking – "when content is blocked that should not have been restricted" (Resnick *et al.*, 2004, 67) and for the ease with which they may be bypassed (Bitso *et al.*, 2012). For example, Comer found that 66 per cent of Indiana's public libraries responding to her survey used filters, of which 35 per cent had experienced one or more types of problem. Twenty-two per cent said that users complained of over-blocking whilst "Twenty-one percent said that patrons are still pulling up 'pornographic' sites" i.e. under-blocking (Comer, 2005, 12).

Approximately half of all public libraries in the USA have implemented the requirements of CIPA:

As such, the number of public libraries filtering access is now at least 51.3 percent, but the number will likely be higher as a result of state and local laws requiring libraries to filter as well as other reasons libraries have implemented filters.

(Jaeger and Yan, 2009, 10)

Conversely, the third most popular reason public libraries did not apply for federally subsidised internet access according to the most recent *Public Library*

Funding and Technology Access Survey was because they did not wish to comply with CIPA's filtering requirements (Bertot *et al.*, 2012).

Arguments in favour of the use of content-control mechanisms in public libraries in the UK resonate with those found in the USA and internationally. Hamilton's (2004) PhD research, funded in part by the IFLA Committee on Freedom of Access to Information and Freedom of Expression (FAIFE), found that of the 42 library associations in countries where filtering was widespread, the primary justification in 35 of them was the protection of children. The issue of children's internet safety in the UK was highlighted in 2008 with the publication of a report - *Safer Children in a Digital World* (Byron, 2008). The "Byron Review" considered internet use including the dangers facing children such as exposure to sexually explicit material. While filtering was considered a useful tool to aid parents it was acknowledged that it had its limitations. Proactive strategies such as teaching children resilience and supporting them to use the internet safely were also suggested. Exposure to offensive content online has also been considered in relation to public library staff. A study of computer based crimes in Scottish PLS based on staff interviews and two online surveys found that while serious incidents of misuse were rare, staff "found checking for misuse, and dealing with it, extremely unpleasant" (Poulter *et al.*, 2009, np).

Opposition to the use of filters in the UK amongst library and information professionals has not been as vehement or as polarised as it is in the USA. In the UK, the Chartered Institute of Library and Information Professionals (CILIP), the professional body for librarians also endorses freedom of and access to information. In 2005, CILIP stated:

It is the role of a library and information service that is funded from the public purse to provide, as far as resources allow, access to all publicly available information, whether factual or fiction and regardless of media or format, in which its users claim legitimate interest... Access should not be restricted on any grounds except that of the law. If publicly available material has not incurred legal penalties then it should not be excluded on moral, political, religious, racial or gender grounds, to satisfy the demands of sectional interest. The legal basis of any restriction on access should always be stated.

(CILIP, 2005)

However, in 2011, CILIP's user privacy guidelines stated that whilst CILIP "does not endorse the use of filtering especially for adult users" it did acknowledge "that a number of libraries do use filtering systems especially if it is required by their parent institution" (CILIP, 2011, 12-13). Research in the 32 PLS in Scotland found that in 18 services the decision to filter was made by local authority management, in seven services it was by library service management and in five it was a joint decision (Brown and McMenemy, 2013).

Recent research by the Oxford Internet Institute has found that there has been an increase in the number of adults in the UK using parental control filters in the home from 35 per cent in 2007 to 44 per cent in 2013 and amongst those who feel that the internet must be regulated to protect children:

There seems to have been a rise in support for government intervention, with 75% of respondents agreeing that government should be responsible compared to 66% in 2011.

