Big Brother versus anonymity on the internet.[1]

Jelke Nijboer (j.nijboer@hva.nl)
Teamleader of the Section Information Services and –Management
of the Institute for Media and Information Management, Amsterdam

Abstract

To communicate anonymously is a basic constitutional right. An anonymous telephone conversation or participating anonymously in a newsgroup or even sending an anonymous letter to the editor of a newspaper is allowed in a democratic society, even if the points of view expressed by someone are very controversial. It is an integral part of the freedom of speech. However anonymity on the internet is increasingly not self-evident. The debate has been going on for awhile. Even journalists plea for regulation or legislation of the internet. In the opinion of some, a digital passport could prevent misconduct.

Anonymity is one of the characteristics of the internet. Is misconduct overemphasized or is improper internet usage on the rise in the last couple of years? Many governments and lobby groups are of this opinion and want more control over the internet to prevent misconduct and misuse. Pleas for digital passports and other forms of (self)regulation and legislation are increasing or in some countries legislation is already being put into place to limit the freedom of speech via the internet.

It looks as if anonymity on the internet will soon be something of the past. Big Brother is watching us as soon as we access our computer. The controversial Patriot Act in the United States is an example of the far reaching powers of authorities to limit our freedom of speech. It doesn't only threaten our freedom of movement on the internet, it also effects the business of internet service providers (ISP's), internet cafes and libraries.

These implications for internet users and institutions, like libraries, will be discussed in this paper. It will be clarified with some cases in the United States and elsewhere.

[1] Paper presented at the 12th BOBCATSSS symposium in Riga (Latvia), Jan. 26-28, 2004. Accepted November 2003.
Revised Febr.-March 2004.

Introduction

To communicate anonymously is a basic constitutional right. Having a discussion at a bus stop or in a bar with people you don't know at all, participating in an internet forum is in a democratic society completely normal, even if the points of view expressed by someone are deplorable. It is an integrated part of our freedom of expression. However anonymity on the internet is increasingly not self-evident. The debate has been going on for a while (see e.g. the online archive of the Electronic Privacy Information Center, http://www.epic.org). Even journalists plea for regulation or legislation of the internet (Blankesteyn 2000). A digital passport could prevent digital misconduct. To save us from the bombardment of "the bad and the ugly" information of the internet?
Anonymity is one of the main characteristics of the internet and misconduct is overemphasized. The majority of internet users behaves according to the accepted "internet netiquette". Communication between internet users is mostly very civilized and satisfactory for most users. There is no need for (more) regulation or legislation of the internet. That was my opinion a couple of years ago (Nijboer 2000), but is this opinion in the wake of the 9/11 attacks and the increase of internet incidents still tenable?

Incidents

During the last couple of years there have been more scandals with paedophile rings, misuse of chat rooms, spam, internet bullying of children and adults with sometimes disastrous results (e.g. suicides). These worrying occurrences and the effect of 9/11 on the internet community are used as arguments to limit the internet freedom by law or by forms of regulation.
The exponential growth of violations on the internet is shown in the table below (incidents reported to CERT® Coordination Center of the Software Engineering Institute of Carnegie Mellon University)

Year	Number of incidents (including hackers and viruses)
2000	21,756
2001	52,658
2002	82,094
2003	137,529

Total number of incidents reported since 1988: 319,992
Source: http://www.cert.org/stats/

The outcome of all these incidents is: filter software installed in schools and libraries, surveillance software installed (by law) at Internet Service Providers (ISP's), pleas for digital passports and other forms of (self)regulation and legislation put in place in many countries to limit the freedom of expression via internet. Microsoft closed down public chat rooms in the autumn of 2003. Spam, pedophiles misusing the chat rooms et cetera were important reasons for Microsoft's decision (critics say it is mostly for commercial reasons that Microsoft closed these chat rooms: it isn't profitable and the scandals involving children had a negative effect on Microsoft's image (Van Jole 2003)). Another nuisance is the exponential growth of spam e-mails. It is not easy to block spam, because spammers adopt new techniques that can bypass

