IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 10, Issue 2, April - May 2022
ISSN: 2320 – 8791 (Impact Factor: 2.317)
www.ijrt.org

Filtering wireless (Wi-Fi) Internet access in public places

Mr. Saurabh Dixit[1],Mr. Anand Rao[2], Mr. Dheerendra Kumar[3],

[1]*Associate Professor, Department Of Computer Science & Engineering R.R. Group Of Institutions Lucknow,Uttar Pradesh,India.*
[2,3]*Assistant Professor,Department Of Computer Science & Engineering R.R. Group Of Institutions Lucknow,Uttar Pradesh,India.*

Abstract

This paper discusses selected results from the AHRC-funded 'Managing Access to the Internet in Public Libraries' (MAIPLE) project and explores Wi-Fi Internet access in UK public libraries. It investigates how this compares to commercial provision of public Wi-Fi. It discusses security issues, filtering of Wi-Fi access and acceptable use policies. A mixed methods approach was used involving a reviewof the literature, a questionnaire survey of UK public library authorities and five case studies of selected authorities. A majority of UK public library authorities offer Wi-Fi access to the public at one or more of their libraries and they generally have an authentication system in place for their users. The majority of survey respondents that provide Wi-Fi use filtering software. There are similarities and differences in the ways that public libraries and commercial outlets provide and manage access to their wireless networks. Differences mainly relate to security and privacy: these differences reflect to an extent the underlying purposes of providing public Wi-Fi accessas well as legal obligations. In some ways, public library Wi-Fi access is better managed than commercially provided public services. Evidence from the case studies suggests reluctant acceptance of filtering on the part of public library authorities, based on a perceived need to balance providing access to information with providing a safe and trusted public space for all.

Keywords

Acceptable use policy, filtering, public libraries, Wi-Fi access

Introduction

The purpose of this article is to review the ways in which public library authorities in the UK are implementingWi-Fi access, and the measures that they are taking to reg- ulate content that may be viewed as harmful or otherwise contrary to the terms of their acceptable use policy (AUP). The article considers selected results from the 'Managing Access to the Internet in Public Libraries' (MAIPLE) pro- ject[1] undertaken by a team at Loughborough University and funded by the Arts and Humanities Research Council(AHRC)

(Dutton et al., 2013). According to the OII, this has been the greatest change in Internet use (Dutton et al., 2013). Figures from the Office for National Statistics (ONS) alsoillustrate this trend. According to the ONS, access to the Internet using a mobile phone rose from 24% of British adults in 2010 to 53% in 2013 in the UK. This has been aided by the increasing number of Wi-Fi hotspots which are 'now regularly seen at locations such as pubs, cafes and hotels' (ONS, 2013: 12).

In 2013, several high profile announcements were madein relation to publicly available Wi-Fi access. These fol- lowed developmental work by the UK Council for Child Internet Safety (UKCCIS), a group of more than 200organisations working in partnership to help keep children safe online. The first meeting of the UKCCIS Board was held in early 2012 and included Members of Parliament and representatives from industry and relevant charities working in the field (UKCCIS, 2012). The minutes of thatboard meeting mentioned three main areas that the public Wi-Fi project would include: retail; public places, includ-ing 'libraries'; and private/public Wi-Fi access (UKCCIS,2012: 4). The public Wi-Fi strand has been led since July 2012 by Anne Heal from BT Openzone. By February 2013 Heal reported that progress had been made with the six largest UK public Wi-Fi providers, 'who together account for upwards of 96 per cent of public

from 2012 to 2014. MAIPLE explored the ways in which public library s

According to the Oxford Internet Institute (OII) Internetuse in the UK is still rising. The most recent Oxford Internet Survey (OxIS) found that the Internet is now usedby 78% of the British population; this is up from 73% in 2011 (Dutton et al., 2013). Furthermore, accessing the Internet on a mobile device has risen from 20% of all Internet users in 2009, to 40% in 2011,

media stories (Gibbs, 2013) based on an initial *Daily Mirror* newspaper investigation suggested progress was patchy: 'But a test of 129 free wifihotspots around the UK including shops, cafes and chil- dren's play areas has found that 32 of them did not block access to pornhub.com, a free website that streams hard- core pornographic videos' (Wales Online, 2013). It is not clear what the situation is now, but the Friendly WiFi web-site allows people to report any instances of access to material that should be blocked (RDI, 2014).

The introduction of Internet access in public librariesin the UK was heralded with a fair amount of publicity and was funded by national lottery monies in the early 2000s. The £100m People's Network (PN) saw all static public library points connected to the Internet by 2002. By 2003, there were approximately 30,000 PCs with Internet access in UK public libraries (Sommerlad et al., 2004). Unlike the PN, the adoption of wireless access has not been a national initiative; to date it has been left to individual public library authorities. However, in March 2015 in a pre-election budget speech, the Chancellor George Osborne announced that £7.4m funding was to bemade available 'to give wi-fi access to all public libraries across England' (Farrington, 2015).