(Dutton *et al.*, 2013, 52)

Society's apparent growing acceptance of filtering was reflected in an announcement by Prime Minister David Cameron, who declared in July 2013 that the government had negotiated with the four largest ISPs to install default family-friendly filters for all new customers. During 2014 it is anticipated that all existing customers will be contacted by their ISPS and given the option to filter internet content. This could potentially result in default filtering for 95 per cent of homes in the UK with internet access although adults are able to opt out and have the filter turned off. In addition, an agreement was reached with public Wi-Fi providers that family friendly filters would be in place by the end of August 2013 wherever children might be:

On public wi-fi, of which more than 90% is provided by 6 companies – O2, Virgin Media, Sky, Nomad, BT and Arqiva – I'm pleased to say we've now reached an agreement with all of them that family friendly filters are to be applied across public wi-fi networks wherever children are likely to be present.

(Rt Hon David Cameron MP, 2013)

3 Methods used in the MAIPLE project

The MAIPLE project has drawn on a mixed-methods approach consisting of a literature review, an online survey of UK PLS and case studies. The survey questions emanated from the desk research and discussions with the MAIPLE External Advisory Board (EAB), established at the beginning of the project in September 2012. The draft survey was shared online with the EAB and following refinement was piloted by three critical friends of the project and a public library ICT manager known to the authors. The 36 question survey was hosted online by Bristol Online Surveys [BOS] during January and February 2013. It was hoped that one member of staff from each PLS might complete the survey and an invitation email was sent to a senior manager within every PLS asking for their co-operation in completing or securing its completion. Following reminder emails the survey finally closed on February 22nd with 80 responses from a potential 206 representing a 39 per cent response rate.

The survey provided respondents with the opportunity to declare an interest in the next stage of the research which involved a series of case studies. From April to November 2013, five case study visits were undertaken to PLS in the East Midlands and South of England, one in Scotland, one in Wales and one in Northern Ireland. The visits included semi-structured interviews with a range of library staff usually six in total and approximately five internet users. Interviews were recorded and transcribed for analysis. Relevant documentation and observation were also used to inform the writing of a draft version of each case study, which was shared with the relevant contact from the PLS to confirm accuracy.

4 Brief overview of findings

The survey results revealed that all 80 responding UK PLS provide filtered access to the internet on all their networked PCs (100.0 per cent). Two-fifths of respondents use Websense filtering software (40.0 per cent) while Bluecoat was the second most popular filtering package used by nine services (11.3 per cent). The decision to use filtering software was fairly evenly distributed across different local authority departments, including the IT departments of local authorities within which the PLS sits (26.3 per cent), by library service senior management (25.0 per cent) or by local authority senior management (22.5 per cent).

In most of the PLS responding to our survey, library users are made aware that internet content is subject to filtering in the Acceptable Use Policy (AUP) (88.8 per cent). The AUP, which sets out the PLS expectations of use including what is and is not permitted, is brought to the attention of internet users primarily when they log-on to a PC (89.9 per cent) while less than half of responding services refer to the AUP on the library service website (48.1 per cent). In addition, more than half of responding services draw users' attention to internet filtering when they log-on to a PC (56.3 per cent). Three services did not make users aware of internet filtering; for example, one of the services we visited in the East Midlands provides filtered access to the internet for the public on both their stand-alone, networked PCs and the library Wi-Fi connection but this was not advertised to users. The case study users we interviewed were not always aware that internet content was filtered on the library PCs unless they themselves had experienced site blocking which in some cases they perceived to be rather arbitrary. In all of the case study sites that we visited, there did not appear to be any publicly available information about the types of material that the PLS might block. According to the results of our survey the top five content categories blocked for all users are sexual (85.7 per cent), hacking (83.1 per cent), violence and intolerance/hate (both 80.5 per cent) and extremist (79.2 per cent).