current approaches used to block and minimize spam (Spam 2003). The Gartner Group estimates that today more than 50% of the e-mails will be spam (Waves 2002). Bill Gates announced at the World Economic Forum in January 2004 that Microsoft wants to get rid of spam within two years (Weber 2004). Instead of the technological route there is also the legal route. E.g. a Danish court fined a local telecommunications firm $67,990 on the 21st of Jan. 2004 for sending up to 1,500 unsolicited e-mails (Danish 2004).
My beliefe in a censor free internet and functioning netiquette has been shaken during the last couple of years, but I still believe strongly in the anarchy and freedom of the internet.

Threats to freedom of expression

Every new incident, especially when children are involved, encourages critics to plea for limitations of the freedom of the internet. Internet opened new ways for paedophiles to reach and abuse children. Police find many times tens of thousands of downloaded age-inapproperiate or illegal material in the possession of suspects. The recent report of the NCH about child abuse, child pornography and the internet is alarming and claims that there is a strong link between internet use and child abuse (Carr 2004). A civil society will not simply sit back and accept these developments. It looks as if privacy and anonymity on the internet will be something of the past. Not only totalitarian countries are filtering or blocking information. Modern western democracies are putting legislation in place which limits this freedom.
You have to realize that anonymity guarantees the full potential of access free information and communication without government - or ISP privacy interference. Anonymity enables users to protect their own privacy and avoid spam and unwanted information. With anonymity a free exchange of critical ideas or unpopular opinons can be stated without reprisals from government or employer. Anonymity protects also whistleblowers of social abuse or fraud (Asscher 2003). The Electronic Frontier Foundation (EFF) was created in the USA to defend the rights to think, speak, and share ideas, thoughts, and needs using new technologies, such as the internet. EFF has taken on several legal cases to protect the identity of employee-whistleblowers who are posting anonymously on the internet for fear of losing their jobs (General).

The most important thing about the internet is the exchange of information between people wherever they are. Everyday billions of e-mail messages are produced, there are 50.000 discussion groups in the world and the internet community produces appr. 550 million internet searches a day (Grossman 2003). Censorship isn't easy to achieve on the internet. Many governments failed in the past, but government actions to censor the internet are becoming more effective and ICT developments, which boosted the freedom of internet in the recent past, makes surveillance easier and easier. Filtering and blocking information increases day by day and threatens the freedom of expression. Often the public is not even aware that governments put untenable demands on internet journalists, ISP's, libraries et cetera. E.g. in Italy every internet journalist has to register to publish on the internet. In Spain ISP's are responsible for the material put on the web by their internet subscribers and they have to screen the content before publishing it (Hardy 2003). This kind of (self)regulation means that ISP's will regulate their subscribers.

In the USA a legal battle was going on between public libraries and the Bush Administration over the Children's Internet Protecting Act (CIPA). The legislation requires schools and libraries receiving federal funds for internet access to install filtering software to block access

to materials that are obscene, child pornography, or harmful to minors (Children's). So if a library doesn't install the software it could well mean a cut in federal funding. In March 2001 the ALA, EFF, ACLU and other organizations filed a lawsuit challenging CIPA (General). The District Court of Philadelphia ruled in May 2002 that installing filters was censoring the freedom of expression, because it would restrict substantial amounts of protected speech "whose suppression serves no legitimate government interest" (Children's). The federal government appealed to the Supreme Court of the US (United 2003). In June 2003 the Supreme Court reversed the lower court's ruling (http://www.supremecourtus.gov/opinions/02pdf/02-361.pdf). It does not prohibit the government from forcing public libraries – as a condition of receiving federal funding – to use software filters to control what library users access online via library computers. According to Hilden (2003) it appears to be a major defeat for free speech, "but closer inspection reveals that in fact, the decision is relatively limited.".In the course of litigation the government promised that the libraries could, and would, remove the filters if users asked to do so. It also promised that users would not have to explain why they were making the request. Hilden (2003) says that this concession may actually promote free speech – at least compared with to the situation in which filters were in place, and library users might not have known they could ask for their removal. Because of this ruling some libraries have renounced federal funding. Others have begun shopping for filtering software. Most are waiting for more guidance (Quint 2003).

