

# The War on Terror and Libraries, 2.45pm Tuesday 16<sup>th</sup> May

## Introduction

For the past four and half years I have been working for the FAIFE core activity of IFLA - the International Federation of Library Associations. FAIFE is the Freedom of Access to Information and Freedom of Expression Committee of IFLA, and its remit is to monitor, investigate and report on intellectual freedom issues that could affect the work of libraries and librarians all over the world. My work with FAIFE began in 2001, about a month and a half after the attacks on the World Trade Center in New York, and the repercussions of those events have been present in nearly all aspects of my research for the last four and a half years.

Since 9/11 we have seen the invasions of Afghanistan and Iraq, and continuing terrorist attacks around the world. Against this backdrop, it is the job of our elected officials to keep us safe, to play their role in a type of contract between the citizen and the nation state – in return for knowing more about us, the state will provide security and ensure our wellbeing in the face of whatever threats are present to our society [Slide 2]. When viewed in this way, it is no surprise that the actions governments all around the world have taken since 9/11 concentrate on the quick identification and imprisonment of terrorists, or making future terrorist atrocities preventable. But, despite governments best intentions, I have ended up considering a question for the last four and a half years that reminds me a little of something Margaret Atwood mentions in her book *The Handmaid's Tale* – namely: what are the differences between „freedom from and „freedom to ? In our quest to protect ourselves, are we going too far towards a world where the need for our governments to be suspicious overwhelms the need of citizens to exercise their intellectual freedom? By promising us freedom *from* terror, are they in fact squeezing our freedom *to* live our lives in accordance with the civil and political rights we have fought so hard to nurture over many years?

This paper will give my opinion on this question, based on my PhD work and on my work as a researcher for FAIFE. As it is the last academic paper I am likely to give for 18 months, and I thought it would be appropriate to recap exactly what has happened since 9/11 in terms of actions that affect librarians and library users. How have libraries become caught up in the war on terror and how have we, as librarians, reacted when intellectual freedoms are at stake?

## The Background

Whether we like it or not, public libraries in the United States, and elsewhere, have a strong connection with the events of September 11<sup>th</sup>. This is because in the weeks before the terrorist attacks, individuals who would later be named as hijackers supposedly used library computers at Hollywood Beach, Delray Beach and Broward County libraries in Florida. Following the terrorist attacks Broward County library patrons and employees called the police saying they thought a man fitting Mohammed Atta's description had used library computers. Katherine Hensman, a research librarian at Delray Beach, also called the police after she recognised one of the hijacker's pictures in the media – notifying them that he had been in the library (Sears, 2001). Elsewhere, it has been alleged that libraries played a central role in the

hijackers' preparations in Germany (DeVise, 2002). According to German prosecutors, a suspect in the hijackings had bragged to a German librarian in Hamburg about a potential attack more than a year before 9/11.

Although it has never been proven beyond doubt that the hijackers used the library computers to facilitate the attack, it was only a matter of time before US law enforcement sought to tie up perceived loopholes in their ability to surveil the communications methods of would-be terrorists. The USA PATRIOT Act, which I am assuming most people in this room will have heard of, was the legislative response to the terrorist attacks, an attempt to give law enforcement agencies more weapons in the fight to track down the perpetrators of such a crime. To understand the Patriot Act however, it is first important to understand the changes wrought by the events of September 11<sup>th</sup>, 2001. The terrorist attacks that day were to a large extent the catalyst for a shift in the nation state-citizen relationship around the world. Two examples from the United States serve to illustrate the change in the US situation regarding freedom of expression and privacy. Immediately following the attacks a White House spokesman declared that "all Americans... need to watch what they say, watch what they do", showing for the first time an official viewpoint that there may be some forms of behaviour more acceptable than others during the aftermath of a crisis (Pittman, 2002). The second example is the comments of then US Attorney General John Ashcroft referring to those who raised concerns regarding the loss of civil liberties following the terrorist attacks. He said: "... to those who scare peace-loving people with phantoms of lost liberty, my message is this: your tactics only aid terrorists, for they erode our national unity and diminish our resolve" (New York Times, 2001). Those who complain about the loss of liberties are playing into the hands of the terrorists. It is more important, he seems to be saying, to concentrate on tracking down terrorists and preventing future attacks. To do so, some civil liberties will need to be given up.