Although there has been an extensive body of aca- demic research carried out internationally on the subject of public libraries and Internet provision, particularly with regard to the difficult issue of content filtering, it is not the purpose of this paper to review this literature:this has been carried out elsewhere (see Spacey et al., 2014). In their review Spacey et al. (2014) note the dif- ficulty in obtaining precise up-to-date

information with regard to UK public libraries and filtering: for example, prior to the MAIPLE project, the most recent UK-wide survey of the use of filtering software in public libraries was the NETbase survey carried out in November 2002 (Brophy, 2003). More recent research has been carried out in Scotland, where Brown and McMenemy (2013) found that 31 out of 32 public library authorities in the country filtered their Internet access. However, there appears to have been no research to date exploring Wi-Fi provision by UK public libraries, with the excep- tion of some surveys mapping the extent of its provi- sion. Insight Media Internet Limited commissioned research in this area in late 2008. Completed from 92 public library authorities (43% of all UK public library authorities) revealed that 47% had already implemented Wi-Fi, 28% were planning to implement it and 25% were not (Insight Media Internet Limited, 2009). Batt (2009) focused on data from three sources: the Review and Evaluation of WiFi in Public Libraries 2006 (MLAC and RegenerateIT), Review and Evaluation of WiFi Services in United Kingdom Public Libraries 2009 (Insight Media Internet Limited) and the National Wi-Fi in Libraries Survey 2009 commissioned by RegenerateIT and conducted by Civic Regeneration and Chris Batt Consulting. From these three sources Batt observed that there had been a significant increase over the period 2006 to 2009 of public library Wi-Fi provision. More recently, research by the Reading Agency (2011: 8) found that: 'Three in five (59.6%) authorities now offer Wi-Fi access in their libraries'. Figures from the Chartered Institute of Public Finance and Accountancy (CIPFA) show that in March 2012, there were 909 public library service points in England, 103 in Wales, 171 in Scotland and 3 in Northern Ireland offering Wi-Fi (CIPFA, 2012). CIPFA estimated, based on the 96% response rate to their survey, that there were 4384 service points in the UK altogether, which sug- gests that 27% of public libraries offered Wi-Fi. By March 2013, this had increased to 1176 in England, 170 in Wales, 204 in Scotland and three in Northern Ireland out of 4313 service points (CIPFA, 2013). According to CIPFA, approximately one-third (36%) of public librar- ies in the UK now offered Wi-Fi.

In terms of the management of UK public library Wi-Fi, Insight Media Internet Limited (2009) reported that the majority of public library authorities provided or were going to provide Wi-Fi for registered library members and casual users. For 84% of public library authorities, the hot- spot provided filtered access to the Internet and for 67% of public library authorities this filtering would be the same as for fixed connections in libraries.

Adaptive Mobile undertook an investigation into public Wi-Fi. The resulting publication Courting Trouble: Why WIFI Hotspots Need to be Part of the Safety Debate (Adaptive Mobile, 2013) reports research using mystery shoppers. The research looked at Wi-Fi hotspots in cities in the UK – London, Birmingham and Manchester – and in the USA. Locations included a total of 179 cafes, hotels, shops, restaurants and public spaces, including libraries and train stations. Public space hotspots were 'the most aggressive blockers of content but still nearly 1 in 10 allowed access to pornography' (Adaptive Mobile, 2013: 9). They were also the locations where over-blocking was most likely to occur: 'Half of all retail and public space Wi-Fi hotspots blocked access to a hidden word site, com- pared with only two in every 10 cafes and restaurants and one in 10 hotels' (Adaptive Mobile, 2013: 12). From an international perspective, a 2014 investigation reports responses from more than 3500 people across more than 40 countries, finding that in relation to content control, 41% had filtering in place, 33% did not and 26% did not know (Purple Wi-Fi, 2014).

Batt (2009) noted that according to the 2009 surveys, around one-third of libraries with Wi-Fi were using the Library Management System (LMS) to authenticate users whilst the National Wi-Fi in Libraries Survey 2009 asked if Wi-Fi signals extended beyond the library (hotspots) – 30% were aware that the signal did reach beyond the library and 28 of 61 libraries with Wi-Fi hotspots (45%) required a user name and password for access.

Wi-Fi access in public libraries is increasingly part of the landscape of publicly available access to mobile Internet connections. However, there is a lack of research on how public library authorities manage access to their Wi-Fi Internet connections. Commercial organisations also provide Wi-Fi as a service to their customers. Whether this access is free of charge or paid for, the underlying rationale for this provision is usually business related. As a publicly funded service, public libraries face some chal- lenging decisions in managing Internet access. Public library authorities have a potential conflict between differ- ent roles (Goulding, 2006). This is particularly evident in the duty of public libraries to facilitate access to informa- tion for all and in protecting young people from harm (Chartered Institute of Library and Information Professionals (CILIP), 2012). There is a lack of research exploring whether public library authorities have anything to learn from commercial provision of public Internet access in this regard.

