"An absolute prerequisite": The importance of user privacy and trust in maintaining academic freedom at the library

Lisa Sutlieff and Jackie Chelin

December 2008

From a dissertation submitted November, 2007 (Fieldwork completed June – August, 2007)

Lisa Sutlieff, BA, MSc
Information Manager

The Childcare Company / LASER Learning Ltd
Tithe Barn
Tithe Court
Langley
Berkshire
SL3 8AS

Tel: 01753 596004
lisa@thechildcarecompany.com

Jackie Chelin, BA, Dip Lib, PGC(HE), MCLIP
Deputy Librarian and
Module Leader on the MSc Information and Library Management programme
University of the West of England
Frenchay Campus Library
Coldharbour Lane
Bristol
BS16 1QY

Tel: 0117 32 83768
Jacqueline.chelin@uwe.ac.uk

About the Authors

Lisa Sutlieff is Information Manager at The Childcare Company and LASER Learning Ltd, which provide vocational training to nursery practitioners. She is currently working towards CILIP Chartership.

Jackie Chelin is Deputy Librarian at the University of the West of England where she has worked for 15 years in various capacities. She is one of the module leaders on the MSc in Information and Library Management, having taught on the course since its inception over 12 years ago, and helped to transfer it from the University of Bristol to UWE.

Abstract

This research investigated the importance of user-library trust in ensuring vital freedom of inquiry in academic libraries. It explored the strength of user-library trust, through comparison with attitudes towards the National Identity Card Scheme (NICS), within the various libraries of a large UK university.

Comprising an online survey of students and interviews with librarians, student opposition to the NICS, and distrust of the Government was revealed. Measurement of pre-existing privacy opinions linked opposition to NICS with concerns about privacy. Students, however, were confident in library data protection practices, although some surprising discrepancies existed between user perceptions and library practices.

Libraries successfully protected personal data from intrusion, but showed a certain complacency and reluctance to prioritise data protection that may be ill-advised given a climate of increasing surveillance.

Librarians are advised to promote institutional privacy awareness as proactive data protection 'champions' in order to maintain the current "privilege" they have of user trust.

The adaptation of the Westin method for measuring pre-existing privacy concerns proved a more accurate tool than the original and may be of benefit for others undertaking similar research.

Keywords: Data protection, privacy, identity cards, academic freedom, trust, library policy.

Introduction

This study assessed privacy practices, perceptions and awareness, in the various libraries of a large UK university. If academic libraries depend on trust in privacy from users (Bowers, 2006; Coombes, 2004), it made good sense to explore the strength of this trust, whether it is deserved, and how it can be protected.

Aim

The aim of the research was to explore the strength of the user-library trust relationship in academic libraries, with regard to the storage and use of personal information, and to add to academic discourse about privacy and libraries at a time when the issue of identity cards was raising questions about trust in the government with respect to their handling of personal information.

The research was based on libraries within a large UK university and aimed to answer the following questions:

- What insights concerning the user-library trust relationship could be provided through gauging the response of students towards the National Identity Card Scheme?
- To what extent are library data protection and privacy practices, and awareness, aligned with user expectations, and how might they need to change, if at all, in order to preserve the user-library trust relationship?

The right to privacy is widely regarded as a fundamental human freedom: “an absolute prerequisite” (attributed to film star Marlon Brando, 1924-2004). Trust relationships surrounding privacy are vital in academic libraries. If users were to begin worrying that loan histories were not private they might become reluctant to borrow controversial books, to supply accurate personal information, or even to use the library. Such restrictions on academic freedom could jeopardise the administration and future role of academic libraries (Bowers, 2006). Therefore, privacy and confidentiality feature prominently in professional codes (Chartered Institute of Library and Information Professionals (CILIP) 2007a; 2007b).

Definitions

According to Bowers (2006: p377), privacy means that “information about an individual is unavailable to others”. Privacy practices include steps taken to protect anonymity, and confidentiality, allowing individuals to “control what information they are willing to share or release to others”. In contrast, data protection means the statutory requirements associated with storing, maintaining and using personal information, as enshrined in the Data Protection Act 1998 (DPA).

Background to the National Identity Card Scheme

In 2006 the UK Government passed the Identity Cards Act, sanctioning the implementation of a National Identity Card Scheme (NICS). Its foundation will be a national identity card containing biometric and biographical information about the bearer, for unique identification against a National Identity Register (NIR), a large database containing unprecedented amounts of information

about individuals. Proponents claim that the scheme will tackle benefit and identity fraud, crime and terrorism as well as increasing national security (Ward, 2005: p37). Opponents claim that it will infringe upon personal privacy, also citing factors such as cost, concerns over effectiveness, and worries about "function creep" (gradual expansion of the scheme's purposes) (ibid.: p43). The debate has centred focus on privacy issues surrounding personal information and its potential purposes.

The NICS has inspired heated debate about the transformation of the individual-state privacy relationship (Mason, 2004; Hunter, 2005; Chakrabarti, 2007). In many ways, libraries display a microcosmic equivalent of this relationship, since users also give personal information in return for access to services, but whereas government initiatives are often suspiciously received (Hari, 2007), libraries have traditionally enjoyed strong trust from users not to misuse their information (Sturges et al. 2003). Coombes (2004) believes, "this goodwill is something that libraries cannot afford to lose" (p495). At a time when privacy relationships are being scrutinised nationally, it was particularly appropriate to explore privacy practices in libraries, and the lessons that libraries can learn from the identity card controversy about preservation of their own user trust relationships.

Such an exploration has additional timeliness. Post 9/11 information legislation has threatened library freedoms: under the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act (2001), the US Government has used library borrowing data in terrorist investigations; the UK's Terrorist Act 2006 came close to

forcing librarians to censor collections (CILIP, 2005a). In June 2002 the Danish parliament adopted the Anti-terror package, to which further measures were added in 2006, following the London terror attacks in July 2005. This provided the Danish Intelligence Police increased authority to access records and collect personal data from libraries and other public institutions (Nierenberg, 2007). Librarians must be aware and ready to defend user privacy, in order to remain democratic institutions (Byrne, 2004) where freedom of inquiry is unfettered. Additionally, in an age where rapidly improving technology demands ever more personal information (Davies, 1997), and young people are becoming more accustomed to social interaction online, personal information is becoming increasingly commoditised (Reed, 2007), raising questions over whether enough is being done to monitor user awareness and opinions about privacy (Johns and Lawson, 2005).

Literature review

Privacy: the surveillance society

In a recent Home Affairs Select Committee Inquiry into 'The Surveillance Society' (2007), the Information Commissioner describes how technology has increased the efficiency of our daily lives, but adds that "the risk that details of people's everyday lives may be used in unacceptable, detrimental and intrusive ways cannot be ignored" (ibid.: p2).

The Commissioner identifies a trend towards synthesis of information, in 'joined-up' Government and elsewhere; he recognises a proven value to business of knowing about customer preferences and habits. However, he is

worried by potential for surveillance: “more discrimination, social sorting, and social exclusion” (ibid.) and a “climate of fear, suspicion or lack of trust” (p3), jeopardising public “trust and confidence” in all organisations holding personal information (p7). The Commissioner criticises a lack of awareness and debate about these developments (p2.), resulting in the arrival of a “surveillance society” in incremental, apparently benign steps (pp4-5).

Attaran and vanLaar (1999) identify some of the risks of losing privacy in the digital age, including increased unsolicited email; monitored internet activity; intrusive and targeted direct marketing; risks of identity fraud; and the potential searching of an individual’s personal information by interested organisations, e.g. potential employers, investigative authorities (p241).

Good advice on how to protect privacy in the networked society, and in general, is available: for example, EPIC provides compiled lists of useful privacy protecting software (2007); Attaran and vanLaar also provide guidance and tips (1999); and Get Safe Online, the privacy portal sponsored by the Serious Organised Crime Agency, provides comprehensive advice on protecting privacy (2007a).

The NICS: public opinion

Soon after 9/11 proposals were tabled for a national identity card by the Home Office (Travis, 2001, cited in Privacy International 2004a). Government consultation found that 79% of the British public supported the proposal, with only 13% opposed (Home Department, 2003). A YouGov (2003) survey commissioned by the Daily Telegraph in September 2003 found that 78% of

the public supported identity cards (p1), in line with government results. However, a majority believed: that criminals would learn to forge the cards; the cards would contain excessive information; and confidentiality could not be ensured. Only 28% believed that information would *not* be passed on to unauthorised persons outside of Government (p2).

The London School of Economics' (LSE) Identity Project, which critiqued the Government's NICS implementation proposals, with significantly negative results (2005b), gave the following overview: "opinion polls consistently demonstrate public support for the concept of an identity card, and yet the detail of those polls indicates that people have little trust in the core elements of the proposed scheme" (2005a: p56). Reinforcing opponents' claims of declining support, the LSE suggested that support falls drastically when implications are made clear: "In Australia, initial support of 90% for an "Australia card" turned within months to opposition of 70% as details of the legislation were analysed by media commentators" (ibid.: p57).