Many commentators have said that the PATRIOT Act, especially Section 215 relating to libraries, aptly captured this mood. Section 215 gave law enforcement agents the power to subpoena any library records, electronic or otherwise; while Section 216 gave the FBI the right to examine any library computer, monitor reading, Internet use or any other activity through roving wiretaps. It also means libraries can be requested to install tracking software on their computers. Requests under Section 215 were secret; librarians who are approached may not inform anyone of that approach under threat of jail. Standards required to request records or place wiretaps were substantially lowered. [Slide 3]

Since the instigation of the USA PATRIOT Act the American Library Association has fought tooth and nail to get the sections of the act relating to library user records repealed. The fight has been long and hard, and has seen an ongoing commentary on proceedings that has been played out in library journals, academic papers and in the regional and national US press. It is possible that the national recognition of US Librarians has never been higher since they stood up to the legislation; Senator Richard Durbin even demanded that the work of librarians to amend the PATRIOT Act be noted in the congressional record (ALA, 2006) [Slide 4]

One person who could tell us about the way US anti-terror legislation is targeting libraries is George Christian, a manager of digital records for three Connecticut

libraries [Slide 5]. In the summer of 2005 FBI agents handed Christian a national security letter which asked him to surrender all subscriber information, billing information and access logs of any person who used a specific computer at a library branch within his jurisdiction. Due to the nature of national security letters, recipients are extremely limited in the extent to which they can disclose that they have been served with one. Despite this, Christian refused to hand over the data, and since then his employer, Library Connection Inc., has been fighting in the courts to protest the FBI demand in public (Gellman, 2005).

Alongside Section 215, the use of National Security letters has grown massively since the passage of the PATRIOT Act. [Slide 6] The Bush administration has transformed the letters into tools that permit the clandestine scrutiny of US nationals and visitors who are not alleged to be terrorists or spies. FBI officials do not have to describe what they are looking for or why, and the letters are not reviewed after their use by the Justice Department or Congress. Records obtained through the letters are no longer destroyed as they were pre-2003 and all information gained is deposited into government data banks where it is shared widely among the federal government and beyond, including "appropriate private sector entities". This facilitates data-mining - which means that the impact of a National Security Letter is heightened because anyone's files can be scrutinized again at a later date "without a fresh need to establish relevance". Such a situation inevitably creates chilling effects but despite US papers publishing a detailed report on the problems regarding National Security Letters, their continued use was sanctioned through the reauthorisation of the PATRIOT Act in March this year. There are some changes from the original act, including a slightly higher bar for FBI agents to cross before being able to obtain library records, and an arrangement whereby recipients of a section 215 order are allowed limited disclosure of the order or can issue a limited challenge to its issuance. Despite this, the ALA analysis of the reauthorized act is that it still leaves the door open to wide search order requests (ALA, 2006)

### **But what of the rest of the world?**

While the PATRIOT Act has had chilling effects on freedom of expression in the US, librarians in the United States are not the only ones to have been affected by the fallout from September 11th. IFLA member countries all over the world have focused on the impact of the war against terror in the last four and half years.

Librarians today are doing their job in a world suffering from a climate of suspicion. It may not affect front desk activities in the vast majority of places but it is a situation, nonetheless, that is happening all around us. After all, since 2001 terrorist atrocities have taken place in Bali, Spain, Russia, Morocco, Saudi Arabia, Egypt and the United Kingdom. With each attack comes fresh suspicion and attempts to cast the net tighter still around the terrorist threat. I have focused to a great extent on the US in the first part of this paper, now I want to move on to a wider approach with a look at attempts to cut off terrorist communications on a medium that is inherently associated with modern librarianship: the Internet.

Since 2001 systemised efforts have been made in three specific areas relating to the online environment [Slide 7]. In the name of the war against terror and the protection of national security, previously unpopular legislative proposals have been re-

introduced that override and weaken existing data protection legislation. First there has been continuing progress towards the creation of a data retention structure, both at national levels and also through international co-operation. This means the preservation of Internet use records by ISPs for specific periods of time mandated by law.

