COVER SHEET

The Impact of Information Security Technologies Upon Society

Mark Carey-Smith
Lauren May

Information Security Institute
Queensland University of Technology

Paper presented to the Social Change in the 21st Century Conference

Centre for Social Change Research
Queensland University of Technology
27th October 2006

The impact of information security technologies upon society

Mark Carey-Smith
Lauren May

Information Security Institute
Queensland University of Technology

Abstract

This paper's aims are concerned with the effects of information security technologies upon society in general and civil society organisations in particular. Information security mechanisms have the potential to act as enablers or disablers for the work of civil society groups. Recent increased emphasis on national security issues by state actors, particularly 'anti-terrorism' initiatives, have resulted in legislative instruments that impinge upon the civil liberties of many citizens and have the potential to restrict the free flow of information vital for civil society actors. The nascent area of cyberactivism, or hactivism, is at risk of being labelled cyberterrorism, with the accompanying change of perception from a legitimate form of electronic civil disobedience to an abhorrent crime. Biometric technology can be an invasive intrusion into citizens' privacy. Internet censorship and surveillance is widespread and increasing. These implementations of information security technology are becoming more widely deployed with profound implications for the type of societies that will result.

Keywords: information security; civil society; cyberactivism; Internet activism

Contact Details:
m.carey-smith@qut.edu.au
l.may@qut.edu.au

Introduction

Information security impacts upon society in positive and negative ways. Nation states such as Australia are increasingly becoming dependent on information infrastructures relied upon by corporate, government and non-government organisations and individuals. In many regards, information security technologies are deployed for the betterment of society and are used to protect important, sensitive information from unwanted disclosure, modification or fabrication. An example is the use of cryptographic software tools that are used to protect sensitive and potentially incriminating information gathered by human rights field workers and investigators.

Information security technologies are also deployed in ways which adversely affect society. Systems of Internet censorship and surveillance use information security technology. The lines between some forms of online activism and cyberterrorism are becoming increasingly blurred. Biometrics, the measure of an individual's physiological or behavioural attributes, can be a violation of one's privacy. Important components of civil society such as environmental, social justice and human rights non-government

organisations (NGOs) are at particular risk. Such NGOs are subject to the same untargeted attacks that every other Internet user faces such as viruses and phishing scams. They are also at risk of targeted attacks because of the work they perform, the manner in which they perform it and the nature of their opponents.

The deployment of increased security measures is frequently accompanied by a justification stressing the need to address threats to national security, especially what is frequently referred to as terrorism. In a climate of fear and loathing it is easier for governments to introduce contentious legislative changes in the name of counter-terrorism. This tactic is not new. In 1946 Herman Goering succinctly described the importance of the propaganda war in convincing the populace they are under threat and that war is necessary and unavoidable. For most of its reign the Nazi regime was operating under what Giorgio Agamben describes as a 'state of exception' which was enacted by Hitler and suspended the civil liberties enshrined in the Weimar Constitution (Agamben, 2005). This suspension of the usual juridicial environment made it easier for the Nazi leaders to wield power as they saw fit, ostensibly to protect the German people (or at least the subset of German people that continued to be recognised as legitimate citizens).

Usually the tension between reductions in civil liberties and the increase in state power is solved by temporarily increasing state power. Once the conflict or crisis is resolved state power is reverted back to its original level (Morgan, 2004). But what of the conflict or crisis that has no end? Has the 'war on drugs', championed by a number of US presidents, been won yet? The parallels with the war currently being waged around the world the 'war on terror', are profound and disturbing. The danger of the obsession by many nation states in maintaining 'security' by fighting the war on terror is that this becomes the most valued measure of a government's performance, insofar as the government defines its own performance criteria. As Agamben states: "A state which has security as its only task and source of legitimacy is a fragile organism; it can always be provoked by terrorism to turn itself terroristic." (Agamben, 2002).

Internet Filtering: Censorship In Action

Internet censorship occurs in different forms. Nation states such as Vietnam, Iran and China deploy national level Internet filtering systems to limit access to Web sites containing material deemed to be unacceptable to the state. Organisations such as businesses and government departments deploy organisational-level Internet filtering systems to stop employees accessing material that would violate acceptable-use policies. PC-based Internet filtering products are increasingly being marketed towards parents as a way of monitoring and safeguarding their children's access to the Internet.

Filtering is the main process involved with Internet censorship. The ways in which filtering is performed are blacklisting, whitelisting and content analysis (Klang, 2005). Blacklists are effectively lists of banned Web sites. Access to a Web site in the blacklist is usually blocked by the filtering software. Whitelists are effectively lists of allowed Web sites. Usually access is limited to only the Web sites in the whitelist and this approach has limited scope. Content analysis does not use lists of Web sites but relies on real-time analysis of content to identify material that is unacceptable and is blocked. Compiling and updating blacklists is a considerable overhead and usually involves abrogating responsibility to another party such as the software producer. While some blacklisting systems allow the user to add to the supplied lists, the majority use a list supplied by the software creator. Commercial Internet filtering companies usually do not allow public scrutiny of the blacklists they compile, which can lead to issues of lack of transparency and public accountability when such products are used without the knowledge or consent of the user population they are designed to protect or control,

depending on one's perspective. The formats of the blacklists are usually encrypted to prevent scrutiny of their content.