Function creep is also a key concern (Beynon-Davies, 2006). Human rights organisation Liberty has expressed concern that future secondary legislation could alter or extend the NIR's purposes (Crossman, cited in Boggan, 2007). This would violate the DPA's second principle that personal data must be used only for purposes for which it was originally collected. The Government recently set out the benefits of relaxing data protection law in a policy review, notably without any mention of the NIR, and specifically criticising present laws where data can only be collected for a single purpose; vehement media concern followed (Independent, 2007; Morris, 2007)

A study by Joinson et al. (2006) explored attitudes towards different ID card implementation scenarios held by Open University students. It concluded that compulsion level and the identity of the organisation storing and maintaining the NIR impacted upon attitudes, with high compulsion and a centralised database receiving the least favourable response.

Privacy: libraries, democracy and foundations of trust

Bowers (2006) expresses library trust-privacy relationships as follows:

> Libraries are built on the concept of freedom, freedom for individuals to use the library and freedom for individuals to access and read any information that they desire and for those activities to be kept confidential. […] If a person does not have an expectation that their library records will be kept confidential, they may be unwilling to ask questions, perform a search, read a book on the premises, or check out a book on a controversial subject for fear of judgement by the community they live in or society at large, or for fear of retribution by the government. (p377)

According to Bowers, if libraries lose user trust, through loss of perceived expectation of privacy, users lose academic freedom. To follow Bowers' consequences through to a logical extreme, in such a situation users might falsify information, take un-issued books, or cease to use the library. This would mean chaos for library administration, and may even jeopardise its very

existence. Coombes (2004) and Byrne (2004) argue that this places an obligation upon librarians to protect and defend user privacy.

Byrne shows how maintenance of privacy and confidentiality across library services is vital to library compliance with the Universal Declaration of Human Rights (2004). Whilst Byrne writes from Australia, a glance at the European Convention of Human Rights (1950), upon which the UK's own Human Rights Act (1998) is based, shows privacy in libraries is also necessary for their compliance with Articles eight, the right to respect for private life, and ten, the right to freedom of expression. Caidi and Ross assert that "libraries have long been associated with stewardship of learning and access in societies, and as such they embody the defence of information rights on behalf of citizens, their users" (2005: p678).

Coombs (2004) and Shuler (2004) also advocate proactive roles for librarians as privacy educators, who should raise awareness in users concerning privacy rights, protections, practices, choices, and changes brought about by technological advances. Johns and Lawson (2005) here identify a gap in professional knowledge: "to better serve and protect library users, university librarians need a better understanding of undergraduate students' knowledge and perceptions about library-related privacy issues" (p488). The authors' subsequent investigation into opinions and perceptions of American students about online privacy issues, finds that students are concerned, but ill-informed in privacy matters. If libraries are, as Byrne (2004) and Caidi and Ross (2005) suggest, institutions of democracy ideally placed to act as mediators and educators in information issues, perhaps they have a duty to intervene.

Privacy: the mutually dependent relationship with trust

One of the LSE Identity Project studies, on biometrics (an important NICS component), public opinion and trust, identifies an inversely proportionate relationship between level of trust in an organisation and level of privacy demanded from it (2005a). Since libraries essentially depend on a trust relationship with their users (Coombs, 2004; Bowers, 2006; Byrne, 2004), if trust decreases, demand for privacy (hereafter 'privacy demand') will increase, which could negatively impact upon students' perceived freedom of academic inquiry. Nierenberg's study of US and Danish public librarians also discovered a strong sense of the need to preserve library users' privacy (2007). She found that the majority of the librarians she surveyed believe that it is *not* worth a possible sacrifice of privacy, access to information or freedom of expression in order to prevent terrorism (p65).

Privacy: library preparedness and user perceptions

Davies (1997) claims that "the management of data protection in university libraries is no better than satisfactory, with several examples of shortcomings either in awareness or practice" (p51). He also asserts that swift technological advances in the library "bring with them attendant anxieties about what is being done with information" (ibid.). He concludes: "mechanisms and procedures to ensure good data protection are a necessity not a luxury" (p52).

Sturges et al. (2003) support Davies' conclusions, finding a significant gap between data protection expectation from library users, and the policies and awareness of their library services, and concluding that "librarians are aware of the importance of privacy to users, however they are not well prepared to cope

with privacy issues, even at the level of data protection" (p48). Sturges et al. also explore the privileged relationship libraries enjoy with users, who "care about the safety of their personal details when using the library, but feel their data is well protected" (ibid.): they "very strongly reject the idea that libraries might pass on user data to official bodies, but even more of them reject the potential commercial exploitation of user data"; 89% expressed little or no concern about risk to privacy whilst using the library (p49). This fits with the LSE's theory (2005a) that privacy demand decreases as level of trust increases, and its findings that "participants consistently identified the profit motive of the private sector as a reason to doubt the information-sharing relationship" (p97). Sturges et al. (2003) subsequently question whether user trust is merited considering findings that privacy was not prioritised by libraries, and that there was a significant lack of awareness for dealing with practical data protection procedures; such "complacency" (p48) should be avoided if the user-library trust relationship is to be maintained.

The Online Computer Library Center's (OCLC) study on privacy and information exchange in the networked society (2007), discovered that half of the general public in six countries, including the UK, believed it was very important that libraries keep personal information and loan histories private (section 7- page 6); 64% believed libraries ought to have a privacy policy (ibid.). However, in accordance with Sturges' findings, the study reported that a majority trusted libraries (s7-p6).

Privacy: experiences in the US and elsewhere

Enacted in response to the 9/11 atrocities, the USA PATRIOT Act (2001) contains new measures for U.S. investigative authorities to request “any tangible things” from any organisation, including libraries, holding records about individuals, in their efforts to track down suspected terrorists. This reaction is reminiscent of the McCarthy “witch hunts” in the 1950s where fear led to abuse of power in order to track down details of Communist sympathisers. The measure comes with a gag order; organisations cannot talk about requests made (Drabinski 2006: p2). Byrne (2004) criticises the legislation, through which libraries are “being employed for surveillance” (p15), not the first incidence of the U.S. Government’s use of library records according to Minow (2002). She describes the Federal Bureau of Investigation’s (FBI) ‘Library Awareness Program’, which “aimed at identifying Soviet spies in research libraries in the 1970s and 1980s” (2002: p2). Circulation and usage of certain items, like technical reports, were monitored, effectively denying patrons freedom to read, a direct contradiction of the Universal Declaration Human Rights (United Nations, 1948: Article 19).

Falk (2004) describes the response, to the Act, of the American Library Association (ALA), which views privacy “as essential to the exercise of free speech, free thought, and free association” (p281). The organisation has taken a decisive lead in informing librarians about the legislation, and in protecting individuals’ privacy by advising libraries to collect only bare essential information about users, offering advocacy, drafting template privacy policies, and educating the public about the legislation (ibid. p283). The ALA has strongly supported legislation designed to protect library records from intrusive scrutiny, such as the Freedom to Read Protection Act, which, according to

Bowers (2006: p378), was “successfully thwarted” by the FBI in Congress in 2004 (also Morgan and Babington, 2004). Many libraries are informing users that their information may become subject to investigative scrutiny (Egelko and Gaura, 2003). Minow (2002) described professional guidelines including ensuring that library privacy policy is consistent with practice, increasing staff awareness of data protection procedures, and training staff to recognise associated legal documents search as search warrants (p5).

IFLA has criticised the USA PATRIOT Act because of “its potential to be used as a model for other countries” (IFLA 2003, cited in Byrne, 2004: p15).

Nierenberg (2007) in her comparative study of Danish and American public librarians’ attitudes towards anti terror legislation finds that Danish librarians have not been so public in their opposition. This, she attributes to cultural and historical factors as well as differences in the legislation itself. One of her particular suggestions to explain this lack of opposition is that librarians trust that the Danish Intelligence Police will not abuse their new extended powers – an example of trust between librarians and the authorities (p15).

Effects of the USA PATRIOT Act upon library usage are difficult to find, since the number of libraries who have been required to hand over records is classified (Doyle, 2005: p5). The Campaign For Reader Privacy (c2005) describes one situation where an FBI agent requested names and details of patrons who had borrowed a book entitled *Bin Laden: The man who declared war on America* (Bodansky, 1999), an example of what Priscilla Regan and

others call a “fishing expedition” (2004: p490). Other anecdotal evidence of this kind is numerous, causing Albitz to identify “a climate conducive to suspicion and mistrust” (2005: p85), which must necessarily impact on the right to free inquiry in the U.S (Bowers, 2006). These concerns were dismissed as “baseless hysteria” by the U.S. Department of Justice (Ashcroft 2003, cited in Coolidge 2004: p7). Indeed, Nierenberg does discover that there is a certain proportion of librarians in the US who support the PATRIOT Act, believing it a necessary measure for providing national security (2007, p91). Ten percent of the librarians she surveyed in both the US and Denmark believe the legislation is worth supporting. This suggests there is a view that privacy rights might be, in themselves, limiting in terms of issues such as national security.