Public library internet users are able to request that a site is unblocked by asking a member of staff in the library in approximately three quarters of responding services (76.3 per cent). However, the process to respond and potentially to unblock a site can be unclear as illustrated by our case study in Wales where staff perceptions of the unblocking process varied from having to "nag IT department" to unblock a site, to "that was just a phone call or an email to X and he releases it". In 53 authorities, responsibility for responding to requests to change the filter rests with just one staff group (66.3 per cent), but in 27 services it rests with more than one group (33.8 per cent) of which 14 respondents selected two groups (17.5 per cent) and 10 respondents selected three groups (12.5 per cent). Senior library service managers are involved in over half of responding services (52.5 per cent) whilst in approximately two-fifths of services, library service IT staff (41.3 per cent) and/or local authority IT staff (41.3 per cent) are involved. In fewer than ten per cent of PLS are frontline library staff empowered to directly and/or immediately respond to requests to unblock a site.

Almost two-thirds of responding services had received complaints from internet users about filtering in the last year (65.8 per cent) compared to almost one-third who had not (30.4 per cent) and 3.8 per cent who did not know. Over-blocking

was the most frequent cause of complaint (88.5 per cent). The inability to share or upload files was cited by over half of PLS in receipt of complaints (53.8 per cent) while grumbles about the presence of filtering software per se were less frequent (19.2 per cent).

Public library managers were asked how useful they judged filtering to be in maintaining acceptable internet use in their libraries. Over half of all respondents judged it to be “very useful” (56.3 per cent) and approximately two-fifths found it “somewhat useful” (41.3 per cent). Only two respondents were negative about filtering, judging it to be “not very useful” (2.5 per cent). However, the use of filters does not mean that misuse has stopped. Breaches of the AUP were still known to occur, of which viewing obscene content was judged the most common misdemeanour. The majority of respondents felt that major breaches of the AUP, which were not defined in the survey, occurred “rarely” (38.0 per cent) and “sometimes” (31.6 per cent) and the largest proportions of respondents felt that minor breaches of the AUP “rarely” happened (43.0 per cent) and “sometimes” happened (39.2 per cent). Strikingly, both major and minor breaches were considered to be the result of internet users viewing obscene (legal and illegal) content (82.2 and 92.7 per cent respectively).

Interviews with library personnel at all levels revealed that staff were generally very accepting of the use of filtering software, thus supporting the survey findings. The question of child protection tended to dominate arguments favouring filtering, as illustrated in this quote from a senior member of library staff at one of our case study sites:

Obviously there is material available on the internet it is illegal to possess or download and also there is material that would be unsuitable for children or younger people to access and so I think we have a duty of care to ensure that, for instance, children’s requirements for a safe environment are catered for.

Ethical reservations with regard to the acceptability of censoring access to certain kinds of information were voiced tentatively, but were seen as secondary to the goal of child protection and the provision of a safe and decent public user environment. Filtering is regarded as a realistic solution to this dilemma:

So I suppose, pragmatically, I’ve realised that although I may have had ethical concerns as a librarian, the reality is, I suspect, that for the half a million uses we have every year, I’m not under the impression that it’s caused any particular problems.

Perhaps more surprisingly is the general acceptance that PLS users demonstrated with regard to their use of the internet being regulated in this way. One male user in his early twenties responded to a question about whether public libraries should filter access to certain websites by saying “Adult ones, 18 and that? Yes, it should yes. You don’t come to the library to look at porn and stuff like that, do you?” This general level of support was echoed by the majority of other users with whom we spoke, and is also reflected in a survey quote from a library manager in the East of England:

Filtering is generally effective and processes for unblocking sites that are caught unnecessarily and for blocking new sites works smoothly. We have had no

complaints about either the principle of filtering or of not offering any sort of filtering based on age. Nor have we had any complaints from people who have been caught breaking the AUP of any sort of restrictive practice or censorship.

However, we were given a number of examples where adult users had met with content restrictions that prevented them from accessing a wide range of material that many would not consider appropriate for blocking. These examples included a young man wanting to access dating sites for over 18s, a writer wanting to research information on field sports who found the relevant site blocked as it featured a picture of a gun, music sites that could potentially lead to file sharing and copyright contravention, a user researching his family history who was blocked from accessing the Royal Artillery site, a user interested in military music who was prevented from accessing the relevant site and one user who was accessing “perfectly legitimate sites” as part of her job search but kept finding herself inexplicably blocked.

