World Library and Information Congress: 69th IFLA General Conference and Council

1-9 August 2003, Berlin

Code Number: 184-E
Meeting: 112. Free Access to Information and Freedom of Expression (FAIFE)
Simultaneous Interpretation: Yes

The War on Terrorism – Towards a 'less free, less choice' Internet for Library Users?

Stuart Hamilton
IFLA/FAIFE, Copenhagen, Denmark

Introduction

Last year's FAIFE Open Session in Glasgow examined the 12 months following the terrorist attacks of September 11th and their effects on libraries. Nearly two years after these events, libraries and their users are still being affected by actions undertaken by governments around the world in name of the 'War on Terror'. The information-seeking environment, particularly on the Internet, has become a different place as new intelligence agencies monitor communications and new regulations govern what information can and cannot be accessed online. In the past twelve months much has happened, not least the fighting of a war in Iraq. It is apparent, as was promised, that the War on Terror is far from over. What role do libraries play in these conditions? How can we continue to provide free, equal and unhampered information to our users at a time when there are increasing constraints on our ability to do so?

This paper aims to update the situation in light of the events of the past year. While the effects of the war in Iraq on Internet-accessible information shall be discussed the main intention is to provide an idea of the overall trends we are facing with regards to freedom of access to information online. Some of the future developments the library community should look out for will be highlighted, along with activities in the private sector that have some bearing on the overall situation. It appears we are seeing a consolidation of anti-terror activities undertaken since September 11th and this, combined with the emergence of a more regulatory approach by governments in all areas of Internet governance, is leading to the possibility of a 'less free, less choice' Internet for library users in the future.

The War in Iraq and the Management of News

Earlier this year coalition forces 'liberated' Iraq in an expansion of the war against terrorism.

In what turned out to be a brief period of major conflict, allied soldiers brought down Saddam Hussein's regime in less than 6 weeks. Coverage of this conflict was played out on TV screens and PCs around the world in a way never seen before, even in the first Gulf War and the war in Afghanistan. Online coverage of the conflict was on a great scale, with hundreds of sources of varying views and opinions. This variety showed the true value of the Internet as an information source, as demonstrated by the numbers of American citizens turning to overseas news sources for opinions different to the prevailing media stances in the United States. Despite the success of cable TV in covering the first Gulf War, those interested in a truly alternative point of view would have been restricted to picking up print copies of foreign newspapers, sometimes days after events, to compare versions of events. 12 years on, those interested in the conflict found themselves with a variety of global television news channels to choose from (BBC, Al-Jazeera) and countless online news sources.

Unfortunately, it would be wrong to think that an explosion of new sources from abroad negated the threat of censorship. On the contrary, it is possible that news from the ground in Iraq was more tightly managed than ever before. And management of news did not stop with the embedding of reporters and the daily news briefings from specially built sets in Qatar – it too extended to the Internet as government supporters sought to prevent publication of information considered unhelpful to allied efforts.

Consider the case of the YellowTimes.com, which was taken offline after it was found to be showing pictures of American prisoners of war in Iraq[1]. Yellow Times, which is an alternative news website, was suddenly shut down by its hosting service during the first week of February 2003. According the MemoryHole website, which "exists to preserve and spread material that is in danger of being lost, is hard to find, or is not widely known" the host claimed that Yellow Times was using up too many resources, yet when the owners of Yellow Times offered to pay for more service, the host refused. This action was taken despite previous pictures of Iraqi prisoners of war on US network television and newspapers[2].

Alternative TV news stations such as the Qatar based Al-Jazeera also courted controversy by showing pictures and interviews with US prisoners of war during the conflict. These actions are thought to have caused the repeated hacking of Al Jazeera's English language website which at the time of writing (18/07/2003) is still not available for viewing[3]. The site was originally hacked so that the front page was replaced by a stars and stripes logo and the words 'Let Freedom Ring'. Al Jazeera has had repeated problems trying to find a hosting service for its website and indeed reported to the New York Times that companies were coming under non-stop political pressure not to do business with the channel. Indeed Yahoo, which in the past has used freedom of speech mandates in the US constitution to justify displaying Nazi memorabilia on its auction sites, refused to carry Al Jazeera advertising due to 'war-related sensitivity'[4].