In making decisions about how they manage access to library Internet connections, public library authorities have to balance their legal obligations and deal with the ethical dilemmas arising from meeting the needs of differ- ent members of their communities (Cooke et al., 2014). UK public services have legal obligations under the United Nations Convention on the Rights of the Child (1989) and there are several pieces of legislation, including the Children Acts (Great Britain, 1989, 2004), the Children (Scotland) Act (Great Britain, 1995a) and the Children (Northern Ireland) Order (Great Britain, 1995b), which require cooperation by public agencies to protect children. The UK is a signatory to the European Convention on Human Rights 1950 (ECHR), including the right to free- dom of expression, which encompasses imparting and receiving information and ideas (Art. 10(1)). The Society of Chief Librarians (SCL, 2014) has developed the con- cept of the Universal Offer for public libraries. Two of the four key service areas that form the basis of the Universal Offer are the Information and Digital Offers, which focus on supporting citizens in accessing information through digital services. The Information Offer recognises that citi- zens increasingly need to go online to interact with public services. Ethical codes for information professionals

reflect a commitment to equitable access to information for all as well as a concern for public good (CILIP, 2012, 2014; International Federation of Library Associations and Institutions (IFLA), 2014).

Research aims and methodology

The aims of the MAIPLE project were addressed through a mixed methods approach involving a review of the litera- ture, a questionnaire survey and case studies in five public library authorities, based primarily on interviews with staff and users. Analysis of commercially provided public Wi-Fi provision was carried out through desk research.

The questionnaire survey was hosted online using Bristol Online Surveys in January and February 2013. An email invitation was sent to the appropriate contact for every public library authority in the UK. Two email reminders were sent to non-responders. In total, 80 responses were received from a potential 206 services, a response rate of 39%. The distribution of responses from the constituent parts of the UK were as follows: 75% of respondents were from English public library authorities, 15% were from Scottish authorities, 8.8% were from Welsh authorities and 1.3% of the response was from Northern Ireland (which is covered by a single public library authority).

The case studies were designed to explore how public library authorities regulate access to their Internet con- nections in more detail. This involved a combination of analysis of policy documents and other relevant material; interviews with key stakeholders such as IT managers and library personnel; and interviews with users. Cases were selected on the basis of survey respondents indicat- ing their willingness to be included in the study, and their geographical location. Five sites were eventually selected and agreed to participate in the study. Two case study authorities were in England, one in Scotland, one in Wales and Libraries NI also participated. Public library authorities varied in size ranging from four libraries to almost 100.

In addition, the project aimed to collect and analyse qualitative data concerning the management and regula- tion of access to Wi-Fi by commercial Wi-Fi access pro- viders, such as cafés, shops and public transport. It was judged appropriate to use secondary data to scope the landscape with regard to publicly available Wi-Fi and the desk research was undertaken in early 2014. This included a thorough search of the literature available in the public domain on the Internet and in academic journals. It also included consideration of published policies and terms and conditions of the main commercial Wi-Fi Internet ser- vice providers as well as a number of well-known com- mercial outlets that the public might reasonably come across in a UK town or city providing access to these services.

According to the Department for Education and the Department for Culture, Media and Sport, the six main commercial Wi-Fi Internet service providers in the UK are: BT; O2; Virgin Media; Sky (The Cloud); Nomad; and Arqiva (DCMS, 2013). BT is the major provider and has more than 5 million hotspots in the UK (BT Wi-fi, n.d.a), whereas The Cloud has more than 200,000 hotspot loca- tions in the UK (The Cloud, 2014a).

BT Wi-fi, formerly known as BT Openzone, provides hotspots throughout the UK for its customers. BT is also used by corporate clients such as the retailers John Lewis and Fenwicks and catering outlets Starbucks and Burger King. O2 Wifi is used by global brands such as Costa Coffee, Debenhams, McDonalds, Tesco, Subway and Pizza Hut. The Cloud is used by Pizza Express, Marks and Spencer (M&S), WH Smith, Cafe Nero, Wetherspoon pubs and Network Rail. Nomad Digital is a service pro- vider to the transportation industry and customers in the UK include East Midlands Trains and Virgin Trains (Nomad Digital Ltd, 2013). London Underground's wire- less Internet is provided by Virgin Media. Formerly known as Spectrum Interactive, Arqiva provides Internet services to the Whitbread restaurant brand, Brewers Fayre and some UK airports, including London Heathrow.