5 Discussion

Our results indicate that filtering is a generally accepted content control mechanism by UK public library professionals that appears to have been adopted widely across the sector. However, the extent to which decisions about filtering are made by library personnel is mixed: in some instances it appears that control rests with the providers of internet services, who may have very different missions with regard to universal information access. Moreover, it would appear that more could be done to ensure that users are aware of the presence, implications and scope of any filtering mechanisms in place. Our results suggest that awareness amongst users – and in some cases, even library personnel – was very mixed. Where users are aware, this appears often to be the result of having met with blocking of access to a specific site. If filters are here to stay then as CILIP Policy Officer, Jacqueline May suggests: “There should be transparency when filtering and blocking takes place in public areas” (May, 2014). PLS need to do more than merely state in their AUP that filtering is used but clearly communicate how users can request that a site is unblocked.

In addition, the unblocking process needs to be straightforward and consistent. As the ALA states in its guidelines to public libraries that filter, the AUP should “include clear instructions for making such requests” (American Library Association, 2012, 20). Our results suggest that practice is currently very varied across the sector, and the balance of power to accept or reject such requests appears to rest primarily with back-office IT personnel, causing the process to be both bureaucratic and lacking in transparency. Many of the respondents in our study did not feel able to make such a request.

Our results also suggest that filtering is an imperfect tool with services experiencing both over-blocking and under-blocking. Arguably, the situation has changed little in the last fifteen years as the following quote from an editorial in the *Journal of Librarianship and Information Science* describes:

The filtering software and services currently available are notoriously clumsy, sometimes blocking perfectly respectable sites, and indeed curtailing whole areas of legitimate enquiry for young people, simply because of the use of a few terms

that might have sexual connotations. The purveyors of pornography are likewise renowned for being one step ahead of other Web providers, by fooling search engines and filters to bring their sites to the notice of an audience because so much of their profits are at stake.

(Stoker, 1999, 4)

Our results give little confidence that things have changed much for the better since Stoker wrote this at the end of the Twentieth Century. We encountered many examples of seemingly innocuous sites, such as those dedicated to military history, blocked on a relatively tenuous basis such as the fact that they contained images of weaponry. Simultaneously, we found examples of under-blocking, with users and library personnel both reporting instances of users accessing pornographic sites in breach of the AUP, seemingly unhampered by the presence of the filtering software. Yet the use of content control software has the potential to lead to complacency on the part of parents, educators and library personnel, who may overlook the need to educate minors with regard to safe internet use on the grounds that content is filtered.

Our results showed that almost all responding PLS had an AUP which users are made aware of and agree to when they log-on to the PC. AUPs are guidelines which set out what internet services the user can expect from the library including the types of resources available and the service's expectations of the user which tend to be activities that are not permitted such as accessing pornography or illegal content:

AUPs can be seen as a passive form of control; while they do not physically restrict a user from inappropriate online behaviour, they rather act as a guideline.

(Laughton, 2008, 2)

They usually stipulate what the consequences of breaching the AUP are and are used to "pass some element of liability onto the customer when accessing internet services" (McMenemy and Burton, 2005, 21). To ensure that users abide by the AUP some form of oversight must take place. In the early days of the People's Network, staff would try visually to monitor internet activity and check internet histories but in the seventeen years since the PN initiative was conceptualised, monitoring has grown more sophisticated with the use of monitoring software. We found that PLS liked to use visual monitoring to manage public internet access (83.5 per cent of responding PLS) as well as the positioning of PCs and use of a booking system (70.9 per cent), collecting internet use data (44.3 per cent) and monitoring software (30.4 per cent).