Secondly, in many countries a system of online surveillance has been instituted, or expanded, to go alongside data retention, and communications between persons considered to be suspicious are monitored through the online equivalent of wiretaps. In most cases, judicial oversight of these proceedings has been lessened and the breadth of application increased with more agencies able to use generic warrants that can be served on multiple service providers. Finally, there has been a trend to re-evaluate what resources are made available online and to remove materials from the Internet on the grounds that terrorists should not be able freely access sensitive information relating to national security.

## **Data Retention**

I want to explore these three areas and their implications for libraries and their users, starting with data retention. Freedom of expression in an online sense means the freedom of the user to communicate and seek out information in an environment where activities are not monitored. Libraries, as providers of an appropriate environment for accessing information, are aware of this, but since September 11<sup>th</sup> the ability of the profession to protect user privacy is becoming less assured.

This is because it is now accepted that the Internet is being used by terrorists around the world to push their objectives and co-ordinate activities that may lead to the deaths of innocent civilians. US Secretary of Defence Donald Rumsfeld is on record as saying 80% of what terrorists need to know to plan attacks can be found on the Web via publicly accessible databases such as Google Earth (Weiman, 2004). Terrorists finding and sharing this information worry government security agencies to the extent that governments are beginning to desire more oversight of traffic on the Internet, and one way of doing this is to store Internet user data in case it is needed in future criminal investigations [**Slide 8**]. In this approach it is Europe that is leading the way. In December last year the European Parliament finalised a Directive on Data Retention that has repercussions for Internet users freedom of expression. Under proposals put forward by Great Britain, Spain, France and Ireland, any telecommunications company or Internet service provider in the EU is now obliged to store traffic data of its customers for a minimum of six months and a maximum of two years (Leyden, 2005). 450 million telecommunications customers will be affected, including libraries. Traffic data is all telecommunications and Internet usage aside from the actual content of messages, which means information about who you have called or emailed, when and where, along with what you have been looking at on the Internet. Taken as a whole, such data can create a map of human associations, human activity and human intention. The reason for such an undertaking is simple: it cannot be precluded that phones, text messages, email or the Internet will be used for a crime (FIFR, 2004).

This situation is a result of the post-9/11 mindset, the climate change that has settled upon the world since that date. Prior to 9/11, the EU's position on data retention was

that it was not needed and should not take place (Privacy International and EPIC, 2004). Post 9/11 everything changed and the bombings in Madrid and London underscored the situation. Elsewhere in the world, from Australia to Argentina, retention of telecommunications data is on the agenda like never before (Privacy International, 2004b). This month, in a reversal of the Bush administration's previous position and one likely influenced by the EU decision, the United States has begun to consider wholesale data retention, a situation which until recently was unthinkable under the terms of the US Constitution (McCullagh, 2006).

What worries defenders of civil liberties is the mission creep that is becoming apparent in these proposals. While data retention legislation is supposedly needed to fight against terrorists, proposals such as the Directive on Data Retention are in fact not limited to this, meaning stored data can be used in normal criminal investigations. Statewatch, an observatory on the European Union commented in 2004: "This is a proposal so intrusive that Ashcroft and company can only dream about it, exceeding even the US Patriot Act." Which is probably why President Bush has been so keen for Europe to undertake this action – agreements between the US and EU in the years following 9/11 mean that US law enforcement agencies are likely to be able to access stored telecommunications data in the same way as they are able to access European air passenger information (Statewatch 2002; 2004).

## **Surveillance**

Alongside the retention of data is the real-time monitoring of Internet use. As digital communications technology has developed it has thrown up more categories of information of use to law enforcement. Tens of web sites can be surfed in a few minutes for example, which could theoretically reveal personal interests, preferences or political affiliations very quickly. In this way it is similar to the content of phone conversations, leaving privacy organisations worried about the extent to which current laws protect access to it (Privacy International, 2003).