9/11 and Internet

Another threat to the safeguarding of freedom of expression are the effects of the aftermath of the 9/11 attacks of al-Qaeda. The US House of Representatives passed the USA Patriot Act (Provide Appropriate Tools Required to Intercept and Obstruct Terrorism) on 24 Oct. 2001. The Patriot Act is a cornerstone of the US antiterrorism policy. The controversial Act is an example of the far reaching powers of authorities to limit our freedom of expression. Monitoring internet data is now legalized. For example all major ISP's have installed surveillance software to monitor e-mail messages and store records of internet activity by people suspected having suspicious foreign contacts. Big Brother is watching us as soon as we access our computer.
The general public is more worried that terrorists are among us and give first priority in catching terrorists. Freedom of expression and other civil liberties are secondary in the eyes of frightened citizens. The American Congress accepted the Patriot Act within two months after 9/11. American citizens were still in shock and it took quite a while when people started to realize the possible negative effects on their privacy. An internal report of the Justice Dept. alleged "dozens of violations of civil rights in the enforcement of the act (Shenon 2003). Not only liberals, like Ronald Dworkin (see his blistering criticism of the Patriot Act in the New York Review of Books), Gloria Steinem, Naomi Klein and Ralph Nader, are worried, also ultra conservatives who realize that their individual freedom could be threatened too. John Ashcroft, the Attorney General, started in August 2003 a campaign in defense of the administration's antiterrorism efforts. He rejects all the criticism and blames e.g. librarians for unfounded hysteria about the Patriot Act (Justitie 2003). His main defense is that critics have distorted what the law does to make it seem more burdensome than it really is (Lichtblau 2003A).

The Patriot Act expands the kind of information the authorities want and they can ask ISP's, libraries and other organizations, without court approval, to hand over internet data, such as records of websites visited. It has a section in the law that allows ISP's to disclose the content

of their customers messages at the request of federal or local authorities if, “in good faith” they think this will prevent death or serious injury. No court involved, a kind of self regulation, in which the ISP’s decide when and what to disclose to the authorities. EFF is very critical about the fact that disclosure will be on the basis of “good faith” rather than “reasonable belief”. The same section allows police to record without any permission any message sent or received by a “protected computer” which is under attack (United 2003). The new law allows a person’s record in libraries, universities and health organizations to be accessed by the FBI. The organizations have to cooperate and are not allowed to inform the involved employee or client. Activists and dissidents are quite worried about the far reaching authority of the FBI (Tromp 2003). It means that library users will not be informed that their internet activities and circulation records can be scrutinized. Some libraries inform the public that they can't guarantee that there isn’t “third-party monitoring" when using library computers. The librarians can’t tell the public or one another when they are confronted with the FBI to gain access to the computers or circulation records (the Patriot Act overrules the law which protects the confidentiality of circulation records!). The librarian who does faces penalties.
So as a library user you have to be careful doing research about al-Qaeda. Even if a library has not installed surveillance software, the library uses an ISP and via their surveillance software the FBI can obtain information about surfing behaviour in the library.
To illustrate what can happen when such laws are executed to protect democracy some examples:

- *Marc Schultz, bookseller in the Chapter 11 store in Atlanta went to a coffee shop before going to work. He was standing in line for a cup of coffee and reading an article “Weapons of Mass Stupidity” in the Weekly Planet of Tampa. Somebody behind him saw what he was reading and called the FBI. Three days later two FBI agents visited the bookstore* (Tromp 2003*).*
- *A bookstore owner purged the files of its customer because he wanted to protect them against the Patriot Act* (Gram 2003*).*
- *Student Andrew O'Connor was interrogated by Albuquerque police and the Secret Service in Febr. 2003. O'Connor was removed from the college library by police after he made negative comments about President Bush in an online chat room. He was ultimately released without being charged. What he said, how the police and Secret Service knew he said it, and the gag order on the college to keep people from talking about his arrest, are all shrouded in silence* (Paretsky, 2003A).