The use of a booking system for PC usage is another popular tool to manage internet access as it provides a record of who used the system particularly if a proprietary software system is used which includes user authentication features in the form of borrower number and PIN and acceptance of the AUP. Over 90 per cent of responding services to our survey used a proprietary software booking system (92.4 per cent) of which more than half used Netloan by Lorensbergs and almost one third use i-CAM by Insight Media Internet Limited. As one manager explained when asked what works in managing internet use: "Having a booking system that links to the Library Management System for verifying both ID and

permissions to access the internet". It is a combination of tools which managers perceive to be the most effective, as one manager in the North West of England clarified:

A PC management/booking system is essential, even if you're enabling turn-up-and-log-on self-service access. Staff awareness of customer behaviour has been very useful: someone's suspicions of what a customer is up to in the library is quite often confirmed by the reports from the filter monitoring system. Areas with unsupervised terminals away from quiet reading areas have caused problems occasionally. Staff being able to tell customers that they can proxy in to the public terminals is a useful deterrent to some bad behaviour, even though it is scarcely ever used in real life. (This can't be done unannounced - customer privacy is protected by a ticker tape message across the centre of the screen [which] warns the customer that staff are about to see what's on their screen). Monitoring the reports of blocked attempts to access sites is important. Partly to identify potential weaknesses; partly to identify customers/libraries/times where the attempts are persistent and may need to be managed at the front line; partly to identify where we have over blocked and prevented access to perfectly legitimate sites. We use DeepFreeze to "wipe clean" each terminal on rebooting to remove anything that may compromise customers' safe use of the Internet, including any persistent cookies that allow people access to users' secure accounts (email, shopping, etc.).

User education is another component PLS can use to equip users with the necessary skills to take responsibility for their actions online. Approximately one third of survey respondents provided some kind of internet training for users. As the CILIP President, Barbara Band, recently suggested in response to the Internet Safety Summit held by the UK Government, public libraries are in a good position to educate and inform users, especially children, about their internet experience:

Children do need protecting but the best way of doing this is not by simply switching off the bits of the internet that we are unsure of but by teaching them the necessary skills to use it proficiently and safely. Given their unique position, librarians in schools and public libraries have an important role to play in this and in advising parents and carers too.

(CILIP, 2013)

Of course, public libraries have a legal obligation to prevent copyright infringement by users. The *Digital Economy Act 2010* amends the *Communications Act 2003* and aims to reduce online copyright infringement. The *DEA 2010* identifies three key roles: ISPs; copyright owners and subscribers to internet services, placing an obligation on ISPs to notify subscribers of unlawful behaviour, when informed by copyright owners. It is anticipated that the Initial Obligations Code will become operational in 2014. At this point in time it is still unclear how public libraries will be classified. CILIP's advice to PLS includes having an internet usage policy or AUP which refers to copyright law and website blocking: "Where possible, access should be blocked to internet sites the sole purpose of which is known to be to facilitate the illegal downloading of materials" (CILIP, 2012, 6).

5 Conclusion

The MAIPLE project was initiated with an ideological perspective that prioritised protecting and extending a user's right to freedom of access to all kinds of information in the public library, as an essential foundation of our professional ethical obligation towards library users. We did not anticipate our final recommendations advocating the use of filtering software in public libraries. Nevertheless, as stated in our original bid document, we recognised that:

As providers of public access to the Internet [library personnel] have to balance the needs of intellectual freedom and access to information with their responsibilities to protect the unwitting user and the underage, or debar those persons intent on using such access for activities proscribed by legislation or the providers. In doing this they are aware of their own, and the personal liabilities of their employees.