The techniques used to monitor Internet activity are based on packet sniffing technology, meaning that the traffic flowing in and out of networks is monitored and sniffed for keywords, phrases, strings, IP addresses or email accounts. This data can be retained or passed on to security forces for examination. Around the world many countries have begun to monitor Internet use including Russia, Iran, Vietnam and Tunisia – which controversially hosted the final phase of the World Summit on the Information Society last year and currently has imprisoned a lawyer for suggesting online that prison conditions in Tunisia resembled those in Iraq. Perhaps the best known example of countrywide Internet surveillance comes from China however, where extremely sophisticated surveillance measures are used to monitor dissident activity on Internet messageboards, in chatrooms and via email [Slide 9]. The effects on freedom of expression in China can be seen in the number of dissidents in prison for Internet-related offences. Reporters Sans Frontiers estimate that there are currently 50 individuals in prison for offences that range from posting critiques of government policy online to disseminating materials advocating democracy (RSF, 2006).

When discussing the issues of Internet surveillance and terrorist use of the Internet it is possible to lose sight of the end providers of Internet access such as libraries. Surveillance equipment is often implemented at a network level, making it appear

distant from public access PCs in libraries, and terrorist webmasters are unlikely to use public Internet facilities to code web sites and update web pages. To imagine this would be to miss the point however, for the consequences of surveillance do affect the atmosphere in which individuals access the Internet in libraries [Slide 10]. In the digital environment of the Internet access to usage records is made simple, for it is easier to monitor email and use of the World Wide Web, and archiving user activity is straightforward. Libraries are able to monitor and store Internet requests for information and form a general knowledge of web pages visited and searches undertaken. It is possible to build up a considerable profile of an individual through an examination of their library use – presumably another reason for the PATRIOT Act's coverage of library business records.

### **Removal of Information**

The terrorist threat has therefore led governments towards a greater interest in being able to retain, investigate and control online information flow. At the same time there has been, especially under the present US administration, a concerted effort to reassess the amount of sensitive information easily available to library and Internet users. In the US, the type of information being removed from websites includes reports on global warming, risk management plans providing information about the dangers of chemical accidents and university research on online maps (Blumenfeld, 2003; Leahy, 2006; OMBWatch, 2002) [Slide 11]. Previously long available declassified information relating to Saudi Arabia is now off limits to researchers at the US National Archives, and, according to the Federation of American Scientists, government classification activity increased 75% between 2001-2004 (Aftergood, 2005). This attitude has directly affected libraries in the US, especially federal deposit ones. Hundreds of thousands of documents have disappeared from the shelves of libraries in North Texas, for example, and the government's Superintendent of Documents is limiting the amount of new paper documents being created. Material that is going out of print includes patent and trademark information, navigational charts and congressional reports and hearings. At the same time as this process, funds for federal deposit libraries are being slashed, with the Fort Worth Weekly reporting last year that at the University of North Texas the depository library was receiving less money than the budget for military bands (Malone, 2005).

Should we, as librarians, aid and abet the removal of information as part of our duty towards national defence? Should we be surprised that a government wishes to limit information access while there is a war on? A more pressing question to ask however is: once a situation like this occurs in a country, how can it be turned back? The US government since 9/11 has erred on the side of caution when releasing information rather than the side of disclosure. It is the *climate* surrounding legislation like the Patriot Act that has caused this situation, rather than any specific language of the law. There is an overwhelming sense that safety and prudence must come first. The cumulative effect of this climate is the lowering of expectations regarding government accountability and doubts in the ability of people to check political abuses or change their leaders. In short, there is a danger that people will expect less access to information. If citizens are unable to examine even the most fundamental actions of government, what are the consequences for democracy, and those cornerstones of democracy, libraries?

## **The IFLA/FAIFE World Report 2005**

Last year the FAIFE Office undertook a survey for the 2005 IFLA/FAIFE World Report. One of the special areas of focus for the world report was anti-terror legislation, and in the responses from 84 countries we discovered that librarians all around the world are concerned about the effects of the current war on terror.

Respondents' comments made regarding anti-terror legislation varied, in that some countries, such as the US, were already experiencing the effects of new laws and others were waiting to find out what the implications for libraries were. This was the case in Japan, the Philippines, Kenya, and Uganda - four countries where anti-terror proposals were pending. In Uganda, for example, open-ended anti-terror legislation was passed in 2002. The Uganda legislation is similar to the USA PATRIOT Act in that it does not explicitly mention libraries in its text. It does, however, empower law enforcement officers through a court order to search for materials on specified premises - which means that an investigating officer has the discretion to search a library or user records if this is considered of substantial value to the investigation. While there have been no investigations into library details and no cases have explicitly affected libraries so far, the respondent worried that library users' privacy may well be affected in the future. This was also the situation outlined in the Canadian response, which mentioned that anti-terror legislation passed in 2001 had not yet affected libraries, although a future amendment might have some impact on users.