In the meantime the Justice Dept. denies it used its powers to demand records from libraries , bookshops and other institutions in pursuit of terrorists. The denial of Attorney General John Ashcroft raises the question if the FBI has never used its powers to demand records, why does it need the authority at all (Lichtblau 2003B). A mystery is the allegation in the Connecticut Law Tribune that the FBI searched library records at least 546 times in the Patriot Act‘s first year (cit. Paretsky 2003B) and zero times according to the Justice Dept. A spokesperson for the ALA said that ” if the Justice Dept. had been more forthcoming with the public this high level of suspicion wouldn’t have developed” (Lichtblau 2003B).

In the autumn of 2003 the senators Craig (Republican) and Durbin (Democrat) proposed new legislation, the Security and Freedom Ensured Act of 2003 (the SAFE-Act). A less far reaching version of the Patriot Act. Records of libraries and bookshops, medical and genetic records will be protected in a more secure way. Information about internet use, reading and borrowing material in libraries can only be accessed by the authorities if there is evidence that the involved user is a “foreign agent” (Nieuwe, 2003). The bill limits the use of "sneak and peek" search warrants, which allow searches without notifying the target, to situations where

a life is at stake, evidence may be destroyed or there is a flight risk. Several organizations endorsed the SAFE Act in a letter to lawmakers, including the ALA, EFF and the American Booksellers Foundation for Free Expression (Hudson 2003). It is an amazing coalition (from gun owners to librarians) and we have to wait if the proposed SAFE act will make it through the legislative process. The fact that senators Durbin and Craig joined forces was for another senator reason to make the following sarcastic comment: "it could only mean one thing: one of them has not read it" (Hudson 2003).
The Ministry of Justice is not amused about these proposals to soften the Patriot Act. John Ashcroft wants even a tougher law then the existing Patriot Act. Beside a tougher law the Bush Administration is working on the Total Information Awareness Project (TIA). The project is part of the Defense Advanced Research Projects Agency's Information Awareness Office. Admiral John Poindexter (indicted during the Iran-Contra Affair under President Reagan) is responsible for the project. The project calls for the development of "revolutionary technology for ultra-large all-source information repositories", which would contain information from multiple sources to create a "virtual, centralized, grand database." The database would be populated by transaction data contained in current databases such as financial records, medical records, communication records, and travel records as well as new sources of information (Most 2003). Privacy International (an independant non-government organization with the privacy role of advocacy an support in the area of human rights) awarded TIA the 2003 US Big Brother Award for "most invasive proposal". The award was presented at the 13th Annual Conference on Computers, Freedom and Privacy in New York (http://www.cfp2003.org).

9/11 and "the rest of the world"

The United States is not the only democracy which threatens the freedom of expression. Is there not a loss of any sense of proportion of necessary measures taken in the aftermath of 9/11 in many other countries? If a similar thing had happened in a EU country there could have been an even more excessive response towards our constitutional right of freedom of expression. Isn't it often a balancing act between freedom and safety and common sense?

Reporters without Borders published in 2002 a report "The Internet on Probation" (http://www.rsf.org/IMG/pdf/doc-1259.pdf), which showed that for security reasons many governments put the internet under surveillance of the security services. The security threat since 9/11 was used by some totalitarian countries to increase repression, but our Western democracies were also threatening the freedom of expression with 'an arsenal of new security measures'. Secretary-general Ménard stated that the United States, the United Kingdom, France, Germany, Spain, Italy, Denmark, The European Parliament, the Council of Europe have all challenged internet freedom since 9/11 (Internet 2002).
In September 2003 a report "Silenced: censorship and control internet" (http://www.privacyinternational.org/survey/censorship/Silenced.pdf) was published. The study has found that censorship of the internet is commonplace in the world. In many countries, there was an increase in efforts to either close down or inhibit the internet since 9/11. The terrorist attacks "have given numerous governments the opportunity to proclaim restrictive policies that their citizens had previously opposed. There has been an acceleration of legal authority for additional snooping of all kinds, particularly involving the internet, from increased email monitoring to the retention of Web logs and communication data. Simultaneously, governments have become more secretive about their own activities, reducing information