Al Jazeera was not the only website defaced during the Iraq conflict - websites from all across

[1] Yellow Times: http://www.fair.org/press-releases/iraq-censorship.html ; http://www.scoop.co.nz/mason/stories/HL0303/S00228.htm ; http://www.thememoryhole.org/war/yt-misleading.htm ;http://www.antiwar.com/orig/yt.html

[2] Prisoners of war on US TV and newspapers: http://www.crimesofwar.org/special/Iraq/brief-pow.html and http://www.news.com.au/common/story_page/0,4057,6200773%255E1702,00.html

[3] Al Jazeera: http://english.aljazeera.net/

[4] The Register: Al Jazeera and the net: Free speech, but don't say that: http://www.theregister.co.uk/content/6/30131.html

the pro and anti-war spectrum were defaced. According to an Estonian firm that monitors hack attacks the first week of the war saw 20,000 such defacements[5]. These actions are troubling for the free flow of information on the Internet as they show how easy it is for individuals to deny access to information. Ironically, attacks like these are motivating efforts to increase regulation of the Internet through new legislation, which ultimately may end up stifling free expression instead of securing it.

Consolidating the 'War on Terror'

Events surrounding the conflict in Iraq followed a year where there has been a distinct effort on the part of several governments to consolidate and even extend anti-terror legislation that affects the information on the Internet.

We are seeing systemised efforts to extend three specific actions relating to the online environment. 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 Internet Service Providers for specific periods of time mandated by law. These records contain information on websites visited and individuals emailed, and are to be made available to law enforcement agencies on request. 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. Finally, in the name of the war against terror and the protection of national security, there is a trend to re-evaluate what resources are made available online and to remove materials from the web on the grounds that terrorists should not be able freely access sensitive information relating to national security. The type of information being removed ranges from location of water resources to university research on online maps[6].

Anti-terror Packages and the PATRIOT Act

These actions come together in what is called an 'Anti-terror' package, a piece of legislation which supposedly provides a government with the tools to combat terrorism in the information age. The rationale behind these acts is the knowledge that terrorists, especially in the case of the September 11th attacks, are using online communications to plan atrocities. Library computers with Internet access were used by terrorists in Florida in the run-up to the World Trade Centre attacks[7].

These anti-terror acts have now been up and running for over year in many countries. With regards to the Internet, the new laws mainly concentrate on data retention or interception of communications, although many countries are concentrating on both.
In Europe, new laws were passed in France, Spain, Denmark, Germany, Italy, United Kingdom and Russia. Russia has attempted to ban all forms of extremist activity on the Internet with a very vague definition of 'extremism' that includes terrorist activity. Prevention of terrorism has also been cited as the reason to pass new laws in Tunisia, South Africa, India,

[5] War hack attacks tit for tat: http://www.wired.com/news/infostructure/0,1377,58277,00.html?tw=wn_ascii
[6] Dissertation could be security threat: http://www.washingtonpost.com/wp-dyn/articles/A23689-2003Jul7.html and Access to government information post September 11th: http://www.ombwatch.org/article/articleview/213/1/1/
[7] Terrorists leave paperless trail: http://www.wired.com/news/politics/0,1283,46991,00.html

Philippines, New Zealand, Columbia, Cuba and Canada. Further vague definitions of 'terrorist' are found in the Philippines law, and also in Tunisia where a special 'Cyber-Police' force has been set up to monitor users of sites the government considers 'subversive'[8].

It is in the United States however, that the most influential anti-terror measures were passed, and these new laws, collectively known as the USA PATRIOT Act, have been used as a template for other countries around the world. To this end it is instructive to consider briefly how the act has been used in the past year, especially in relation to libraries, for this might give a taste of things to come for other nations.

The PATRIOT Act is a very broad anti-terror package that was passed in October 2001. Section 215 of the act is of most consequence to librarians, as it gives federal investigators greater authority to examine all book and computer records at libraries. While investigators are required to get a search warrant from a federal court before seizing library records, those proceedings are secret and not subject to appeal. The act forbids libraries from informing patrons that their reading or computer habits are being monitored by the government.

'Libraries are for democracy not surveillance'[9]

So far it has been difficult to assess to what extent the act has been applied in libraries due to the gag order that prevents individuals from going public with the information. Requests by civil liberties groups for information on its use has produced little except for an admission from security agencies that some investigation into library records has taken place. Surveys undertaken at the University of Illinois, however, show that 545 libraries out of 1505 surveyed have been approached by law enforcement agencies, including the FBI, for information about patrons' reading habits and Internet preferences. Whether this figure is in reality higher is open to question, for the PATRIOT Act makes it illegal for persons or institutions to disclose whether or not a search warrant has been served[10].