In Europe there were also worrying responses, the most notable of which was from the Netherlands where oversight and transparency are the two core concerns of the library community in the face of anti-terror legislation that could have serious consequences for library users. The legislation is very similar in format to that of the PATRIOT Act, in that it gives law enforcement the ability to access records of all 'holders of data' - including libraries. According to Dutch librarians and the NGO European Digital Rights (EDRi), the law makes it much easier for security agencies to get access to data by lowering legal barriers and safeguards. As a statement by FOBID, the national umbrella organisation for co-operation between the national library organisations, put it:

"Libraries are not convinced by soothing remarks that all law enforcement activities in the Netherlands are supervised by the public prosecutor or judge. That provides no guarantee against a too broad use of the powers granted by the draft law. In the United States, where the powers are more broadly defined, many more inquiries have been made than originally claimed, and with a much broader scope than could have been expected from the original intention to fight terrorism. The intended fight against terrorism could thus easily degenerate into a kind of moral police supervision."

The parallels with the situation in the United States are all too clear. Librarians in the Netherlands are worried about the potential for abuse of new laws and the potential impact on users' freedom of expression. They are concerned that law enforcement agencies will not reveal the extent to which libraries are used in investigations, and they are anxious that this step will be the first on a slippery slope towards an acceptance of the monitoring of library use.

As a postscript to the 2005 World Report we have seen libraries in the UK caught up in the fallout of the July 7 bombings in London. Following moves by the government to introduce new anti-terror legislation, CILIP commissioned a barrister's opinion on the right of the police and other security agencies to look at library records or undertake surveillance in libraries, and they were also active in the LIS consortium that lobbied for amendments to the Terrorism Bill 2006. The consortium succeeded in getting the idea of intent included in clause 2 of the Bill – which was the clause dealing with the dissemination of terrorist publications. Without this, any member of library staff could have been open to being charged with disseminating Terrorist publications for simply doing their job and with little in the way of effective defence open to them - especially as the definition of a Terrorist publication in the bill was so vague. CILIP's intervention means that now they have to be shown to have intended to promote terrorism by the dissemination of "terrorist publications".

## **Conclusion**

In light of everything I have just said, how can we live up to our responsibilities towards our users? For instance, how many of our patrons know – or care – that their information seeking choices are likely to be stored somewhere for up to two years?

The problem for our profession is that we have seen the effects of law enforcement in the library before, for example in the case of the Library Awareness program that ran in the US from 1973-76, and again from 1985 onwards. During this time FBI agents were visiting libraries all over the country requesting information on foreign users. The profession was up in arms, to the extent that it was later discovered the FBI had investigated over 100 US librarians and their associates. Furthermore, because the program was supposed to have ended in 1987 but was later discovered to be still going in 1989, US librarians felt grossly misled by the FBI – something that is likely filtering through in attitudes to the Justice Department today. When authorities have lied in the past it is not unnatural to be suspicious in the future.

And unfortunately the future is here now. Post-September 11<sup>th</sup> we are in a new environment, a new climate of information provision. Some of the trends we are seeing, such as electronic surveillance and data retention, are not new – the novelty is the speed with which they have gained acceptance. With fear of terrorism stoked by governments and the media, the environment in which we operate might be changing, along with public perceptions of it. If fewer people are convinced that privacy is a fundamental right then governments are free to interfere with access to information even to the extent of monitoring library use. It has been done before. Likewise, if information disappears from the public sphere and things stay that way, then there is an acceptance of the situation and it becomes more difficult to turn the clock back to an environment of freedom of information. Librarians have been part of freedom of information struggles in the past and we must not let this work go to waste in an environment characterised by fear. We must be on guard, because there is a danger that this situation could be abused, in the same way as certain governments around the world use the pretext of fighting terror to stifle freedom of expression or silence political opponents. Society will need its watchdogs and it will need people holding governments to account. Libraries have an important role to play in making this happen, by opening our doors to an area for discussion which lets all sides of an argument be presented. We must strive to provide an environment where an

individual can explore their intellectual concerns free from prying eyes looking over their shoulder to their book, or to their computer screen, and we must explain to our communities and our politicians the value of such an environment and show that libraries are able to make a difference to the way that people understand each other. It is our business to provide our users access to information; it is not our business to be party to a system whereby information-seeking activities are hampered by surveillance and censorship.