Caidi and Ross (2005) warn: “library associations and their members worldwide will need to be increasingly diligent in order that the values that they have held continue to be respected in the present information environment” (p678). To avoid the UK Information Commissioner’s fears of “sleepwalking into a surveillance society” (2004, cited in Privacy International 2004b), such measures, Seifert and Relyea assert, are best “debated and implemented during a time not under duress when decisions made in the heat of the moment can lead to unintended consequences” (2004: p405).

This critical juncture is therefore a key time to assess privacy awareness and practice in libraries, learn from American experiences, and contribute to the privacy discourse.

Privacy: advocacy in the UK

UK librarians, like their US counterparts, have defended the human rights embodied by the library. The Terrorism Act 2006 originally contained a clause which essentially criminalised librarians lending material to individuals who used it for terrorist purposes. According to CILIP, at least 13 organisations joined a consortium committed to getting the legislation changed. After a lengthy process of lobbying in defence of librarians' professional duty to disseminate information freely, the consortium was successful in having the Act amended (CILIP, 2005a).

At the CILIP Umbrella Conference, John Pateman (criticised by some for using the forum to air his own political opinions (Bruce, 2007)) claimed that the War on Terror "is allowing the Government to erode the civil liberties and democratic values which underpin our library services" (2007: p1). He called upon librarians to defend the information rights of patrons and warned against complacency, citing examples of the Government's historical use of UK library records to identify poll-tax defaulters (p9), and recent government requests to universities for assistance in weeding out extremists at their institutions, which "would include the reporting to police of students' research activities, internet use and reading habits" (p8).

Conclusions from the literature

Privacy in the library is important to engendering user trust, a relationship which supports academic freedom, the foundation of the academic library (Byrne, 2004; Bowers, 2006). In light of the change of direction in information policy at home (CILIP, 2005a) and abroad (Minow, 2002), vigilance is required

in academic libraries to ensure that previously revered library freedoms are not lost in the quest for national security (Caidi and Ross, 2005). Libraries are institutions of democracy that embody human rights (Byrne, 2004) and should lead defence of user privacy (Coombes, 2004; Falk, 2004; Shuler, 2004; Bowers, 2006), about which users may not be well-educated (Johns and Lawson, 2005). User-library trust is strong, but not necessarily deserved (Sturges et al., 2003). If libraries appear to neglect user concerns they risk losing their privileged level of trust (Poynder, 2002) and of jeopardising academic freedom (Coombes, 2004; Bowers, 2006). The NICS controversy highlights the importance of trust to information gathering initiatives (LSE, 2005a), and the relationship between trust and privacy demand. For all these reasons the user-library trust relationship must be prioritised; libraries need to understand user privacy perspectives (Johns and Lawson, 2005) and provide clarity in their practices (Poynder, 2002). This research learns more about the current balance of user-library trust within one UK large academic library and the relative risk of government schemes such as NICS negatively impacting upon this through the creation of an increasing suspicion about “surveillance”. As a result the researcher is able to offer recommendations to help to mitigate that risk.

Research Design

To discern student perspectives on both NICS and library practices, an online survey was undertaken on the University students in question, using SurveyMonkey, and running for 8 weeks during the summer of 2007.

The second aspect, relating to library practices, required input from librarians. Therefore, qualitative interviews with six librarians were undertaken. Face-to-face interviews were chosen in order to provide authoritative responses against which to compare user perceptions.

Online survey

The online survey aimed to:

- Gauge student response towards the NICS and their trust in the Government;
- Gauge student trust in library privacy practices;
- Ascertain student perceptions of the types and purposes of personal information kept by libraries.

It consisted of:

- University-related demographic questions (age, course and year of study)
- Westin privacy segmentation questions (from Joinson et al., 2006), although altered slightly to remove Westin's commercial emphasis
- A measurement of NICS attitudes through use of a Likert scale question borrowed from MORI. Preset skip logic directed supporters to give reasons for support and those opposed their reasons for opposition. Reasons were offered in checklists. Lists were set to scramble randomly for each respondent, negating the primary-recency effect (Frey and Oishi, 1995).

- A measurement of trust in Government through one question using a Likert scale and another, to measure consistency, a statement of choice.
- Perceived types and purposes of library personal information (multiple response checklist options: some banal, some more intrusive). These randomised lists helped remind respondents of potential types and uses whilst a free text 'Other' option ensured capture of volunteered information.
- A measurement of trust and confidence in libraries.

Joinson's methodology (2006) was of particular use to this research. To identify pre-existing privacy attitudes, his survey used formulaic questions developed by Alan Westin and Harris Interactive (Taylor, 2003). Respondents' answers to these questions put them in one of three categories: privacy unconcerned ("no real concerns about privacy"), privacy pragmatists ("strongly concerned about privacy issues and active in protecting themselves from the abuse or misuse of their personal information", but "often willing" to exchange information for "tangible benefits"), or privacy fundamentalists ("feel they have lost a great deal of privacy and are strongly resistant to any further erosion of it"). Whilst Westin's work has been criticised for ostracising the highly privacy-concerned as extremists and for his sponsorship agreements with businesses with a vested interest in personal information (Electronic Privacy Information Centre (EPIC), s.d.), Joinson et al. find that the segmentations provide "useful insights into people's responses to different privacy threats" (p342).The Harris Poll of 2003 found that two thirds of people fall into the middle category, 'privacy pragmatists' (Taylor, 2003). This approach was adopted, but as will

be seen, was adapted to make the results of the current study more meaningful.

SurveyMonkey hosted the survey and summarised the data, which was also downloadable as an Excel spreadsheet. A codebook was produced, as advised by Litwin (1995), from which tables of raw data were compiled and graphs produced. Responses were broken down by library, subject grouping and Westin privacy segmentations; where possible, responses were aggregated into generalised opinions.

Since NICS support varies slightly with age (Home Office, 2005), a limited age group was targeted. Undergraduates form a more consistent age group than postgraduates, and are more numerous, therefore being an undergraduate was made a stipulation for survey completion. Convenient and efficient online distribution and collection allowed a large response over a short period and comparison with previous quantitative research. Librarians at seven of the university's libraries liaised with relevant students and staff in order to organise distribution of the survey to undergraduate mailing lists. This provided access to body of 2,750 students, approximately one quarter of the university's undergraduate population. In order not to limit responses, a sampling strategy was not applied. Respondents were self-selecting since completion of the survey was voluntary.

Interviews

The interviews aimed to: ascertain the various libraries' usage of personal information, for comparison with student perceptions; explore the libraries' treatment of, awareness of, and attitude towards data protection issues and practices; present survey findings for response.

Questions were grouped by topic (Frey and Oishi, 1995) beginning with factual questions about data protection policy, followed by types and purposes of personal information. Interviewees were then presented with three fictional data protection scenarios, which helped gauge awareness of good practice. Subsequent questions also checked for awareness and gave interviewees a chance to self-evaluate their practices. Opinion was sought on librarians as privacy educators (Coombes, 2004; Shuler, 2004) and comments invited on the survey findings for each interviewee's particular library. Many questions were suggested by Sturges et al. (2003) who investigated: "level of awareness of privacy issues"; "data protection preparedness"; "the importance of privacy to the relevant stakeholders"; "the extent of data processing in libraries"; and the "state of policies devoted to ensuring privacy to users" (p46).

All seven Librarians agreed to participate, although one later cancelled due to unforeseen circumstances. A pre-interview information sheet was distributed, briefly outlining topics for discussion. Prior to interview, each librarian received the students' survey results summary.

The technique of asking several different questions on a topic was employed, to increase data richness and reliability. The interview script was standardised

for consistency, but respondents were encouraged to expand or clarify responses considered particularly pertinent.

Survey findings and discussion

The response

A 20.5% response rate was achieved (566 responses) for the survey. Some results were excluded from analysis for various reasons which left 539 results for the analysis, five per cent of the University's total undergraduate body.

First-year students were over-represented within the sample. More first years are housed in University accommodation than any other year group and are therefore more likely to have free University library internet access, increasing ease of access to the online survey.

Westin privacy segmentations

According to the Westin methodology (described in Joinson et al., 2006) respondents giving privacy-oriented responses to all three Westin questions were classed as 'privacy fundamentalists', all non-privacy-oriented responses, 'privacy unconcerned', and a mixture, 'privacy pragmatists' (see Figure 1). The proportion of fundamentalists, in this study (18.4%), was lower than Joinson's, 32.5% (2006), and Harris Interactive's, 26% (Taylor, 2003); the proportion of unconcerned, 14.7%, was slightly higher than Joinson's sample (11.6%) and Harris Interactive's (10%). The "de-commercialised" question wording may explain this increased relaxedness, since students particularly distrust

commercial motives (Sturges et al., 2003; LSE, 2005a). Or, perhaps, privacy-concerned individuals were reluctant to participate in the survey because of those very privacy concerns.