(Cooke *et al.*, 2011)

The project aimed to shed greater transparency on measures being taken in UK public libraries to regulate access to internet content, and the effectiveness or otherwise of such measures. Our findings have demonstrated that filtering is an almost ubiquitous solution and one that is seemingly favoured by library staff and users alike. Although library users (and in some instances, library staff) may be alerted to its deployment in the AUP, do users read the Terms and Conditions in detail and what opportunities are available for having material unblocked? And, as previously noted, it is a blunt instrument that will lead to the blocking of legitimate content whilst still allowing access to some potentially harmful and/or offensive content. Other perhaps more transparent measures, such as the use of AUPs, electronic booking systems, visual and electronic monitoring, and the provision of user education are also used, but appear to be relied on more as secondary solutions. The latter measure, in addition, has suffered as a result of declining numbers of library personnel, and we found that, where it was provided, it was often done via the use of volunteers or "computer buddies", rather than professional library staff who simply did not have the capacity or resources to offer such provision.

Whilst the overwhelming reliance on filtering software as a primary solution may not easily be reconciled with our ethical commitment to the user's right to freedom of access to information, the results of the study suggest that (at least for the present time) it is a pragmatic solution that is here to stay. If public sentiment in general is more pro-control as evidenced in the number of e-safety developments such as family friendly public Wi-Fi, it is difficult to argue that unrestricted access in PLS is appropriate. Rather than agitate against the deployment of filtering software in public libraries per se, our findings suggest that it is more appropriate to work towards recommendations for best practice in the use of filtering software and rebalancing reliance on filtering with the other potential measures open to library personnel. Whilst the final recommendations from the MAIPLE project have not yet been formalised, initial suggestions for good practice arising from project findings as outlined in this paper include:

-
- Public libraries need to be more proactive in alerting users to the use of filtering software and its potential impact on users' information access;
 - Clear, simple, and well-publicised policy and procedures need to be in place to enable users to unblock sites, with respect given towards the sensitivities and privacy of users;
 - Decisions concerning the use of filtering software (and categories and levels of material to be blocked) should be made with the full involvement of library personnel and not left solely to PLS IT personnel, parent bodies, or the commercial providers of internet services;
 - All decisions concerning the use of filtering software should be taken with the primary consideration of allowing the widest possible access to information for all users possible within the limits of safety and legality;
 - At a time when government rhetoric appears to prioritise both the digitisation of government transactions and children's internet safety, ring fenced resources should be made available to local authorities to ensure that public libraries are not only protected as an essential public service to which members of the public are statutorily entitled, but that these libraries are staffed with adequate numbers of professional personnel able to help, guide and support their users through the digital minefield. Over-reliance on electronic "baby-sitting" software as a single, fool-proof solution should be avoided at all costs;
 - Greater standardisation and harmonisation of practice would be beneficial. This could be co-ordinated through CILIP and based on guidance from the final outcomes of the MAIPLE project.

References

- American Library Association (2012) *Libraries & the Internet Toolkit. Tips and guidance for managing and communicating about the Internet*. URL: <http://www.ala.org/advocacy/sites/ala.org.advocacy/files/content/intfreedom/ifttoolkits/litoolkit/2012internettoolkit.pdf> [accessed 12.2.14].
- Bertot, J.C., McDermott, A., Lincoln, R., Real, B. and Peterson, K. (2012) *2011-2012 Public Library Funding & Technology Access Survey: Survey Findings & Report*. College Park, MD: Information Policy & Access Center, University of Maryland College Park. URL: http://www.plinternetsurvey.org/sites/default/files/publications/2012_plftas.pdf [accessed 11.2.14].
- Bitso, C., Fourie, I. and Bothma, T. (2012) *Trends in transition from classical censorship to Internet censorship: selected country overviews*. IFLA: FAIFE Spotlight. URL: http://www.ifla.org/files/assets/faife/publications/spotlights/1%20Bitso_Fourie_BothmaTrendsInTransiton.pdf [accessed 5.3.14].