## Bibliography

- Aftergood, S. 2005. The age of missing information. [online], available: <http://slate.msn.com/toolbar.aspx?action=print&id=2114963> [April 11, 2005]
- American Civil Liberties Union. 2005. Patriot acts abuses and misuses abound, ACLU says. [online], available: [www.aclu.org/news/NewsPrint.cfm?ID=17920&c=206](http://www.aclu.org/news/NewsPrint.cfm?ID=17920&c=206) [April 11, 2005]
- Bascombe, D. 2004. An update of anti-terror legislation in the Commonwealth. [online], available: <http://www.commonwealthtuc.org/CHRI%20Report.doc> [April 11, 2005]
- Coolidge, K. "Baseless hysteria": The controversy between the department of justice and the ALA over the USA PATRIOT Act. [online], available: [http://www.aallnet.org/products/pub\\_llj\\_v97n01/2005-01.pdf](http://www.aallnet.org/products/pub_llj_v97n01/2005-01.pdf) [April 18, 2005]
- DeVise, D. 2002. Terror hunt may end privacy at the library. *The Miami Herald*. [online], available: <http://www.miami.com/mld/miamiherald/news/3979136.htm> [April 18, 2005]
- Diaz, J. 2003. A librarian's dilemma. *San Francisco Chronicle*. [online], available: <http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2003/02/02/ED103750.DTL> [April 11, 2005]
- EDRI. 2005. Ireland sneaks data retention into law. [online], available: <http://www.edri.org/edriagram/number3.5/ireland> [April 11, 2005]
- EDRI. 2005. Secret minutes EU data retention meeting. [online], available: <http://www.edri.org/edriagram/number3.7/retention> [April 11, 2005]
- EDRI. 2005. UNESCO NL recommendations to human rights and Internet. [online], available: [www.edri.org/edriagram/number3.5/unesco](http://www.edri.org/edriagram/number3.5/unesco) [April 11, 2005]
- Eggen, D. 2005. Patriot act changes to be proposed. *The Washington Post*. [online], [www.washingtonpost.com/ac2/wp-dyn/A26235-2005Apr4?language=printer](http://www.washingtonpost.com/ac2/wp-dyn/A26235-2005Apr4?language=printer) [April 7, 2005]
- Finch, B. 2004. Government studies vanish from reporters' view. *Nieman Reports*, Summer 2004, Vol. 58, No. 3, P20-22. [online], available: <http://www.nieman.harvard.edu/reports/04-2NRSummer/V58N2.pdf> [April 18, 2005]
- Forum Computer Professionals for Peace and Responsibility. 2004. The EU wants to know ... [online], available: [www.statewatch.org/news/2004/sep/prel-trafficdata-retention.pdf](http://www.statewatch.org/news/2004/sep/prel-trafficdata-retention.pdf) [April 11, 2005]