The American Library Association has reacted to the act by denouncing it and seeking to have sections of it amended. So far, according to the ALA website, 47 library associations across the US have added their support to this position[11]. In many libraries, signs have gone up warning users that their activities could be monitored by federal agents. Librarians are taking steps to protect user privacy by avoiding the creation of information that could personally identify patrons. The idea is that information that is not created cannot be collected. On top of this, legislation is now in the US Congress to exempt library and bookstore records from the PATRIOT Act. Several dozen other lawmakers, from both sides of the political spectrum, have endorsed the measure which also has the backing of the ALA and the American Booksellers Association. IFLA/FAIFE has not been silent on this issue either – a press release was issued in June stating opposition the activities being carried out in US libraries and noting

---

[8] Significant Developments in Global Internet Law in 2002: http://www.cov.com/publications/321.pdf and RSF The Internet Under Surveillance: http://www.rsf.org/IMG/pdf/doc-2236.pdf

[9] IFLA/FAIFE Press Release: Libraries are for democracy not surveillance: http://www.ifla.org/V/press/faife050603pr.htm

[10] Leigh Esterbrook, Public Libraries and Civil Liberties: http://www.lis.uiuc.edu/gslis/research/civil_liberties.html and Nancy Kranich, The Impact of the USA PATRIOT Act on Free Expression: http://www.fepproject.org/commentaries/patriotact.html

[11] USA PATRIOT Act resolutions of State Library Associations: http://www.ala.org/Template.cfm?Section=State_IFC_in_Action&Template=/ContentManagement/ContentDisplay.cfm&ContentID=29738

that a library's purpose is undermined by the threat of surveillance[12].

Towards a regulated Internet

Alongside the anti-terror acts and actions specifically relating to tackling the war on terror, it is possible to see another trend emerging on the Internet that could have consequences for the way libraries and their users access information. At a pre-conference for the World Summit on the Information Society in Bucharest last November, the General Secretary of the International Telecommunications Union, one of the organisers of the summit, gave a keynote speech[13]. In it, he called for a new framework of global governance for the Internet, a new system of regulation applicable to all. In nearly all sectors of the Internet, we are seeing increasing moves towards regulation by governments and regional administrative bodies. From a position a few years ago when regulation of the information superhighway was considered unwise and almost impossible, we are today in a position where a variety of initiatives look set to change the way the Internet operates.

For example, there is the eEurope 2005 Action Plan which, among other things, is proposing a European Network and Information Security Information Agency that will help establish a secure communications environment for the exchange of classified data amongst governments. The EU is also taking data retention to a regional level through the Electronic Communications Data Protection Directive. Retention times being discussed vary from between 12 months to 5 years, and this directive is being used as a template in other parts of the world such as Australia. Cybercrime is now being tackled through governmental co-operation and harmonization of laws as a result of the EU Convention on Cybercrime, and the US government has increased penalties for Cybercrime offences in the Homeland Security Act of 2002. This act also allows for ISPs to voluntarily disclose information on users it deems likely to cause a risk of death or serious injury, putting large amounts of power into the hands of the private sector. There is also the Council of Europe's Treaty on Hate Speech to consider, which criminalizes Internet speech relating to unlawful discrimination. International co-operation between governments is less comprehensive in this case due to the inability of the United States to reconcile the treaty with the First Amendment, but co-operation between states is at the top of the EU's agenda, and the G8 and APEC (Asia Pacific Economic Co-operation) countries have also signalled their intent to co-operate in cyberspace[14].

Regulation and Libraries

Why does this matter for libraries? How will it change the way we provide information services? It is fair to say that libraries should not shelter lawbreakers and to this extent the new regulations covering Cybercrime should have little effect on the way we provide services. However, the change in the information-seeking environment caused by more regulation of the Internet will mean libraries have to keep up to date on exactly how our users will be affected. More surveillance of activities, for example, can act as a brake on the user's freedom of expression and perhaps prevent the seeking of certain types of information for fear of being flagged as a potential lawbreaker. Libraries have always been bound by national laws, and it is not in our interest to break these, but it is also important that users are aware that, for example, Internet use records are being retained for periods of time. The recent

[12] See 9 above.
[13] Yoshio Utsumi: http://www.itu.int/wsis/docs/rc/bucharest/speech_utsumi.doc
[14] Covington and Burling – Significant Development in Global Internet Law in 2002: http://www.cov.com/publications/321.pdf

IFLA/FAIFE World Report 2003 shows that a clear majority of library associations see the keeping of user records as having an effect on users' freedom of expression[15]. It also shows that at present, few of the contributing countries are retaining this information. Future world reports will monitor this situation for changes. Using the Internet to seek information remains similar in many respects to using printed sources, and it has not been a policy of the library profession to turn over to law enforcement agencies records of which books users are checking out. We have to maintain a similar approach with regards to the Internet.