On further examination, the privacy pragmatist category appeared inadequate and overly broad: those giving strongly privacy-oriented responses to two of three questions and one somewhat non-privacy-oriented response were classed as pragmatists alongside those answering the exact opposite. This seemed slightly misleading. Therefore the researcher divided up this category into two sub-categories: pragmatist concerned (PC) and pragmatist unconcerned (PU) (Figure 2). The former was assigned where a respondent gave two privacy-oriented responses; the latter for two non-privacy-oriented responses. This was fairer, more valid, and more useful to any future study measuring shift in opinion over time or in response to external factors, since the new categories register change more sensitively. The new segmentations also allow helpful generalisation into 'privacy-concerned' categories (fundamentalists, PCs) and 'privacy-relaxed' categories (unconcerned, PUs). Therefore, these new segmentations were used for all subsequent Westin analyses of the results.

Respondents were slightly more privacy-relaxed than concerned. This may be because the current university generation is more adept at interacting with society online than the general public (OCLC, 2007), e.g. social networking sites such as Facebook, online purchasing, etc. This necessarily involves exchanging information and a certain waiving of the right to privacy, in order to access those services, but does not necessarily equate to corresponding

awareness of the consequences. Get Safe Online acknowledges of young people, “being an expert in technology doesn’t mean they have the life-experience and wisdom to handle all the situations they may run into” (2007b, p1). Indeed, if students are ill-informed in privacy matters, as Johns and Lawson discovered (2005), this would go some way to explain Joinson et al.’s relatively high level of fundamentalists; the mean age of that study was 42.3 years (2006: p336), not an age group generally considered part of the “net generation” (Mi and Nesta, 2006). Whilst not demonstrating the “attendant anxieties about what is being done with information” that Davies expected to accompany technological change (1997: p51), the respondents showed greater privacy concern than Sturges et al. who found “low general levels of anxiety about threats to privacy (28%)” (2003: p47). This finding suggests the importance of discovering students’ awareness of privacy matters, since potentially dangerous ignorance of the risks of losing privacy online, could also produce privacy-relaxedness.

Medical Scientists and Mathematical and Physical Scientists were significantly less privacy-concerned than other subject groups, respectively, whereas Humanities students tended towards privacy concern (Figure 3). This suggests that academic communities may influence individual opinions beyond the boundaries of academic study; or, perhaps certain subject areas attract students with certain proclivities.

Attitudes towards the NICS

A majority of respondents were opposed to the NICS (53.6%, 25% of those strongly), with only 28.8% in favour (Figure 4). This is possibly due to selection bias, or heightened awareness of the scheme's practical implications (LSE, 2005a). Attitude was linked to pre-existing privacy opinion, with privacy-concerned respondents significantly more inclined towards opposition. Questions about potential impact of the NICS upon library practices showed an inclination for respondents (particularly the privacy-concerned) to believe that information purposes might become more intrusive.

The results are in line with recent public opinion polls from No2ID (2006), and negate the level of support (73%) claimed by the Government (Home Department, 2003). Support was startlingly lower than found in the MORI poll (80%) from which the question was taken. It is possible that those particularly opposed to the NICS may have seen the survey as a protest opportunity; equally, the negative response could display heightened awareness of the scheme's practical implications (LSE, 2005a).

Trust in the Government

Trust in the Government as instigator of the NICS was higher than expected (it did not correspond closely with NICS support level), but still low overall. 42.3% of the responding students agreed with the statement of trust in Government, though only 7.4% agreed strongly; 35.8% disagreed, 10% strongly (Figure 5). The findings exemplified the mutually-dependent relationship described by the LSE (2005a): low trust was accompanied by high privacy demand and NICS opposition. The finding does not prove cause and effect, but the association is

apparent and should confirm for libraries that to lose user trust would be to their detriment; students could become similarly opposed to library usage of personal information and take steps to avoid its collection. It could certainly result in students' feeling that their personal information was unsafe, subsequently limiting academic freedom (Bowers, 2006). Therefore, user trust must be valued, respected and prioritised by academic libraries.

Perceptions of types and purposes of personal information at the library

All libraries had access to basic contact information, details of loans, reservations and overdues through their library management systems. No libraries stored information on political opinions, religious beliefs or information inferred from loan histories. Reactions to the latter were vehement and several librarians interviewed found their very suggestion ridiculous, although one acknowledged their theoretical possibility.

Three interviewees did not know whether the library system stored complete loan histories (i.e. for the duration of a student's University career), another thought that upon return of the item all record of the transaction was erased, and two thought that a complete history *was* stored. The lack of comprehensive awareness of types of information collected by the system is of concern. Interviewees were also uncertain about whether they stored notes on students' areas of academic interest.

All interviewees used students' details for purposes associated with loan administration; none for monitoring students' interests or opinions. Where

details of loans were used to improve library stock, interviewees were unanimously more interested in noting item statistics, rather than details of any specific users' borrowing habits. Libraries that had swipe card access did not monitor door logs, although some were uncertain about log storage. One library had CCTV which enabled investigation of deliberate taking of un-issued books. No libraries disclosed personal information to help other users obtain books.

Generally, the student responses to the questionnaire gauged correctly the types and purposes of their personal information. However, there were some surprising discrepancies. The comparatively low number who believed libraries maintained contact details seemed odd in light of libraries' well-recognised need to chase overdue books. Numbers of students perceiving use of more intrusive information for more dystopian purposes were relatively small, but still substantial: 36 respondents (6.7%) thought libraries informed investigative authorities of questionable content in reading material, a breach of confidentiality and an act of censorship reprehensible to most information professionals (Shenker, 2005). This result is worthy of swift redress by the libraries.

When students were asked what they thought of the purposes of this information both before and after NICS implementation, responses stayed much the same, apart from the lowest-rated, and most intrusive suggested purposes (purposes 4, 6 and 7), as shown on Figure 6. The majority of those expecting a change in each case (11.1%, 8.7%, and 11.3%, respectively) were in the two privacy-concerned Westin categories.

Perceptions of whether the library passes on personal information

Respondents rejected the idea that their libraries pass on information about them to outside agencies, (82.9%, 27.2% of those strongly). Only 2.8% believed libraries did pass on information (Figure 7). This supports Sturges et al.'s findings that students "feel their data is well protected" by libraries (2003: p48), and very strongly reject that "libraries might sell or pass on personal information" (ibid.).

When asked whether information might be passed on post-NICS, the negative response was still strong at 66% (with 19.1% answering 'definitely not'), but the affirmative response increased to 10.7% (though 10.2% answered 'probably' rather than 'definitely'). This shift was significant although the effect of asking the question at all, which would have implied a change, must be considered. However, the shift still indicates a lack of certainty about potential NICS impact.

Confidence in proper and professional library practice and compliance with the DPA

Respondent confidence was strong, suggesting that user-library trust is healthy. Respondents were confident that libraries dealt with personal information in proper and professional ways (81.3%); only 3.5% were not confident (Figure 8). Trust in libraries was significantly higher than trust in Government for both the privacy-concerned and the privacy-relaxed. Again, the findings support the LSE theory (2005a) of interplay between trust and

privacy concern; they also support OCLC's (2007) and Sturges et al.'s (2003) findings that libraries are trusted by users.

However, a comparatively large group were 'not sure' about their libraries' practices. This uncertainty was also exhibited in the slightly less confident response to libraries' compliance with the DPA, possibly due to lack of knowledge about the Act's afforded protections.

Usage of the University Card

Students' University cards provide physical access through security doors, verify identity against University databases, and provide entitlement to services. Interviewees reported widespread card usage for access to library borrowing services. Four of the six libraries also operated a swipe-card access system.

Ascertaining the breadth and range of the card's usage reveals that if the University card were ever combined with, or superseded by, the national identity card, and access points such as security doors and library issue desks verified identity using the NIR, the NIR would theoretically have access to detailed information about students' activities, courses of study and topics of personal interest.

Library and University policy

There were no individual *library* data protection policies. Five of the six interviewees displayed confidence in existence of broader organisational

policy, but only three could be supported by actually available documents, and, conversely, one failed to mention that a policy existed.

Lack of policy did not appear to be compensated for elsewhere. Interviewees gave the overall impression that in some libraries, data protection was not relevant to everyday practice. Sturges et al. (2003) found similarly low prioritisation. This impression, combined with interviewees' limited DPA knowledge, and lack of policy, could put interviewees at risk of "unwittingly breaching" its principles (Poynder, 2002), perhaps, for example, by keeping redundant information, something easy to overlook, and against which Coombes (2004) and Bowers (2006) warn vigilance. Good privacy practices and trust are essential to unfettered intellectual inquiry (Bowers, 2006: Byrne, 2004); therefore general complacency and lack of data protection prioritisation are incongruous with any university committed to preserving academic freedom.

Overall alignment of library practices with user perceptions

All interviewees felt their privacy practices and awareness were aligned with user perceptions, with only one asserting that particular discrepancies left them slightly uncertain. One commented that libraries must necessarily ensure alignment, since "if they're not they can get into a lot of trouble", a reference to legal obligations. One suggested, when asked, that student perceptions needed to change rather than library practices. Another referred back to the survey respondents who were 'unsure' about proper library practice, and was

critical of their lack of opinion, given their status as intelligent students; she recommended that students should "need to start doing some asking as well".