- Gellman, B. 2005. The FBI's Secret Scrutiny. *Washington Post*. [online], available: [www.washingtonpost.com/wp-dyn/content/article/2005/110](http://www.washingtonpost.com/wp-dyn/content/article/2005/110).. (nb. reference unfinished) [May 3, 2005]
- Hudson, M. U.S. Libraries and the "War on terrorism". *New Politics*, vol. 10, no. 1, whole no. 37, Summer 2004. [online], available: <http://www.wpunj.edu/~newpol/issue37/Hudson37.htm> [April 18, 2005]
- Jashik, S. 2005. \$7 billion to fix a non-problem. *Inside Higher Education*. [online], available: <http://insidehighered.com/news/2005/10/24/wiretap> [May 3, 2005]
- Kull, S. 2004. The press and public misconceptions about the Iraq war. *Nieman Reports*, Summer 2004, Vol. 58, No. 3, P64-66. [online], available: <http://www.nieman.harvard.edu/reports/04-2NRSummer/V58N2.pdf> [April 18, 2005]
- Lawyers Committee for Human Rights. 2003. Assessing the new normal: Liberty and security for the post-September 11<sup>th</sup> United States [online], available: <http://www.humanrightsfirst.org/pubs/descriptions/Assessing/AssessingtheNewNormal.pdf> [October 31, 2004]
- Leahy, S. 2006. When Science Inconveniences Bush. *IPS News*. [online], available: Source: <http://www.ipsnews.net/news.asp?idnews=33032> [April 27, 2006]
- Lewis, A. 2004. The responsibilities of a free press. *Nieman Reports*, Summer 2004, Vol. 58, No. 3, P60-62. [online], available: <http://www.nieman.harvard.edu/reports/04-2NRSummer/V58N2.pdf> [April 18, 2005]
- Leyden, J. 2005. Privacy „dark ages“ force activist rethink. *The Register*. [online], available: [www.theregister.co.uk/2005/04/01/privacy\\_resistance/print.html](http://www.theregister.co.uk/2005/04/01/privacy_resistance/print.html) [April 7, 2005]
- Lichtblau, E. 2005. Antiterrorism law defended as hearings start. *New York Times*. [online], available: <http://www.nytimes.com/2005/04/06/politics/06patriot.html?ex=1113969600&en=04b82752dd55e62e&ei=5070> [April 11, 2005]
- McCarthy, A. 2005. Why sections 214 and 215 should be retained. [online], available: [www.patriotdebates.com/sections-214-and-215](http://www.patriotdebates.com/sections-214-and-215) [April 7, 2005]
- McCullagh, D. 2006. Congress may consider mandatory ISP snooping. *CNET*. [online], available: [http://news.com.com/Congress+may+consider+mandatory+ISP+snooping/2100-1028\\_3-6066608.html](http://news.com.com/Congress+may+consider+mandatory+ISP+snooping/2100-1028_3-6066608.html) [May 3, 2005]
- Malone, D. 2005. Governing in the dark. *Forth Worth Weekly Online*. [online], available: [www.fwweekly.com/issues/2005-02-23/metropolis.asp](http://www.fwweekly.com/issues/2005-02-23/metropolis.asp) [April 11, 2005]
- Markoff, J. 2005. U.S. Steps Into Wiretap Suit Against AT&T. *New York Times*. [online], available:

<http://www.nytimes.com/2006/04/29/us/29nsa.html?ex=1147147200&en=e062476208273876&ei=5070&emc=eta1> [May 3, 2005]

Mathieson, S. 2005. Closing the net on crime. *The Guardian*. [online], available: <http://technology.guardian.co.uk/print/0,3858,5312879-117422,00.html> [May 3, 2005]

Matthews, J. and Wiggins, W. 2001. Libraries, the Internet and September 11<sup>th</sup>. *First Monday*. [online], available: [http://www.firstmonday.org/issues/issue6\\_12/matthews/index.html](http://www.firstmonday.org/issues/issue6_12/matthews/index.html) [April 11, 2005]

Mendoza, M. 2005. AP Review: Government reducing access to info. *The Guardian*. [online], available: [www.guardian.co.uk/worldlatest/story/0,1280,-4862137,00.html](http://www.guardian.co.uk/worldlatest/story/0,1280,-4862137,00.html) [April 11, 2005]

Minow, M. 2001. The USA PATRIOT Act and Patron Privacy on Library Internet Terminals. *California Libraries*, Vol. 11, No. 11. [online], available: [http://www.cla-net.org/resources/articles/minow\\_usapatriot.php](http://www.cla-net.org/resources/articles/minow_usapatriot.php) [April 18, 2005]

Moeller, S. The President, press and weapons of mass destruction. *Nieman Reports*, Summer 2004, Vol. 58, No. 3, P66-68. [online], available: <http://www.nieman.harvard.edu/reports/04-2NRSummer/V58N2.pdf> [April 18, 2005]

Newsletter on Intellectual Freedom. 2004. November, Vol. LIII, No.6. p250

OMB Watch 2002. Access to government information post September 11<sup>th</sup> [online], available: <http://www.ombwatch.org/article/articleview/213/1/1/> [October 31, 2004]