-
- Brown, G. and McMenemy, D. (2013) The implementation of internet filtering in Scottish public libraries, *Aslib Proceedings* **65**(2), 182–202. URL: <http://strathprints.strath.ac.uk/37396/> [accessed 30.4.14].
- Byron, T. (2008) *Safer Children in a Digital World. The Report of the Byron Review*. Department for Children, Schools and Families & Department for Culture, Media and Sport. URL: <http://media.education.gov.uk/assets/files/pdf/s/safer%20children%20in%20a%20digital%20world%20the%202008%20byron%20review.pdf> [accessed 5.3.14].
- CILIP (2005) *Statement on Intellectual Freedom, Access to Information and Censorship*. URL: <http://www.cilip.org.uk/get-involved/advocacy/information-society/foi/Pages/intellfreedom.aspx> [accessed 30.4.14].
- CILIP (2011) *User Privacy in Libraries. Guidelines for the reflective practitioner*. Revised May 2011. URL: http://www.cilip.org.uk/sites/default/files/documents/Privacy_June_AW.pdf [accessed 11.2.14].
- CILIP (2012) *The Digital Economy Act 2010 Impact on educational institutions and public libraries*. URL: http://www.cilip.org.uk/sites/default/files/documents/Digital%20Economy%20Act%20-%20impact%20on%20libraries_0.pdf [accessed 20.2.2014].
- CILIP (2013) Filtering and blocking the internet won't protect young people, educating them will. *CILIP News*. URL: <http://www.cilip.org.uk/cilip/news/filtering-and-blocking-internet-won-t-protect-young-people-educating-them-will> [accessed 20.2.2014].
- CIPFA (2013) *Public library statistics. 2013-2014 Estimates and 2012-2013 Actuals*. London: The Chartered Institute of Public Finance and Accountancy.
- Comer, A. D. (2005) Studying Indiana Public Libraries' Usage of Internet Filters, *Computers in Libraries*, **25**(6), 10-15.
- Cooke, L., Muir, A. and Creaser, C. (2011) *Case for support: Managing Access to the Internet in Public Libraries (MAIPLE)*. Bid submitted to the Arts & Humanities Research Council, June 2011.
- Dutton, W.H. and Blank, G. with Groselj, D. (2013) *Cultures of the Internet: The Internet in Britain. Oxford Internet Survey 2013*. Oxford: Oxford Internet Surveys. URL: http://oxis.oii.ox.ac.uk/sites/oxis.oii.ox.ac.uk/files/content/files/publications/OxIS_2013.pdf [accessed 5.3.2014].
- Hamilton, S. (2004) *To what extent can libraries ensure free, equal and unhampered access to Internet-accessible information resources from a global perspective?* Copenhagen: Department of Library and Information Management, Royal School of Library and Information Science/FAIFE. URL: <http://www.ifla.org/files/faife/publications/StuartHamiltonPhD.pdf> [accessed 11.2.14].
- Hope, A. (2013) The shackled school internet: zemiological solutions to the problem of over-blocking, *Learning, Media & Technology*, **38**(3), 1-14.