Two interviewees were asked what contributes to successful alignment. One mentioned attributes of "clear policy", "trust", and "good relations" between students and other members of the University. The other suggested the "open ethos", and that excellent student representation on committees meant that students had "no right to be ignorant of what's going on". Whether interviewees actually practice this philosophy is unclear, but the descriptions emphasise trust, clarity, openness and responsibility, negating Poynder's belief that transparency is "something few librarians […] appreciate" (2002), and all of which actively contribute to successful negotiation of Coombes' "privacy tightrope" (2004, p493).

General opinions about young people

Whilst specific questions about the respondents' generation were not asked, the topic was raised voluntarily by three interviewees. One said they would expect young people to be concerned about privacy, whilst two others said that young people were "laid-back" and "no more concerned about privacy than they are about pensions". It is interesting to see such dichotomous opinions. If the former attitude prevails in wider society a potentially dangerous assumption exists that young people are able to protect their privacy in an informed way. If the latter prevails then, arguably, the older generation is guilty of neglect through lack of privacy training provision, or of awareness in privacy matters itself. Perhaps this 'don't care' attitude towards privacy is more likely to be

'don't know', i.e. ignorance. This is exemplified by Oxford University's forays into Facebook photo-sifting for finding and fining rule-breakers (Foster, 2007), which proved that some students were unaware that their personal photos were not protected from prying eyes.

Is student trust merited by libraries?

Whilst interviewees were keen to defer to other authorities, the responses showed general good practice, and a commendable desire to protect user information, although, in practice, interviewees might find it difficult to refuse a genuine warrant: the Act allows a fine of up to £5,000 for such obstruction (1998). Responses were an improvement on Sturges et al.'s findings (2003) that 40% of librarians were unacquainted with necessary procedures for dealing with user information requests (p97).

In many ways students were right to be confident in library practices: the interviewees all understood and respected data protection. Whilst tending to refer data protection matters to other authorities within the institution, interviewees all dealt commendably with three presented scenarios, in ways that would primarily protect user information. The scenarios related to the police asking librarians for information on who might have borrowed sensitive material, for example. However, this is not to say there is no room for improvement. The researcher has identified two types of data protection practices in the course of this study: 'defensive' data protection, or reaction to threats of intrusion from outside sources, which, arguably, can be managed with common sense and basic knowledge of data protection principles; and

‘proactive’ data protection, which involves a daily prioritisation of privacy principles, and demonstration of clarity and accountability, something the libraries demonstrated less convincingly. The former may be legally adequate, but if librarians wish to be information leaders (Davies, 1997; Coombes, 2004; Shuler, 2004), it would be useful to achieve the latter.

Conclusions

What insights concerning the user-library trust relationship can be provided through gauging the response of students towards the NICS?

Libraries should oppose any linkage between the NICS and library activity, acknowledging the strength of opposition exhibited by students and the possibility of being tainted by association. If identity cards became a standard means of identification, distancing themselves from the scheme would be perceived as showing solidarity with users. This is relevant for any library where user NICS opposition is strong, and is essential in maintaining the academic library's democratic status (Byrne, 2004) and preserving user-library trust. In addition, proactive defence of users' information and privacy interests (Caidi and Ross, 2005), perhaps through vocalising opposition to the scheme in the professional literature, would show libraries' commitment to preserving confidentiality of service, as required in the CILIP professional codes (2007a; 2007b).

Widespread use of the University card for accessing services makes the possibility of NICS linkage real, if hypothetical. Students may alter library behaviour based on expectations of future links, or as part of a general decline in trust, for all personal information holding organisations, which accompanies the "surveillance society" (ICO, 2007: p7). Libraries could gain a trust advantage prior to NICS implementation by reviewing data protection and privacy practices and proving student trust justified.

To what extent are library data protection policy and privacy practices and awareness aligned with user expectations and how might they need to change?

Whilst acknowledging the competing demands of library management (Davies, 1997) certain time-efficient steps could return long-term benefits, and redress discovered weaknesses in the user-library trust relationship. Since all academic libraries are founded on academic freedom (Byrne, 2004; Coombes, 2004; Bowers, 2006) the recommendations also have some relevance to other universities and therefore the following approaches are suggested. Further work with librarians in other organisations/sectors would help to test these ideas further, bearing in mind the limited nature of the current study.

Librarians should familiarise themselves with the DPA, self-assess practices for gaps and inconsistencies. Most interviewees suggested that whilst they lacked detailed legislative knowledge, they knew enough to run a DPA-compliant library service. Librarians suggested they felt their libraries required no more detailed knowledge. However, this is worrying since regardless of their size, content or location, "there is no excuse for librarians to get it wrong because their whole training and ethos is about managing information properly"(Davies, cited in Poynder, 2002).

A truly healthy trust relationship should arguably be founded on informed awareness, not ignorance, or complacency, which may run much deeper than the survey suggested. If privacy-relaxedness is at least partly due to ignorance

of privacy issues and if this ignorance were gradually lessened, privacy concern would increase, and trust decrease (LSE, 2005a). However, if libraries can proactively prove student trust merited, and address privacy concerns openly, they may escape the general lowering of trust (ICO, 2007), which could otherwise result in student recalcitrance over library usage, symptomatic of restricted academic freedom (Bowers, 2006). Additionally this would win for libraries user trust more firmly founded in awareness.

Librarians should raise the policy's profile within the organisation, perhaps by encouraging incorporation into a relevant website and by advocating familiarisation with it. Librarians could benefit from becoming data protection champions; the informational nature of the DPA links directly to libraries' core function as information providers. To champion student rights as data subjects could create favourable trust associations in the student psyche, and would raise the profile of data protection within libraries themselves.

Proactive student education about library data protection practices might include development, distribution, and display of a library 'privacy statement', as advocated by Johns and Lawson (2005). The statement's purpose would be threefold: to present how information is and is not used, thereby fully re-aligning practice and perceptions; to provide accountability, and impetus for Librarians to adopt a more professionally-thorough attitude to privacy protection; and to reassure students of the library's utmost respect for personal information.

Encouraging privacy awareness in students would engender a trust relationship based on informed understanding, rather than ignorance or apathy. Librarians could advocate attendance at privacy training courses (e.g. risks of losing privacy online, how to avoid them, privacy rights and protections afforded by legislation, etc.). Promotion of such courses would encourage students to take responsibility for their privacy awareness, as would compilation of a resource list on privacy topics. These measures could strike an ideal balance by making librarians privacy advisors (the educational role advocated by Coombes (2004) and Shuler (2004)), whilst not diverting excessive time away from core library administration.

Finally Librarians should stay aware of professional data protection developments (Davies, 1997), and be vigilant about possible changes to legislation (Caidi and Ross, 2005), being aware that "data protection is an essential barrier to excessive surveillance" (Information Commissioner, cited in Privacy and Data Protection, 2007). They should lend their voices to campaigns which threaten user privacy (Coombes, 2004). Such measures would prove library users' privacy valued, protected and defended. It is perhaps unsurprising to find that public librarians in the US and Denmark are much more sceptical about anti-terror legislation and its effectiveness than the general population, thanks to the core values of the profession, namely access to information, freedom of expression, intellectual freedom, protecting the privacy of users (Nierenberg, 2007).

The current campaign to weed out extremists at universities places the issues raised at the heart of debates about academic freedom (Hood, 2007); new

legislation has already threatened previously revered library freedoms (CILIP 2005a). Libraries cannot afford to be complacent about user trust (Coombes, 2004). The best way to protect that trust is to proactively ensure, and assure, that data protection awareness and practices reach the highest standards. The recommendations outlined above should begin such a process when combined with long-term plans to raise the priority of data protection for both students and library staff.

Final observations

The students trust their libraries with considerable confidence, which, to an extent, is merited. However there is a certain complacency in libraries' attitudes towards data protection which cannot be afforded when the development of the surveillance society, the implementation of the NICS and the potential for relaxation of data protection law threaten to create a climate of suspicion against personal information-holding organisations, including libraries. If user trust in privacy were to fail, academic freedom in the library would be jeopardised (Bowers, 2006). Therefore, libraries must prioritise data protection issues. They can do this by: assessing their own practices (Coombes, 2004); improving their awareness of system information storage and capabilities (ibid.); improving policy and staff awareness of the DPA (Poynder, 2002); advocating the privacy rights of users (Caidi and Ross, 2005); improving awareness of library practices, and privacy, in users (Coombes, 2004; Shuler, 2004); and producing privacy statements to provide transparency (Poynder, 2002) and clarity (Coombes, 2004). Libraries should also avoid association with the NICS, to which a majority of the students appear to be opposed.

These steps will pre-emptively prove to students that their trust is merited, thereby strengthening the user-library trust relationship, and preserving academic freedom.