Popp, T. 2005. Wireless Wiretapping by Trey Popp. *Technology Review*. [online], available: [http://technologyreview.com/articles/05/08/wo/wo\\_082205popp.0.asp](http://technologyreview.com/articles/05/08/wo/wo_082205popp.0.asp) [May 3, 2006]

Privacy International and EPIC. 2004. Privacy and Human Rights 2004. [online], available: [www.privacyinternational.org/survey/](http://www.privacyinternational.org/survey/) [April 11, 2005]

Privacy International. 2003. Silenced. [online], available: <http://www.privacyinternational.org/survey/censorship/Silenced.pdf> [June 23, 2005]

Privacy International. 2004a. Privacy International and EPIC release 2004 annual global privacy survey. [online], available: [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-83992](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-83992) [April 11, 2005]

Privacy International. 2004b. Invasive, illusory, illegal and illegitimate: Privacy International and EDRI response to the Consultation on a Framework Decision on Data Retention. [online], available: [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-103020](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-103020) [April 11, 2005]

Privacy International. 2005. Ireland's parliament approves communications data retention. [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-140716](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-140716)

Rasch, M. 2005. Wiretapping, FISA and the NSA. *The Register*. [online], available: [www.theregister.co.uk/2006/01/12/us\\_wiretapping\\_laws/](http://www.theregister.co.uk/2006/01/12/us_wiretapping_laws/) [May 3, 2005]

Rosenbaum, D. 2001. "A Nation Challenged: Questions of Confidentiality; Competing Principles Leave Some Professionals Debating Responsibility to Government," *New York Times*, (23 November).

RSF. 2006. Cyberdissidents imprisoned. [online], available: [http://www.rsf.org/rubrique.php3?id\\_rubrique=119](http://www.rsf.org/rubrique.php3?id_rubrique=119) [May 3, 2006]

Schell, J. 2005. Faking civil society. [online], available: [http://www.truthout.org/docs\\_2005/040705E.shtml](http://www.truthout.org/docs_2005/040705E.shtml) [April 18, 2005]

Sears, R. 2001. Librarians face new issues in patron confidentiality. *New York Times*. [online], available: [http://www.infoshop.org/alibrarians/public\\_html/article.php?story=01/12/12/3987276&mode=print](http://www.infoshop.org/alibrarians/public_html/article.php?story=01/12/12/3987276&mode=print) [April 18, 2005]

Sherman, M. 2005. Officials urge renewal of Patriot Act. [online], available: [www.nola.com/printer/printer.ssf?/base/politics-6/111270224852670.xml&storylist](http://www.nola.com/printer/printer.ssf?/base/politics-6/111270224852670.xml&storylist) [April 7, 2005]

Singel, R. 2005. The business of fighting terror. *Wired*. [online], available: <http://wired-vig.wired.com/news/print/0.1294,66177,00.html> [April 11, 2005]

Starr, J. 2004. Libraries and national security: An historical review. *First Monday*. [online], available: [http://www.firstmonday.org/issues/issue9\\_12/starr/](http://www.firstmonday.org/issues/issue9_12/starr/) [April 18, 2005]

Statewatch 2002, European parliament to cave in on data retention [online], available: <http://www.statewatch.org/news/index.html> [May 29, 2002]

Statewatch. 2004. Data retention comes home to roost – telephone and Internet Privacy to be abolished. [online], available: <http://www.statewatch.org/news/2004/apr/21dataretention.htm> [April 11, 2005]

Swire, P. 2005. A response to Andrew McCarthy. [online], available: [www.patriotdebates.com/sections-214-and-215](http://www.patriotdebates.com/sections-214-and-215) [April 7, 2005]

Whalen, S. 2003. Secret Saudi History. *The Palestinian Chronicle*. [online], available: <http://palestinechronicle.com/story.php?sid=20030812221737540> [April 18, 2005]

Zetter, K. 2004. Big business becoming Big Brother. *Wired*. [online], available: [www.wired.com/news/print/0.1294,64492,00.html](http://www.wired.com/news/print/0.1294,64492,00.html) [April 11, 2005]

## **Email**

Becker, B. ([bbecker@ala.org](mailto:bbecker@ala.org)). (April 12 2005). Re: questions for world report gathering. Email to Stuart Hamilton ([sha@db.dk](mailto:sha@db.dk))