that was previously available and refusing to adhere to policies on freedom of information" (p.7).
The anarchy, the total freedom of expression of the internet is disappearing rapidly. Not only governments will threaten the internet freedom. There is a massive effort by corporations to transform the internet arena, where anyone can anonymously participate, to a sign-in affair where "digital certificates" identify who you are. Levy (2003) recently showed us the following situation: an information infrastructure that encourages censorship, surveillance and creative suppression. Where anonymity is outlawed and every Euro spent is accounted for.

Ideas and competition can be suppressed from the start and no one can publish anything without the official licence of Big Brother. It could well be a situation in which ISP's are the self regulators: the Bureau of Censorship deciding which information will be distributed and which information will be taken down (e.g. copyright infringement). You can be sure that ISP's take the pre-emptive approach. Reducing the risk of liability arising from failure to act on direct complaints.
This kind of "trusted computing" will also mean digital rights management to pictures, documents and sound. No one can access or post anything without permission if one uses the secure system. The moguls in the entertainment and publishing industry will welcome this very much. Governments will be able to tax e-commerce and non democratic governments keep track of their surfing citizens at home, in libraries and internet cafes. The expenses of internet access in libraries probably will increase substantially. One of the predictions is that corporations will rival governments in censoring the internet in the next decade (Silenced 2003).

Conclusions

Governments, corporations and obedient citizens have many reasons (copyright infringement, anti-terrorist laws, child protection, hackers, e-fraud, spammers et cetera) to control the internet. However public awareness must be raised to make sure that our fundamental right of freedom of expression and free and unlimited access to knowledge in the internet arena will be guaranteed. We must be very alert that governments and especially our MP's will promote this fundamental right and make sure that legislation against terrorist activities, child pornographers, spammers, copyright infringement et cetera doesn't threaten this fundamental right in such a way that it will have the opposite effect to the one intended. The Patriot Act in the USA is an example of this opposite effect.
The individuals and political or criminal groups who have real intent to harm society will obtain technology which by-pass the surveillance software and other ICT obstacles. So why introduce this kind of new legislation? Probably a main reason is to give citizens a false sense of protection against the evil, however society must not fight terrorism in a way that destroys democracy. We don't want to accept terrorists methods and maybe walk into a trap that will have given them a major victory.
Librarians have to be activists in protecting our democracy, if they take the "UNESCO Public Library Manifesto" seriously: "Freedom, prosperity and the development of society and of individuals are fundamental values. They will only be attained through the ability of well informed citizens to exercise their democratic rights and to play an active role in society. Constructive participation and the development of democracy depend on satisfactory education as well as on free and unlimited access to knowledge, thought, culture and information" (UNESCO 1994).
The mere suspicion that internet users (in libraries and elsewhere) are being watched can intimidate them in expressing their views. Before you know it many of us will only express

and read what is "politically correct". The American and West European style democracies will be in deep trouble and it will remind our new EU members of a recent past they most likely don't want to go back to.
Let's not start regulating the freedom of expression on the internet. Regulating internet usage, digital passports and other forms of censorship will be undesirable and obstacles in this process. Libraries must be in the forefront to protect and defend free and unobtrusive access to internet and appeal to the Unesco Public Library Manifesto of 1994 in order to prevent a Georg Orwell's world of 1984 becoming our reality.

© photograph: Jelke Nijboer, 2003.