Westin privacy segmentations

The Westin method (Taylor, 2003; Joinson et al., 2006) for measuring pre-existing privacy concerns proved extremely useful in analysing survey responses, since it produced such consistent result patterns, suggesting "predictive validity" (Litwin, 1995: p40). Whilst Westin's original 'pragmatist' category inadequately measured the large mid-section of respondents, the simple half-way division increased the scale of accuracy and validity. Additionally, having four segments allowed useful division of responses into privacy-concerned and privacy-relaxed categories. Rephrasing the Westin questions to remove emphasis on commercial privacy made them more widely applicable. The method could now be useful to academic libraries for measuring privacy concern. If concern increases then libraries would be aware of the need to do more to inspire trust. Whilst further experimentation would be required reliably to prove the new segmentations' effectiveness, and to establish a baseline response for the rephrased questions, the amended Westin methodology provided a wealth of insights and is recommended for future research.

References

Albitz, B. (2005) 'Dude, where are my civil rights?', *The Journal of Academic Librarianship* 31(3) 284-286.

Attaran, M. and VanLaar, I. (1999) 'Privacy and security on the internet: how to secure your personal information and company data', *Information Management and Computer Security*, 7(5): 241-247.

Beynon-Davies, P. (2006) 'Personal identity management in the information polity: the case of the UK national identity card', *Information Polity: an International Journal of Government and Democracy in the Information Age*, 11(1): 3-19.

Bodansky, Y. (1999) *Bin Laden: the man who declared war on America*. Rocklin, Calif.; [Great Britain]: Forum.

Boggan, S. (2007) 'No more secrets', *The Guardian*, 27th February.

Bowers, S. L. (2006) 'Privacy and library records', *The Journal of Academic Librarianship*, 32(4): 377-383.

Bruce, D. (2007) *Libraries and the War on Terror: censorship and diversity - John Pateman* (David Bruce). [online] Available at: http://clippers2007.pbwiki.com/Libraries+and+the+War+on+Terror:+censorship

+and+diversity+-+John+Pateman+(David+Bruce) [Accessed 2 December 2008]

Byrne, A. (2004) 'Libraries and democracy – management implications', *Library Management*, 25(1/2): 11-16.

Caidi, N., and Ross, A. (2005) 'Information rights and national security', *Government Information Quarterly*, 22: 663-684.

Campaign For Reader Privacy (2005) 'What we know about library and bookstore searches since 9/11' [online]. Available at http://www.readerprivacy.org/info.jsp?id=4 [Accessed 9 December 2008]

Chakrabarti, S. (2007) 'Yet another step along a dangerous road', *The Independent*, 15th January.

Chartered Institute of Library and Information Professionals (2005a) *The Terrorism Act 2006* [online]. Available at http://www.cilip.org.uk/policyadvocacy/informationsociety/intellectualfreedomprivacy/terrorismbill [Accessed 2 December 2008]

Chartered Institute of Library and Information Professionals (2007a) *Code of professional practice* [online]. Available at http://www.cilip.org.uk/policyadvocacy/ethics/code.htm [Accessed 2 December 2008]

Chartered Institute of Library and Information Professionals (2007b) *Ethical principles* [online]. Available at: http://www.cilip.org.uk/policyadvocacy/ethics/principles.htm [Accessed 2 December 2008]

Coolidge, K. (2004) '"Baseless hysteria": the controversy between the Department of Justice and the American Library Association over the USA PATRIOT Act', *Law Library Journal*, 97(1): 7-29.

Coombs, K.A. (2004) 'Walking a tightrope: academic libraries and privacy', *The Journal of Academic Librarianship*, 30(6): 493-498.

The Data Protection Act 1998 (c.29).

Davies, J. (1997) 'Managing information about people: data protection issues for academic library managers', *Library Management*, 18(1): 42-52.

Doyle, C. (2005) *Libraries and the USA PATRIOT Act*. (Congressional Research Service Report). [online] http://www.fas.org/sgp/crs/intel/RS21441.pdf [Accessed 30 March 2010]

Drabinski, E. (2006) 'Librarians and the Patriot Act', *Radical Teacher*, December, 22.

Egelko, B., And Gaura, M.A. (2003) 'Libraries post Patriot Act warnings', *San Francisco Chronicle*, 10th March.

Electronic Privacy Information Center, [s.d.]. *Public opinion on privacy* [online] Available at: http://www.epic.org/privacy/survey/ [Accessed 2 December 2008]

European Convention of Human Rights 1950 [online]. Available at: http://conventions.coe.int/treaty/en/Treaties/Html/005.htm [Accessed 30 March 2010]

Falk, H. (2004) 'Privacy in libraries', *The Electronic Library*, 22(3): 281-284.

Foster, P. (2007) 'Caught on camera and found on Facebook', *The Times*, 17th July.

Frey, J.H. and OISHI, S. (1995) 'How to conduct interviews by telephone and in person', *The Survey Kit, Vol.4*. London, New Delhi: Sage Publications.

Get Safe Online (2007a) 'Protect your privacy' [online]. Available at: http://www.getsafeonline.org/nqcontent.cfm?a_id=1132 [Accessed 9 December 2008]

Get Safe Online (2007b) 'Resources for parents, teachers and young people' [online]. Available at: http://www.getsafeonline.org/nqcontent.cfm?a_id=1182 [Accessed 9 December 2008].

Hari, J. (2007) 'When the government acts, why do we always assume there is something to fear?', *The Independent*, 15th January.

Home Department (2003) *Identity cards: a summary of findings from the consultation exercise on entitlement cards and identity fraud,* (Cm 6019). London: The Stationery Office.

Home Office (2005) *Identity cards: an assessment of awareness and demand for the Identity Cards Scheme.* London: The Stationery Office.

Hood, J. (2007) 'Oration by the Vice-Chancellor', *Oxford University Gazette*, Supplement (3) to No.4818: 93-101.

The Human Rights Act 1998 (c.42).

Hunter, P. (2005) 'London terrorist attacks heat up identity card debate and highlight uncertainties over their efficacy', *Computer, Fraud and Security* 2005(7): 4-5.

The Identity Cards Act 2006 (c.15).

The Independent (2007) 'Personal privacy and the power of the state', *The Independent*, 15th January.

The Information Commissioner's Office (2007) *Home Affairs Select Committee Inquiry into 'The Surveillance Society?': evidence submitted by the Information Commissioner* [online]. Available at http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_g

uides/home_affairs_committee_inquiry_into_surveillance_society.pdf

[Accessed 2 December 2008]

Johns, S. and Lawson, K. (2005) 'University undergraduate students and library-related privacy issues', *Library and Information Science Research,* 27: 485-495.

Joinson, A.N., Paine, C., Buchanan, T. and Reips, U. (2006) 'Watching me, watching you: privacy attitudes to identify card implementation scenarios in the United Kingdom'. *Journal of Information Science*, 32(4): 334-343.

Litwin, M.S. (1995) 'How to measure survey reliability and validity', *The Survey Kit vol.7* London, New Delhi: Sage Publications.

The London School of Economics (2005a) *The Identity Project: an assessment of the UK Identity Cards Bill & its implications: interim report*. London: LSE.

The London School of Economics (2005b) *The Identity Project report: executive summary*. London: LSE.

Mason, S. (2004) 'Is there a need for identity cards?' *Computer, Fraud and Security,* 2004(8): 9-15.

Mi, J., And Nesta, F. (2006) 'Marketing library services to the Net Generation', *Library Management,* 26(6/7): 411-422.

Minow, M. (2002) 'The USA PATRIOT Act', *Library Journal* [online]. Available at http://www.libraryjournal.com/index.asp?layout=articlePrint&articleid=CA245044 [Accessed 2 December 2008]

Morgan, D. and Babington, C. (2004) 'House GOP defends Patriot Act powers', *The Washington Post*, 9th July.

Morris, N. (2007) 'Big brother: what it really means in Britain today', *The Independent*, 15th January.

Nierenberg, E. (2007) Anti-*terrror legislation and public libraries: a comparison of librarians' concerns in the USA and Denmark*, Oslo University College [online. Available at http://www.hio.no/content/download/79265/562882/version/1/file/Nierenberg,+Ellen.pdf [Accessed 29 April 2009]

NO2ID (2006) *Opinion polls* [online]. Available at http://www.no2id.net/IDSchemes/opinionPolls.php [Accessed 2 December 2008]

Online Computer Library Center (2007) *Sharing, privacy and trust in our networked world* [online]. Available at http://www.oclc.org/reports/sharing/default.htm [Accessed 26 April 2009]

Pateman, J. (2007) 'Libraries and the War on Terror: the power of nightmares', CILIP Umbrella 2007, De Havilland Campus, University of Hertfordshire, 28-30 June.

Poynder, R. (2002) Key moves for information professionals. *Information World Review* [online], 2nd December. Available at http://www.computing.co.uk/information-world-review/features/2083997/key-moves-information-professionals [Accessed 2 December 2008]

Privacy and Data Protection (2007) *News* [online]. Available at http://privacydataprotection.co.uk/news/ [Accessed 2 December 2008]

Privacy International (2004a) *Mistaken identity: exploring the relationship between National Identity Cards & the prevention of terrorism [Interim report]*. London: Privacy International.