There are similarities and differences in how Wi-Fi Internet service providers regulate use of their wireless net- works. End users (members of the public) must usually reg- ister or set up an account for the service, even if it is offered free of charge. The Cloud requires that users create an account, providing contact details, mobile phone number and date of birth. Registered users then enter an email address and a password to access the service. Users may be exposed to marketing material on The Cloud landing pages, depending on where they access the service. O2 provides free Wi-Fi access to anyone, but also requires that people register for the service, providing contact details and date of birth. Once registered, users can connect to an O2 hot- spot without having to input user names or password. However, access to the free service is denied unless the user consents to receiving marketing material from O2 and 'selected third parties'. According to its terms and condi- tions, Virgin Media only contacts end users or passes per- sonal data to third parties with the consent of those users.

The Wi-Fi networks of these Internet service providers are generally not encrypted and information passing across such open networks could be intercepted. Not all of the some reference to security precautions in its terms and conditions, but does not provide detailed advice.

The Wi-Fi Internet service providers take slightly differ- ent approaches to implementing and publicising filtering. For example, Virgin Media's publicly available documen- tation only indirectly refers to filtering in a FAQ, saying 'Virgin Media has a responsibility to ensure that the content available is suitable for young people to access themselvesor to look at over someone else's shoulder' (Virgin Media, 2012a). It is not clear whether Nomad provide filtered Internet content to their UK customers. O2's Wifi service has been subject to content filtering since its inception in 2011, claiming to be the first in the industry to do so (O2, 2013). The Cloud's service is filtered by default, but their corporate customers may opt out if they wish. According to The Cloud website page on staying safe online, 'content filtering system is provided by an independent third-party called SonicWALL, which classifies websites into pre- defined categories based on its own guidelines and is done via automated system' (The Cloud, 2014b). Page 4 of the AUP notes that it relies on URLs provided by IWF as wellas URLs relating to drug use, pornography, offensive or illegal speech, and network malfeasance (The Cloud, 2014c). The AUP also directs users to a SonicWALL webpage to check on the status of individual sites which may be blocked. SonicWALL produces Internet content control appliances and was acquired by Dell in 2012. Categories blocked by default are violence, hate and racism, pornogra- phy, illegal drugs, hacking and proxy avoidance, criminal and illegal skills and nudity. There is no mention of filtering in Arqiva's terms and conditions (Arqiva, 2014a, 2014b). However, according to a writer for the website thinkbroad-band.com, who contacted Arqiva in June 2013, Arqiva 'apply content filtering in accordance with the clients' requirements. Where no requirements are specified by theclient, we implement "family-friendly" content filtering as a default' (Ferguson, 2013). BT Wi-Fi is unusual in that itoffers its customers or partners the opportunity to restrict access but filtering is not a default option, or a feature which is actively promoted. BT offer BT Wi-fi Protect which conforms to the UK Government-driven family friendly public Wi-Fi initiative allowing 'our wi-fi partnersto restrict access to pornographic websites' (BT Wi-fi, n.d.c). Emphasised as a benefit, this product 'allows BT Wi-fi site partners who choose to apply content filtering, toblock access to pornographic material' (BT Wi-fi, n.d.c).

Public Wi-Fi Internet access providers

Wi-Fi Internet access is increasingly available in public places in the UK. Many businesses provide Wi-Fi access to their customers using one of the Wi-Fi Internet service providers described above. Most of the public library authorities included in the MAIPLE project provide their

own Wi-Fi services, but there was evidence that authorities also use commercial service providers.

Customers of the commercial outlets which provide Wi-Fi access on their premises are usually subject to the conditions of the Wi-Fi Internet service provider or to terms and conditions agreed by the service provider and the access provider. However, East Midland Trains First Class passengers usually do not need to do anything other than tick a box to confirm acceptance of the service terms and conditions, which is offered free as part of the First Class service. Customers travelling in Standard Class car- riages have to provide more information, as Wi-Fi access is charged for. The Virgin London Underground service is free to Virgin Media customers and available to other travellers by purchasing a Wi-Fi pass (Virgin Media, 2012b).

More than four-fifths of responding public library authorities offer Wi-Fi access to the public at one or more of their libraries. At the time of the case study research, three (out of five) case study sites did so, and staff per- ceived that it had been well received. They saw people in the library using mobile devices. In one case, the Head of Libraries commented that:

whereby we think that we need to reorganise the layout of the

Over half of the public library survey respondents pro- vide secure Wi-Fi access, using WPA or WPA2 protocols (59.7%). However, approximately one-quarter of respondents did not know (25.4%) and 10 services do not provide secure access (14.9%). This is in contrast to other public Wi-Fi services, which are usually unencrypted. An exception is Heathrow Wi-Fi, provided by Arqiva, which is protected by '256 SSL encryption'. The Heathrow Wi-Fi FAQ also provides advice to users on how to mini- mise security risks when using the service (Heathrow Airport, n.d.).