Literature

- Asscher, Lodewijk and Anton Ekker (2003). *Anonimiteitswet is hard nodig*. De Volkskrant, 26 Aug.
- Blankesteijn, Herbert (2000).*'Anonimiteit op internet keert zich tegen de gebruiker'*. De Volkskrant, 6 Dec.
- Carr, John (2004). *Child abuse, child pornography and the internet*. London, NCH.
- CERT/CC Statistics 1988-2003. http://www.cert.org/stats/ (last updated Jan.22, 2003).
- *Children's Internet Protection Act (CIPA).* Electronic Privacy Information Center. http://www.epic.org.free (visited Dec. 21 2003).
- *Danish court fines Telecom company for sending spam* (2004). http://www.gigalaw.com.
- Dworkin, Ronald (2003). *Terror & the attack on civil liberties*. The New York Review of Books, vol. 50, no. 17 (Nov. 6).
- Gram, David (2003). *'Patriot Act' prompts bookseller to purge files*. The Associated Press, Febr. 18.
- Grossman, Lev (2003). *Search and destroy.* Time. Dec. 22, p.46.
- Hardy, Christiane and Karin Spaink (2003). *Nieuwe censuur bedreigt internet*. De Volkskrant, 13 June
- Hilden, Julie (2003). *A recent Supreme Court decision allowing the government to force public libraries to filter users' internet access is less significant than it might at first appear.* July 1. http://writ.news.findlaw.com/hilden/20030701.html
- Hudson, Audrey (2003). *Senators join forces to roll back parts of Patriot Act*. The Washington Times, 16 Oct.
- *Internet on probation; 11 September 2001-11 September 2002.* Reporters without Borders. http:/www.rsf.org/IMG/pdf/doc-1259.pdf
- *Internet on probation, The : anti-terrorism drive threatens Internet freedom worldwide.* Reporters without Borders 5 Sept. 2002. http://www.rsf.fr.
- *Justitie van VS misbruikt de anti-terreurwet* (2003). NRC Handelsblad, 29 Sept., p.5.
- Levy, Steven (2003). *A net of control.* Newsweek. Special issues 2004, Dec. 2003-Febr. 2004, p.64-66.
- Lichtblau, Eric (2003A). *Ashcroft going on road to lobby for Patriot Act*. International Herald Tribune, 20 Aug., p.3.
- Lichtblau, Eric (2003B). *Government says it has yet to use new power to check library records.* The New York Times, !8 Sept.
- *Most invasive proposal* (2003). http://www.privacyinternational.org/bigbrother/us2003/
- *Nieuw Anti-Patriot Act* (2003). Informatie Professional, vol. 7, no.11, p.11.
- Nijboer, Jelke (2000). *'Anonimiteit op internet'*. Online posting 8 Dec. www.teacherslab.hva.nl
- Paretsky, Sara (2003A). *'For Those Who Wish to Dissent: Speech, Silence and Patriotism'*. Chicago Tribune, 21 Sept.
- Paretsky, Sara (2003B). *The new censorship*. New Statesman, 2 June, p.18-20.
- Quint, Barbara (2003). *Public libraries face net filtering following Supreme Court decision.* June 30. http.//www.infotoday.com/newsbreaks/nb030630-1.shtml
- Shenon, Philip (2003). 'Report on US Antiterrorism Law alleges violations of civil rights.' The New York Times, July 21.
- *Silenced: censorship and control internet* (2003). http://www.privacyinternational.org/survey/censorship/Silenced.pdf.

- *Spam control problems and opportunities*. The Ferris Group, Jan. 2003. http://www.ferris.com/200301/SM.html
- *General information about the Electronic Frontier Foundation.* http://eff.org/about/ (visited Jan. 10 2004).
- Tromp, Jan (2003). *Sinds 11/9 mag FBI in ieders leven snuffelen*. De Volkskrant, 11 Sept.
- *UNESCO Public Library Manifesto 1994.* http://www.ifla.org/VII/s8/unesco/eng.htm
- *United States*. Press release. Reporters without borders, 18 June 2003. http://www.rsf.org.
- Van Jole, Francisco (2003). *Internet verliest zijn ruwe kantjes*. De Volkskrant, 27 Sept.
- *Waves of information disruption due in 2003*. The Gartner Group, 3 Dec. 2002. http://www4.gartner.com/Init.
- Weber, Tim (2004). *Gates forecasts victory over spam*. BBC News 24 Jan. http://www.bbc.co.uk/i/hi/business/3426367.stm.