Privacy International (2004b) *Information Commissioner warns of ID cards and surveillance society* [online]. Available at: http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-66664 [Accessed 30 March 2010]

Reed, D. (2007) 'Question of trust', *Precision Marketing,* 19(16): 25-28.

Regan, P. M. (2004) 'Old issues, new context: privacy, information and homeland security', *Government Information Quarterly*, 21: 481-497.

Seifert, J.W. And Relyea, H.C. (2004) 'Do you know where your information is in the homeland security era?', *Government Information Quarterly,* 21: 399-405

Shenker, J. (2005) 'Oxford libraries join fight against 'government censorship''. *The Oxford Student* [online], 17th November. Available at: http://www.oxfordstudent.com/mt2005wk6/News/oxford_libraries_join_fight_against_%E2%80%98government_censorship%E2%80%99 [Accessed 2 December 2008]

Shuler, J. (2004) 'Privacy and academic libraries: widening the frame of discussion', *The Journal of Academic Librarianship*, 30(2): 157-159.

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

Taylor, H. (2003) 'Most people are "privacy pragmatists" who, while concerned about privacy, will sometimes trade it off for other benefits', *The Harris Poll*, March [online]. Available at http://www.harrisinteractive.com/harris_poll/printerfriend/index.asp?PID=365 [Accessed 9 December 2008]

The Terrorism Act, 2006 (c.11)

United Nations (1948) *Universal Declaration of Human Rights* [online]. Available at http://www.udhr.org/UDHR/default.htm [Accessed 9 December 2008]

USA Patriot Act, 2001

Ward, P. (2005) *The Identity Cards Bill*. London: House of Commons Library (Research Paper 05/43)

YouGov, on behalf of the Daily Telegraph (2003) *Survey results: identity cards* [online]. Available at http://www.yougov.com/archives/pdf/TEL020101033.pdf [Accessed 26 April 20909]

Illustrations

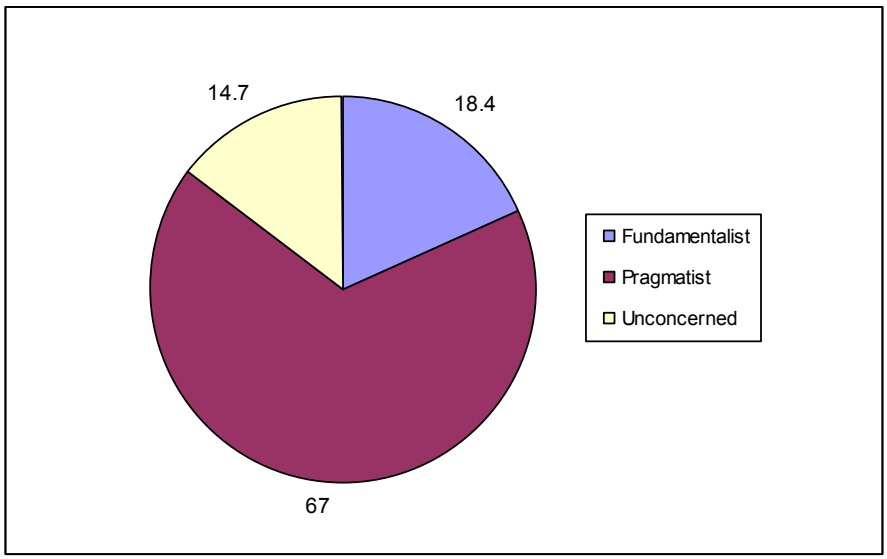

Figure 1. Westin privacy segmentations of survey respondents (as percentage of total response)

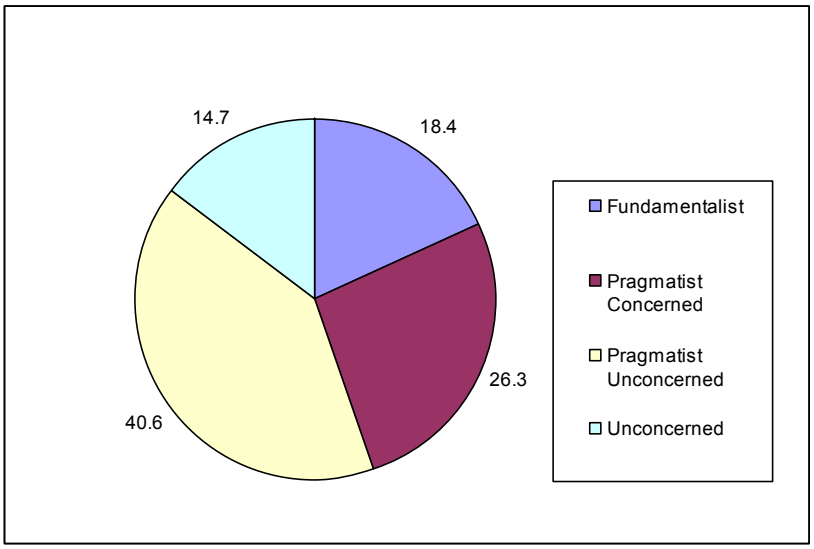

Figure 2. Westin privacy segmentations of survey respondents, showing new sub-categorisation (as percentage of total response)

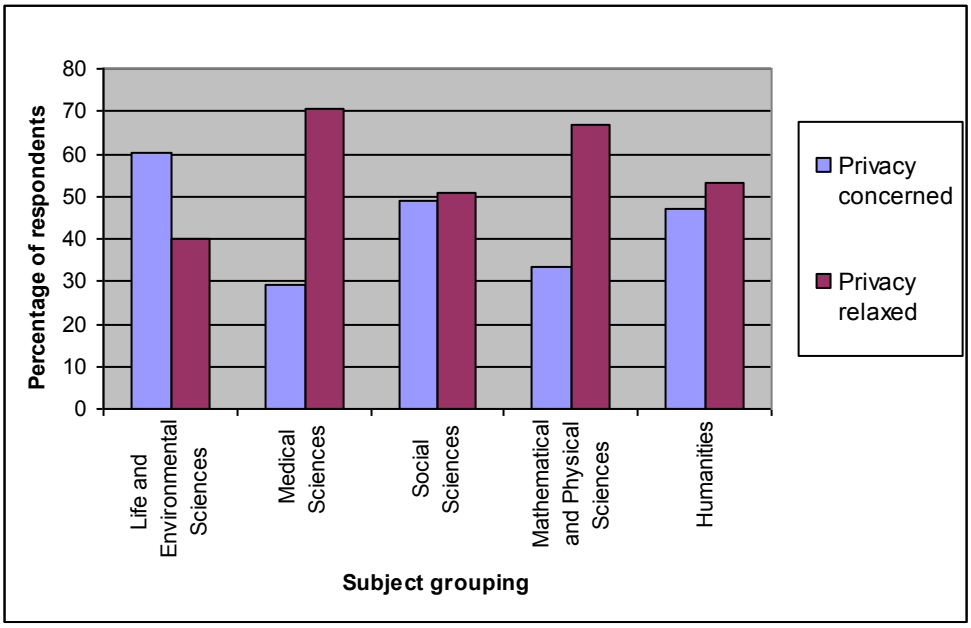

Figure 3. Westin privacy segmentations, generalised into privacy concern and privacy relaxedness, by subject grouping, as percentage of subject group.

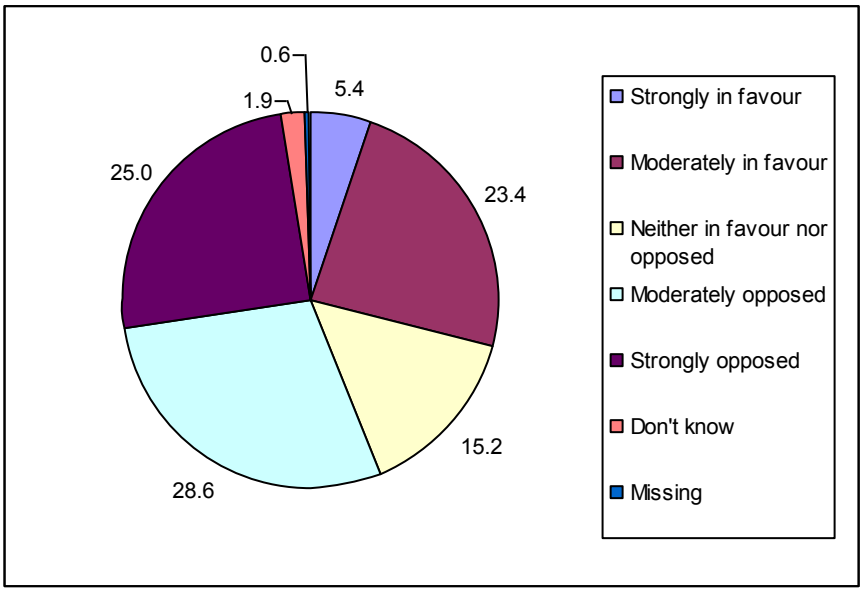

Figure 4. Attitudes of respondents towards the NICS (as percentage of total response)