Of the 67 public library survey respondents that provide Wi-Fi Internet access, the majority filtered this access (83.6%). Interviewees at the case study sites made various observations about how their Wi-Fi is provided and their assumptions about their responsibilities for its provision and how it should be used. For example, at one site, the fact that both fixed and wireless connections are filtered is not advertised to users. At another, where Wi-Fi is pro- vided, filtered and managed via The Cloud, it was made clear that: 'it's a privately provided service, it's not a Council provided service'. Another approach taken by a case study site is for Wi-Fi access to be filtered at the same level that is used for children:

The only difference being because I have no control over where you sit in the library: as an adult you will be filtered as a child if you're using your own device just because you could be sitting beside a child.

The main public Wi-Fi access providers take slightly different approaches to implementing and publicising fil- tering. The London Underground approach to filtering is similar to the case study library which applies filtering suitable for children to all users. For example: 'As WiFi on the London Underground is a public WiFi network, Virgin Media has a responsibility to ensure that the content avail- able is suitable for young people to access themselves or to look at over someone else's shoulder' (Virgin Media, 2012a). By contrast, it is not clear whether Nomad provide filtered Internet content to their UK transport customers. There is no mention of filtering in East Midland Trains' terms and conditions, but there is a content disclaimer which advises:

East Midlands Trains does not control, nor is it in any way liable for, data or content that you access or receive via the service. The Internet contains unedited materials, some of which are sexually explicit or may be offensive to you. East Midlands Trains has no control over and accepts no responsibility for such materials. (East Midlands Trains, 2013: 4.1)

Corporate customers may opt out of The Cloud's filtering by default if they wish. Filtering is specifically referred to in relation to Internet kiosks located in hotels and airports: Heathrow Airport makes it very clear that the service is

building to deal with it.

Of the five case study sites, two were waiting for Wi-Fi to be installed. Staff in one case anticipated it would be widely used because people now expect this. In the other case, there had been enquiries from the public about Wi-Fi access.

The questionnaire survey responses showed that a PIN or password is the most popular requirement to use Wi-Fi connections in public libraries: for library members (61.2% of respondents offering Wi-Fi connections) and for non- members (39.6% of respondents). Almost half (49.3%) of responding services require library members to have their borrower number, although in almost one-fifth of respond- ing services (19.4%) no authentication is required. There was no clear trend in how libraries treat casual library users in terms of authentication. The options of requiring proof of identity (28.3%) and requiring no authentication (26.4%) drew similar numbers of responses. Analysis of the comments submitted by respondents selecting 'other' means of access control revealed that requirements include email address (5), a mobile telephone number (2), use of a guest card/log-in (2), accepting the AUP or Internet use policy (2), setting up an account (1) or adhering to the Wi-Fi Internet service provider's terms and conditions (4). Approximately four-fifths of the responding public library services show Wi-Fi users a special web page on which to log-on/authenticate before using the Internet, known as a captive portal (80.6%).

filtered; highlighting its family friendly credentials in its Wi-Fi FAQs (Heathrow Airport, n.d.).

Internet use in public libraries is governed by an AUP (98.8% of MAIPLE survey respondents) or terms and con- ditions which stipulate what may and may not be viewed whilst using the Internet. This method is supplemented by others, including visual monitoring of screens. However, use of a library's Wi-Fi connection on a user's handheld device or mobile phone means that, unlike stand-alone net- worked PCs, library staff and other library users are unable to see easily what the user is viewing. This will almost always be the case for commercial public Wi-Fi access providers. Terms and conditions of use and AUPs are also used by these commercial outlets to set out what users may and may not do using their connections. Public library Internet users are alerted to the AUP in a number of differ- ent ways. In over four-fifths of services, library users are made aware on a log-in screen (89.9%) whilst in just under half of responding services, there is information on the library website (48.1%). Public library AUPs proscribe use of Internet connections for criminal and other unlawful activity. This includes viewing, uploading or downloading obscene content, copyright infringement, hacking, dissem- ination of malware or viruses, bullying and harassment and viewing violent, extremist or hate content. AUPs also cover issues such as causing damage to equipment, stream- ing live TV, using up excessive bandwidth and using other people's details to log-in to the system.

Access to, and use of, commercially provided public Wi-Fi connections are also subject to terms and conditions, usually those of the Wi-Fi Internet service provider. As with public library AUPs, there are similarities across different service providers, the major difference being in the amount of detail given. The O2 Wifi Terms of Service document is available on the O2 website. It notes that access to some types of content will be subject to age verification and that O2 will decide what content to classify as suitable for adults only. If a user does not agree with the classification of a particular site they are able to contact O2 by email 'to raise concerns' but ultimately 'if you don't agree with our classi- fication then you are free to stop using the service at any time' (O2 Wifi, 2014: 1). Prohibited activities online are 'unlawful, fraudulent, criminal or otherwise illegal activi- ties' (O2 Wifi, 2014: 3), which include uploading and/or downloading material which is offensive, obscene or unlaw- ful or breaches copyright or intellectual property rights. The Virgin Media WiFi site's FAQs refer to its Terms and Conditions which 'vary depending on which [access] pro- vider you connect with' (Virgin Media, 2012a). The Virgin Media AUP (2014) states clearly that the connection must not be used for unlawful purposes (3.1) and use must com- ply with all relevant laws (3.2). Additionally, 'You must not use our services in any way that is unlawful or illegal or in any way to the detriment of other Internet users' (3.1) (Virgin Media, 2014: 1). The Virgin Trains Wifi FAQs