With regards to issues of national security and the removal of information considered sensitive from libraries' collections and the Internet, these are more difficult issues to take a stance on. Libraries believe in freedom of access to information but yet cannot be seen to advocate access to all types of information, all of the time. We cannot, on the other hand, sit by idly while information that has been in the public domain previously is 'disappeared' along with mechanisms and processes for accessing it. It is our duty to ensure that those who need information are able to retrieve it, regardless of the medium of delivery. How to balance this duty with the needs of governments in, as they see it, a time of war, will be an obstacle to overcome over the next few years.

Future developments: The potential for a "Less free, less choice" Internet

This is all the more true when we move on from the current trends towards regulation to anticipating the next moves, five or ten years down the line, relating to ensuring that governments can regulate use of the Internet. The war on terrorism has bred a feeling within the United States administration that larger and more elaborate methods should be in place to prevent future terrorist attacks before they occur. In turn, business opportunities are being offered to the companies that can make this happen, and consequently similar technology is being made available to countries with poor human rights records on the grounds that terrorism must be tackled effectively.

Indeed, private companies are already on board governments' efforts to regulate the Internet. Sun, Nortel and Cisco have helped create the architecture of surveillance that stifles freedom of access to information and freedom of expression in China[16]. Over the last twelve months, however, the demand for more invasive technologies caused by the PATRIOT Act has caused more and more companies to enter the field of surveillance software provision[17]. New security requirements in the act have created demands for software compatible with government systems and firms in the private sector have rushed to buy these new products. Financial institutions and universities have to check user and foreign student records against government terrorist lists, which creates a flow of information between the private, academic and government sectors.

This is important to recognise in light of the much-criticised Total Information Awareness project that was being developed by the US Defence Advanced Research Project Agency

---

[15] *IFLA/FAIFE World Report 2003*
[16] China's Golden Shield: http://www.ichrdd.ca/english/commdoc/publications/globalization/goldenShieldEng.html and State Control of the Internet in China (Amnesty): http://web.amnesty.org/library/Index/engASA170072002?OpenDocument?OpenDocument
[17] The PATRIOT Software Bonanza: http://archive.salon.com/tech/feature/2003/04/23/patriot_software/index.html and Spying for Fun and Profit: http://www.alternet.org/story.html?StoryID=16009

(DARPA). This project was aiming to mine a giant database of citizens' personal details such as Internet use records, telephone records, credit card and banking transactions and travel documents so as to help track and prevent potential terrorist activities[18]. Such a project would break down the walls between commercial and government databases and, in light of the PATRIOT Act, it is almost inconceivable that library use records would not be included in the database. TIA came under so much criticism from all sides of the political spectrum it was renamed 'Terrorist Information Awareness' so as to placate critics who were outraged at its Orwellian machinations. Despite some serious opposition to funding the project in Congress, its very development is an indication of the current administration's thinking, and we should not be surprised to see it return in some form in the future[19].

The US Leads the Way?

This situation is likely to continue when we consider what is on the agenda in the United States. If it is considered that the first anti-terror package in the US begot the raft of measures we have outlined above in many other countries, it is instructive to monitor the situation in the States to see what else might follow. Currently being considered is Attorney General John Ashcroft's Domestic Security Enhancement Act of 2003, which is also known as "PATRIOT II". Documents obtained by the Centre for Public Integrity show that this proposal goes further still than its predecessor. Wire-tapping would be made easier, credit and library records would be accessible without a search warrant and surveillance and detention powers would be greatly expanded[20].

Another trend to look out for in the future is not immediately related to terrorism, but it will exacerbate any effects future anti-terror moves will have. Closely connected to the increasing involvement of private sector firms in providing technologies to governments is the consolidation of Internet infrastructure by the private sector. It is this sort of behaviour that led to the Yellow Times anti-war website being closed down – the plug was pulled by a private hosting company rather than the government. This type of self-censorship – caused by an unwillingness to be associated with views opposing a government's foreign policy – may become more widespread as the war on terror goes on. With liability of ISPs for information posted on sites by third parties still a confused issue, self-censorship could continue for some time as ISPs seek to avoid costly legal battles over speech. Sides are definitely drawn up in this conflict and in these conditions it can be difficult for dissenting voices to be heard.