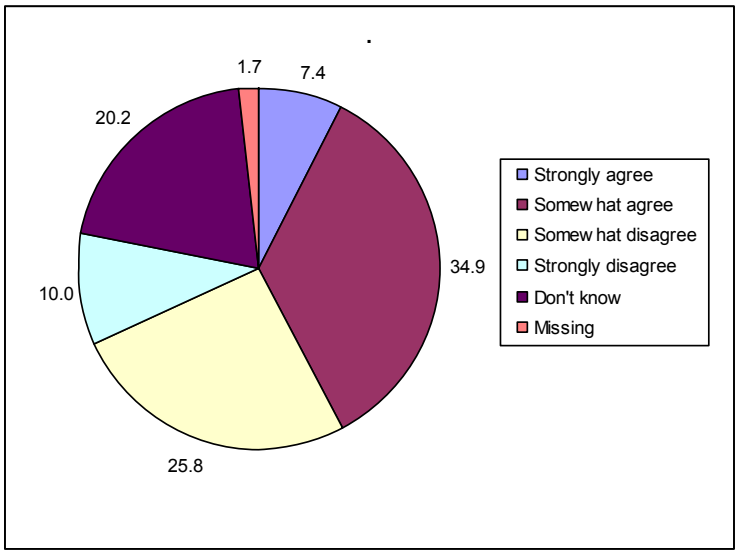

Figure 5. Respondents' agreement/disagreement with statement of trust in Government regarding purposes of the NICS, as percentage of total response

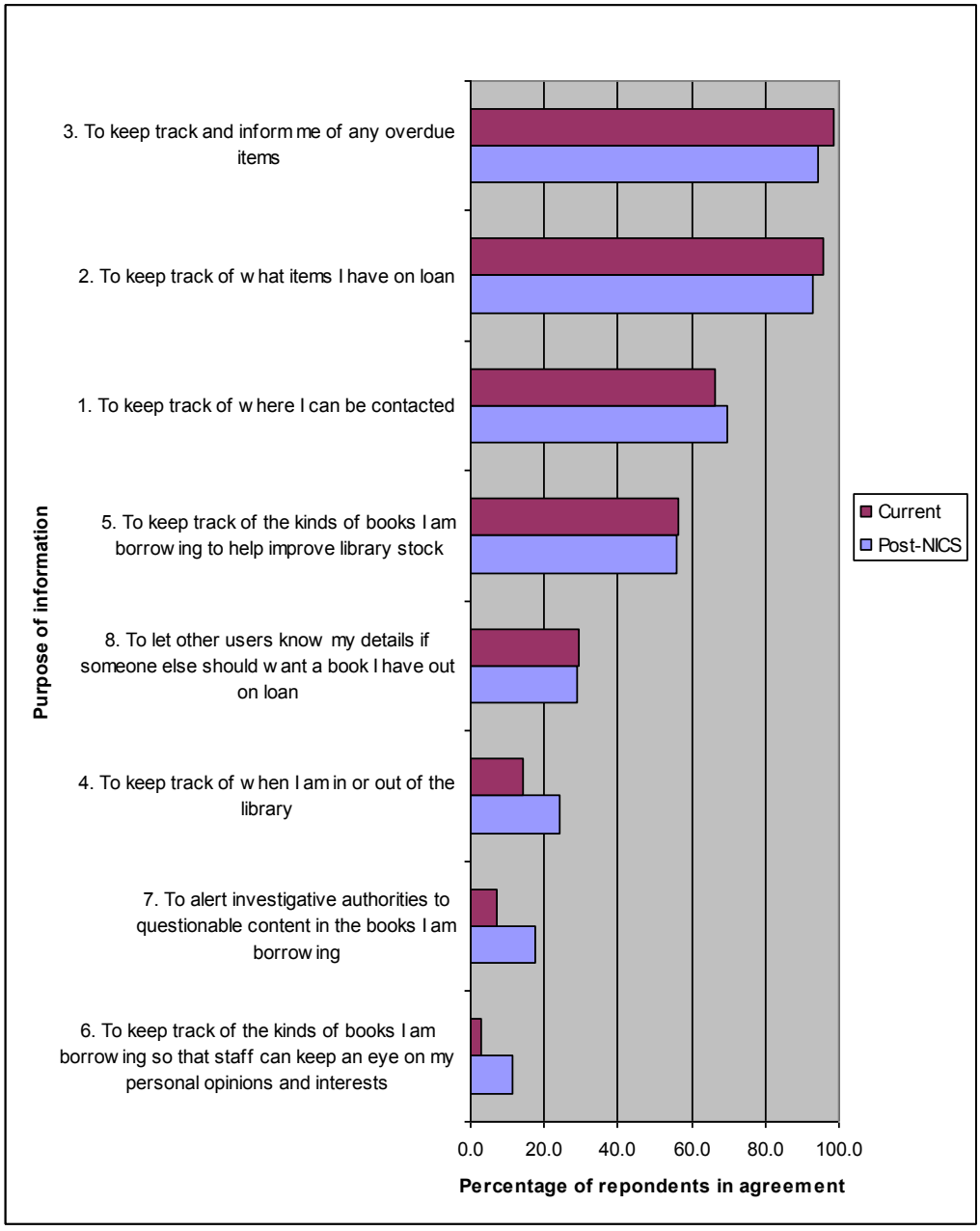

Figure 6. Comparison of respondents' agreement with potential purposes of information held about them by their libraries, currently and after the implementation of the NICS (as percentage of total response)

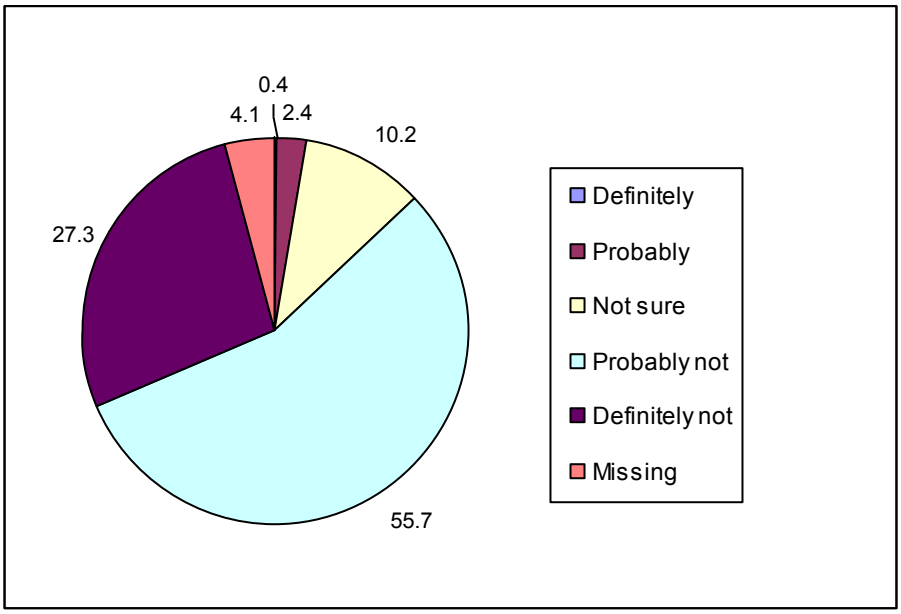

Figure 7. Respondents' opinions as to whether their libraries pass on information about them to other agencies outside the University

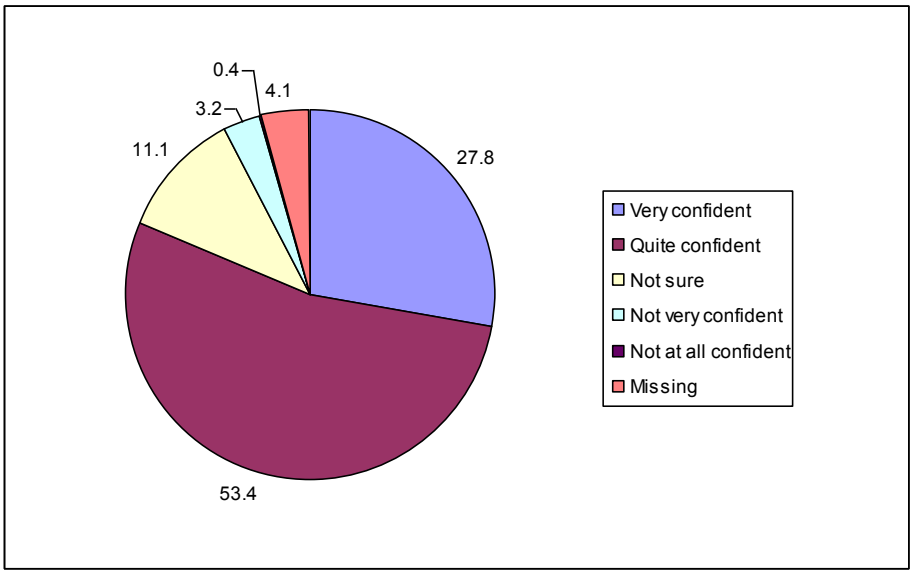

Figure 8. Respondents' confidence that their libraries dealt with their personal information in a proper and professional way, as percentage of total response