advise users that: 'as you are sitting in a public environment, please do not view content that others may find offensive or inappropriate' (Virgin Trains, 2014: 2). More direct control is indicated for some prohibited content, including material that is regarded as 'threatening, harassing, invasive of pri- vacy, discriminatory, defamatory, racist, obscene, indecent, offensive, abusive, harmful or malicious', material that 'infringes or breaches any third party's intellectual property rights', material that is in violation of any UK law or regula- tion, etc., whereby '[a]t our sole discretion (and without prejudice to any of our other rights pursuant to this AUP and our terms and conditions), we reserve the right to remove any material from any server under our control' (Virgin Trains, 2014: 2). The Cloud has an AUP (The Cloud, 2014c) and users agree to its terms and conditions by pressing a 'continue' button (p.1). Section 4.5 states:

[y]ou agree to indemnify us against all losses, liabilities, costs (including legal costs) and expenses which may incur as a result of third party claims against us arising from, or in connection with, your misuse of the WiFi Service or breach of this Contract. (The Cloud, 2014c: 2)

They request that Wi-Fi users 'Don't use the WiFi Service illegally!' (The Cloud, 2014c: 4) and that users do not use the Wi-Fi service to 'send, receive, store, distribute, trans- mit, post, upload or download any materials or data which violates any law, is defamatory … or may be harmful to minors', amongst other stipulations (The Cloud, 2014c: 4). Nomad provides Wi-Fi access for East Midlands Trains (Nomad Digital, 2012). East Midlands Trains' customers see what appear to be the train company's terms and con- ditions. These stipulate that users do not 'use the service for anything unlawful, immoral or improper' (3.1a), or 'use the service to harm or attempt to harm minors in any way' (3.1c) and that 'the service is used in accordance with any third party policies for acceptable use or any rel- evant internet standards (where applicable)' (3.1g) (East Midlands Trains, 2013: 1). There is also a disclaimer of liability for the content accessed or downloaded using the service, and a warning that users may come across explicit and/or offensive content (4.1) (East Midlands Trains,
2013: 2).
The BT Wi-fi AUP (BT Wi-fi, n.d.d) details a number of prohibited uses which include illegal/criminal activity such as infringement of intellectual property; security vio- lations; spamming; obscene or offensive content and threatening or offensive behaviour. Additionally users should not 'transmit to recipients material which is inap- propriate for them, including obscene or offensive materi- als to children' (BT Wi-fi, n.d.d: 2). If BT detects a violation of their policy they may take action; however, they attempt to reassure the user that 'it is not our intent to monitor, control, or censor communications on the BT Network' (BT Wi-fi, n.d.d: 3). Interestingly, filtering may be used in response to a violation:Violations of this Policy may result in a demand for immediate removal of offending material, immediate temporary or permanent filtering, blocked access, suspension or termination of service, or other response appropriate to the violation, as we determine in our discretion. (BT Wi-fi, n.d.d: 3)

In 2009, Starbucks began offering BT Wi-fi in their coffee shops, free to those with a Starbucks reward scheme card. In 2011, this qualifier was removed and Starbucks rolled out free BT Wi-fi in all of its UK stores. Users have to accept the terms and conditions of using the Wi-Fi on a pop-up screen. Starbucks was the subject of some controversial media cover- age in 2012 (e.g. see Martin, 2012) when it was revealed that customers were able to view pornographic material. In 2013, Starbucks moved to filter pornographic content. The Starbucks website does not mention filtering or acceptable use. BT has been working with Mumsnet as part of the UK's Friendly WiFi programme. Mumsnet is a UK-based inde- pendent network for parents, providing support and advice on matters of concern, including child safety online (Mumsnet, 2012). The Arqiva AUP is available on its website (Arqiva, 2014a). The AUP sets out prohibited uses including storing, sending or distributing copyright materials, anything