A further example of this concerns a yet unresolved situation relating to the publishing of academic work in the United States by academics from countries on a list of US enemies – from the axis of evil countries for example. It appears that the US Treasury Office of Foreign Asset Control may have instituted a policy whereby American scholarly journals are unable to provide 'services' such as editing to papers originating from certain nations (i.e. countries affected by US sanctions). It would appear, therefore, that unless papers are accepted without revisions they would be unable to be published in American journals[21]. There are also signs that federal funds for research in the US are now coming with more strings attached in an

[18] Pentagon Plans a Computer System that would Peek at Personal Data of Americans: http://query.nytimes.com/search/article-page.html?res=9F05EFD61431F93AA35752C1A9649C8B63
[19] White House Protests cuts on Terrorist Data: http://www.washingtontimes.com/national/20030715-114942-2412r.htm
[20] Nancy Kranich, The Impact of the USA PATRIOT Act on Free Expression: http://www.fepproject.org/commentaries/patriotact.html
[21] Email from Mark Vasquez, Conference Publications Product Manager, IEEE, 30/06/03

effort to keep sensitive information out of the hands of terrorists[22]. Such strings include reviewing papers on certain topics with the option of blocking publication or refusing to fund projects unless foreign students working on them are approved by the government. These moves in turn are creating a climate where researchers are asking themselves whether they should self-censor in order to protect information. Research libraries and librarians are inevitably caught up in this situation and will have to strike an appropriate balance between protecting national security and making sure appropriate information reaches users.

Conclusion

The picture I have just painted is almost unremittingly dark. However, this is only an outline of some of the legislation and actions relevant for an understanding of current and future trends regarding Internet regulation in the wake of the war against terror. If one takes a step back from this and looks at the development of the Internet in the twelve months since the Glasgow conference we can see some encouraging signs too. More and more people have come online in the last year – there are now some 606 million users worldwide[23]. A new phenomenon has seen users flock to start blogging – posting heavily linked online diaries or regularly updated WebPages that are easy to use and post online. Bloggers have been responsible for getting information out of Baghdad during the recent bombing, and have been a success, especially for women to express their opinions, in countries such as Iran. It is possible that a greater explosion of blogging over the next twelve months could be responsible for the Internet finally delivering on the oft-quoted promises of greater democracy for all, especially when one sees the use being made of the medium by presidential candidates such as Howard Dean in the United States. On top of this, the Internet has been seen to have a positive effect in traditionally restrictive places like China where users complained about the blocking of search engine Google to the point of it being reinstated by government censors[24].

Success stories like this can increase demand for the Internet and enable millions more users to gain quick access to the information they need. The amount of people around the world with access is still unequal however, and the recent IFLA/FAIFE World report shows that the extent of libraries offering Internet access is very much affected by the Digital Divide. If the cumulative affects of governments' attitudes to the war on terror is increased regulation of Internet access then the gap between the information have and the information have nots may be bridged even more slowly. The current world situation where an increased level of online surveillance and data retention is becoming accepted is not good for the free flow of information on the Internet, and is seriously damaging for the freedom of expression of users, especially in traditionally closed regimes. The new danger of the situation though, is that those users who have never before had to worry about what they are looking at online, who can surf for the information they need in libraries without fear of somebody looking over their shoulder – these users may now have to seek information in a tainted environment where accessing information on terrorism makes one a potential terrorist and where ones' information searching activities are potentially called into question as never before.

How can we react when our users' intellectual freedom is under threat? Libraries must remain

[22] Researchers worry fear of terrorism could muzzle science: http://www.freedomforum.org/templates/document.asp?documentID=17428
[23] Nua.com: http://www.nua.com/surveys/how_many_online/index.html
[24] China Ends Blocking of Internet Search Engine Google: http://www.siliconvalley.com/mld/siliconvalley/news/editorial/4059152.htm and http://yaleglobal.yale.edu/display.article?id=2133

within the law, but we can take some action. Closely monitoring the situation with regards to Internet legislation will flag areas of potential conflict for libraries and their users. We cannot afford to react late to policies that threaten user privacy and the free flow of information – we need to be fully prepared from the outset to take a position that protects freedom of access to information in libraries. On top of this, we need to bring our users onside, and make them aware of the environment their information seeking activities are taking place in. We are able to take a stronger stand if the community stands with us. If we can do this, then co-ordinated lobbying and advocating the cause of the library community when new legislation is proposed is a start down the path towards ensuring online information access remains equal and unhampered, wherever our libraries are. There is too much at stake to remain quiet on these issues.