-
- IFLA (2012) *IFLA Code of Ethics for Librarians and other Information Workers*. URL: <http://www.ifla.org/news/ifla-code-of-ethics-for-librarians-and-other-information-workers-full-version> [accessed 10.1.14].
- Jaeger, P. T. and Yan, Z. (2009) One Law with Two Outcomes: Comparing the Implementation of CIPA in Public Libraries and Schools, *Information Technology and Libraries*, **28**(1), 8-16.
- Jivanda, T. (2013) BT Internet filter gives parents option to block 'gay and lesbian lifestyle' content, *The Independent*, 20 Dec. URL: <http://www.independent.co.uk/life-style/gadgets-and-tech/news/bt-internet-filter-gives-parents-option-to-block-gay-and-lesbian-lifestyle-content-9018515.html> [accessed 7.2.14].
- Kranich, N. (2001) Should Public Libraries Use Filters to Block Obscenity and Pornography on the Internet? NO, *The CQ Researcher*, **7**(21), 481.
- Laughton, P.A. (2008) Hierarchical analysis of acceptable use policies, *SA Journal of Information Management*, **10**(4). URL: <http://www.sajim.co.za/index.php/SAJIM/article/viewFile/330/320> [accessed 20.2.14].
- LISU (2012) *MAIPLE (Managing Access to the Internet in Public Libraries): About Us*. URL: <http://www.lboro.ac.uk/microsites/infosci/lisu/maiple/about-us.html> [accessed 7.2.14].
- May, J. (2014) What's the best way to keep children safe online? *CILIP News*. URL: <http://www.cilip.org.uk/cilip/news/what-s-best-way-keep-children-safe-online-0> [accessed 20.2.2014].
- McMenemy, D. and Burton, P.F. (2005) Managing access: legal and policy issues of ICT use. In: McMenemy, D. and Poulter, A. (eds.) *Delivering Digital Services. A handbook for public libraries and learning centres*. London: Facet Publishing, 19-34.
- Poulter, A., Ferguson, I., McMenemy, D. and Glassey, R.J. (2009) Question: where would you go to escape detection if you wanted to do something illegal on the Internet? Hint: shush! In: *Global Security, Safety and Sustainability: 5th International Conference, ICGS3 2009*. Communications in Computer and Information Science (1st). New York: Springer-Verlag. URL: <http://strathprints.strath.ac.uk/29302/1/FRILLSisc02.pdf> [accessed 20.2.14].
- Resnick, P. J., Hansen, D. L. and Richardson, C. R. (2004) Calculating Error Rates for Filtering Software, *Communications of the ACM*, **47**(9), 67-71.
- Rt Hon David Cameron MP (2013) The internet and pornography: Prime Minister calls for action. URL: <https://www.gov.uk/government/speeches/the-internet-and-pornography-prime-minister-calls-for-action> [accessed 11.2.14].
- Simpson, B. (2008) New labor, new censorship? Politics, religion and internet filtering in Australia, *Information & Communications Technology Law*, **17**(3), 167-183.
- Spacey, R., Cooke, L., Creaser, C. and Muir, A. (2014a) Regulating internet access and content: findings from the MAIPLE project. *Journal of Librarianship*

and *Information Science*. Print version in press. URL:

http://lis.sagepub.com/content/early/2013/09/11/0961000613500688.abstract?paper_etoc [accessed 10.1.14].

Spacey, R., Cooke, L., Muir, A. and Creaser, C. (2014b) Regulating use of the internet in public libraries: a review. *Journal of Documentation*. **70**(3). Print version in press. URL:

<http://www.emeraldinsight.com/journals.htm?articleid=17101492&show=abstract> [accessed 10.1.14].

Stoker, D. (1999) Filtering out minorities. *Journal of Librarianship and Information Science*, **31**(1), 3-6.

Stol, W.P., Kaspersen, H.K.W., Kerstens, J., Leukfeldt, E.R. and Lodder, A.R. (2009) Governmental filtering of websites: the Dutch case, *Computer Law and Security Review: the International Journal of Technology and Practice*. **25**(3), 251-262.

Ybarra, M.L., Finkelhor, D., Mitchell, K.J. and Wolak, J. (2009) Associations between blocking, monitoring, and filtering software on the home computer and youth-reported unwanted exposure to sexual material online, *Child Abuse & Neglect*. **33**(12), 857-869.

Acknowledgement

MAIPLE is funded by a grant from the Arts and Humanities Research Council [AHRC]. The authors would like to thank all the public library staff who kindly completed the online survey and agreed to participate in the five case studies.

Open access and copyright

Library and Information Research is an open access journal. A freely available copy of this paper may be downloaded from the journal's website:

<http://www.lirgjournal.org.uk>.

Copyright and associated moral rights in works published in *Library and Information Research* are retained by the author(s) but this paper may be used freely, with proper attribution, in educational and other non-commercial settings.