Discussion

There are similarities and differences in the ways that pub- lic libraries and commercial outlets provide and manage access to their wireless networks. The differences mainly arise when considering security, convenience and privacy. For example, most of the public library respondents to the questionnaire survey encrypt their wireless networks. It may be that the respondents who did not know if they used encryption also did in fact do so. This is not generally the case for public hotspots, making them potentially more risky for the public, especially for people who are not adept at managing security on their devices. Public library authorities who provide their own Wi-Fi services to the public can do so with minimal requirements with regard to processing of personal data. They have a public service remit and are not trading off a free service for access to personal data for marketing purposes.
Public libraries have particular legal and ethical obliga- tions and expectations to fulfil in providing Internet ser- vices. Key considerations are the obligation to safeguard children and the expectation that a public library is a safe and inclusive place (Leckie and Hopkins, 2002). Public concern for children is also reflected in commercial provi- sion of filtered Wi-Fi: being a member of the friendly Wi-Fi scheme can be a commercial benefit for these Wi-Fi so the question of the core purpose of a public library, which is to provide access to information for all, for the benefit of members of the community who would not otherwise have access to that information (Goulding, 2006).
Most of the public library survey respondents filter access to content online. The major Internet service pro- viders also filter their services. Public libraries are part of local government authorities which also provide education and social services and have legal as well as corporate responsibilities to protect children. Commercial service and access providers may not have the same legal respon- sibilities but they are still subject to moral pressure by par- ents and government to filter access to content available via Internet connections.
The MAIPLE research indicates similarity in the cate- gories of material blocked by public library and commer- cial public Wi-Fi services. While libraries providing their own Wi-Fi networks can potentially apply different levels of filtering according to member categories, it may be pos- sible for children to see 'adult' content on the screens of mobile devices if Wi-Fi connections are available freely throughout library spaces. If they use commercial service providers, they may not have (willingly or not) any control over how Wi-Fi access is filtered. Commercial Wi-Fi ser- vice and access providers may not be concerned over issues of freedom of access to lawful content for adults. It could be argued that if public library authorities apply the strictest filtering for all users of Wi-Fi connections, they are infringing people's fundamental right to receive and impart information. The obligation of public libraries to protect children and to be a safe place for them effectively overrides the right of adults to access to lawful information without undue hindrance.
Evidence from the MAIPLE case studies shows accept- ance of filtering by library staff and users, even if this acquiescence is sometimes reluctant. The participating library authorities in the project do provide opportunities for users to complain if they feel that something has been blocked in error and to ask for it to be unblocked. This is not clearly the case for the commercially provided public Wi-Fi services. Indeed, the O2 approach is more or less take it or leave it. The responses from survey and case study participants indicate that the process of having sites unblocked is not as straightforward as it might be and deci- sions could be made closer to the point of use. The research findings suggest that public library authorities are prepared to accept these restrictions to maintain public libraries as safe and trusted public spaces.

Conclusions

It is not clear from the data collected during the MAIPLE project that public libraries have much to learn from public Wi-Fi providers. In some ways, the public library servicesare better managed and more concerned with the best interests of the users, particularly when it comes to secu- rity and targeting users for marketing purposes. This is understandable given the different purposes of public libraries and commercially provided public Wi-Fi.

Some public library authorities use external service providers in the same way that businesses do and this may well increase over time. If this happens, library authorities may not have direct control over filtering, which may have freedom of expression implications for users depending on agreements between authorities and Wi-Fi providers.

Filtering of Internet content in libraries arguably goes against the professional ethics of librarians. The point could be made that libraries have always censored; they have never been able to provide access to everything and they have sometimes chosen to exclude material from their collections. This argument does not really justify filtering Internet access, because it is possible to provide access to all lawful material that is publicly available on the Internet. As highlighted in one of the project case studies, public library authorities could devote attention to library space design and seating arrangements to address the difficulties raised by wireless access to library Internet connections.

Data gathered during the MAIPLE project suggest that library staff, in the main, take decisions based on a balanced appraisal of the right to information and the feelings of peo- ple offended by what they see on the screens of other library users. It would appear that users understand and accept these limitations to their information access. However, it would also appear to be the case that current arrangements can lead to denial of access to lawful content and services for adults. Decision-making in this respect may increasingly be taken out of the hands of librarians, and be left to the altogether less transparent arena of Internet service provid- ers. The latter, moreover, are not immune to the interven- tions of those in the UK political sphere, such as the Prime Minister's 'opt-in' filtering intervention (Strange, 2013). The fight for greater public library autonomy and transpar- ency in decision-making may be where the real future battle lies, rather than an already lost fight against filtering per se.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Adaptive Mobile (2013) Courting Trouble: Why WIFI Hotspots Need to be Part of the Safety Debate. Dublin: Adaptive Mobile (report available upon request).

Arqiva (2014a) Acceptable Use Policy for WiFi Services. Available at: http://www.arqiva.com/support/wifi/acceptable-use- policy.html (accessed 3 November 2014).

Arqiva (2014b) Terms & Conditions for WiFi Services. Available at: http://www.arqiva.com/support/wifi/terms-and-conditions. html (accessed 3 November 2014).

Batt C (2009) WiFi in the UK's Public Libraries Survey 2009: From Punched Tape to WiFi and Beyond. London: Civic Regeneration. Available at: http://ebookbrowse.com/gdoc. php?id=106129795&url=740af855763c9fbbd97903560391 9b2a (accessed 25 May 2015).

Brophy P (2003) The People's Network: A Turning Point for Public Libraries. London: Resource.

Brown GT and McMenemy D (2013) The implementation of Internet filtering in Scottish public libraries. Aslib Proceedings 65(2): 182–202.

BT Wi-fi (n.d.a) Find a Hotspot. Available at: https://www. btwifi.co.uk/find/ (accessed 3 November 2014).

BT Wi-fi (n.d.b) Security when Using BT's Wi-fi Hotspots. Available at: https://www.btwifi.co.uk/help/security/index. jsp (accessed 4 March 2014).

BT Wi-fi (n.d.c) BT Wi-fi Protect. Available at: http://www. btwifi.com/Media/pdf/WIFI_PROTECT_250313_wifi.pdf (accessed 4 March 2014).

BT Wi-fi (n.d.d) Terms and Conditions. BT Wi-fi Acceptable Use

Policy (including BT Openzone). Available at: http://www. btwifi.com/terms-and-conditions/acceptable-use-policy.jsp (accessed 3 November 2014).

Chartered Institute of Library and Information Professionals (2012) Code of Professional Practice. Available at: http://

Chartered Institute of Library and Information Professionals (2014) Ethics. Available at: http://www.cilip.org.uk/cilip/ about/ethics (accessed 10 February 2015).

Chartered Institute of Public Finance and Accountancy (2012) Public Library Statistics: 2012–13 Estimates & 2011–12 Actuals. London: CIPFA

Chartered Institute of Public Finance and Accountancy (2013) Public Library Statistics: 2013–14 Estimates & 2012–13 Actuals. London: CIPFA.

The Cloud (2014a) Get Fast, Reliable and Free WiFi from The Cloud. Available at: http://www.thecloud.net/free-wifi/get- the-app/ (accessed 3 November 2014).

The Cloud (2014b) Stay Safe Online. Available at: http://www. thecloud.net/free-wifi/wifi-security/ (accessed 3 November 2014).

The Cloud (2014c) UK WLAN Terms and Conditions. WiFi Hotspots from The Cloud. Available at: http://www. thecloud.net/free-wifi/uk-wlan-terms-and-conditions/ (accessed 3 November 2014)

Cooke L, Spacey R, Muir A, et al. (2014) Filtering access to the Internet in public libraries: An ethical dilemma? In: Ethical dilemmas in the information society: Codes of ethics for librarians and archivists. Papers from the IFLA/ FAIFE satellite meeting (eds A Valloton Preisig, H Rösch and C proactive-approach-to-seek-out-child-sexual-abuse-content (accessed 14 February 2014).

Dutton WH and Blank G with Groselj D (2013) Cultures of the Internet: The Internet in Britain. Oxford Internet Survey 2013. Oxford Internet Institute, University of Oxford. Available at: http://oxis.oii.ox.ac.uk/blog/oxis-2013-top- line-findings-internet-use-continues-grow-big-increases- low-income-households#sthash.1Uzgrka8.dpuf (accessed 14 February 2014).

East Midlands Trains (2013) Wi-Fi Terms and Conditions. Available at: http://www.eastmidlandstrains.co.uk/information/contact-us/policies-procedures/Wi-Fi-Terms-and-Conditions/ (accessed 14 February 2014).

Farrington F (2015) All libraries in England to get wi-fi fund- ing. The Bookseller, 19 March. Available at: http://www. thebookseller.com/news/all-libraries-england-get-wi-fi- funding (accessed 23 March 2015).

Ferguson A (2013) Arqiva announces winning exclusive con- tract with several London boroughs. Thinkbroadband.com, 10 June. Available at: http://www.thinkbroadband.com/ news/5876-arqiva-announces-winning-exclusive-contract- with-several-london-boroughs.html (accessed 3 March 2014).

Gibbs S (2013) Porn, knives and drugs websites accessible on most public Wi-Fi. The Guardian, 25 September. Available at: http://www.theguardian.com/technology/2013/sep/25/ porn-knives-and-drugs-websites-accessible-on-most- public-wi-fi (accessed 14 February 2014).

Goulding A (2006) Public Libraries in the 21st Century: Defining Services and Debating the Future. Aldershot: Ashgate.

Great Britain (1989) Children Act 1989. Chapter 41. London: HMSO. Available at: http://www.legislation.gov.uk/ukpga/1989/41/contents (accessed 19 March 2015).

Great Britain (1995a) Children (Scotland) Act 1995. Chapter 36. London: HMSO. Available at: http://www.legislation.gov.uk/ukpga/1995/36/contents (accessed 19 March 2015).

Great Britain (1995b) Children (Northern Ireland) Order 1995. London: HSMO. Available at: http://www.legislation.gov.uk/nisi/1995/755/contents/made (accessed 2 June 2015).

Great Britain (2004) Children Act 2004. Chapter 31. London: HMSO. Available at: http://www.legislation.gov.uk/ukpga/2004/31/pdfs/ukpga_20040031_en.pdf (accessed 19 March 2015)