Given the overheads of list maintenance and the value of the accuracy and timeliness of the list it is not surprising that companies wish to keep their contents a trade secret. The challenge for companies categorising Web sites is the massive number of Web sites on the Internet and the dynamic nature of Web site addresses, content and growth. While many Internet filtering companies claim to include human checking of their blacklists, it is highly unlikely that this is conducted to any significant extent (Electronic Frontier Foundation & Online Policy Group, 2003).

A number of empirical studies conducted in recent years have found significant errors in underblocking and overblocking performance of Internet filtering products (Edelman, 2001; Electronic Frontier Foundation & Online Policy Group, 2003; Greenfield, Rickwood, & Tran, 2002; Kaiser Family Foundation, 2002; NetAlert Limited, 2006). Underblocking errors occur when Web sites that should be blocked are not. Overblocking errors occur when Web sites that should not be blocked are (Edelman, 2001). One of the dangers of overblocking is that 'legitimate' content is deemed objectionable, such as the categorisation of many pages on Amnesty International's Web site as being of a sexual nature (Haselton, 2000).

Web proxy programmes such as The Circumventor have been specifically designed to bypass Internet censorship controls and are free to use (Haselton, 2004). The Circumventor system works as a number of Web proxy servers. Each Circumventor site provides a Web site with a form in which the Web site address is entered that the user ultimately wishes to view but is unable to due to Internet filtering. Upon submitting the form the Circumventor proxy server retrieves the required Web site and displays it to the user. Any Internet filtering software installed on the user's PC or ISP only sees Web site traffic being sent to and from the Circumventor sites rather than the Web site that is actually being 'viewed' by the user. As Circumventor sites are created by ordinary Internet users who have volunteered to install a Circumventor site on their PC, the addresses of these sites are not initially known to the companies that produce Internet filtering software. Every few days the Circumventor operators send out an email message detailing new Circumventor sites, thus staying ahead of the Internet filtering software companies until they update their blacklists so that their users can update the Internet filtering software.

Government Surveillance

One of the results of the increased emphasis by nation states on security measures has been an increase in government surveillance. In the United States, many were shocked to discover the extent of the "massive and illegal" wiretapping operation carried out by AT&T for the National Security Agency (NSA) (Electronic Frontier Foundation, 2006a). The surveillance operation was authorised by an executive order of President George W. Bush in 2002, without obtaining a warrant or court order that is usually required for such wiretapping activities.

The Electronic Frontier Foundation (EFF) launched a class-action lawsuit against AT&T in January, 2006 alleging AT&T broke communications privacy laws in allowing government agencies access to phone and Internet communications as well as the massive 300 Terabyte "Daytona" database of caller information (Electronic Frontier Foundation, 2006a). One of the more interesting, though not surprising, aspects of this case is the United States government's legal attempts to stop public scrutiny of the issue. On May 15, 2006, the U.S government filed a classified motion to immediately stop the EFF lawsuit proceeding (Electronic Frontier Foundation, 2006c). As the motion

contained classified material the contents could not be publicly disclosed but a redacted, public version disclosed the reasoning behind the motion was “because any judicial inquiry into whether AT&T broke the law could reveal state secrets and harm national security” (Electronic Frontier Foundation, 2006c). In effect, the U.S government was arguing that they were above the law. The motion was dismissed by a federal judge on July 20, 2006 and the case is proceeding (Electronic Frontier Foundation, 2006b).

In a related case, on August 18, 2006 the American Civil Liberties Union (ACLU) was successful in a lawsuit against the NSA alleging that the wiretapping carried out by the organisation breached the First and Fourth Amendments to the US Constitution which protect free speech and privacy (American Civil Liberties Union, 2006a). The federal court called for an immediate end to the warrantless wiretapping programme conducted by the NSA. A number of social justice organisations supported the lawsuit, including the National Association for the Advancement of Colored People, the American-Arab Anti-Discrimination Committee and the Asian American Legal Defense and Education Fund (American Civil Liberties Union, 2006b).

The U.S federal government mounted similar arguments in the ACLU lawsuit as they have in the EFF lawsuit, stating that the President has executive powers which override any law in a time of war. The U.S Attorney General, Alberto Gonzales, was quoted following the court’s decision as saying: ”I believe very strongly that the president does have the authority to authorize this kind of conduct in a time - particularly in a time of war.” (Holahan & Kopecki, 2006). The U.S government will appeal the decision.

In January, 2006 the U.S government asked the search engines Yahoo!, MSN, America Online and Google to supply them with details of users’ searches (Fisher, 2006). Allegedly the government originally wanted three months worth of search data and the Web site addresses to every entry in the search engines’ indexes. Both demands were negotiated down to one week’s worth of search data and one million randomly chosen Web site addresses. It appears that Google was the only company to fight the subpoena by refusing to supply the requested data, which was allegedly wanted to aid the government’s attempts to regulate online pornography. This refusal to cooperate by Google stands in contrast with their willingness to comply with the Chinese government’s requirements for Internet censorship for a search engine to operate in mainland China.

China is a good example of how information security technology can impact upon society in general and civil society organisations in particular. The system of Internet surveillance and censorship in China is the most advanced ever seen (OpenNet Initiative, 2005). China’s Internet censorship and surveillance regime covers a wide variety of content including Web sites, blogs (Web logs), on-line discussion forums, university bulletin board systems and e-mail messages.

Online discussion forums and bulletin boards are very popular in China, and constitute the freest form of media (Reporters Without Borders, 2003). Censorship of content posted to discussion forums is filtered through automated keyword filtering and additional manual checking by forum Webmasters (OpenNet Initiative, 2005). The forum Webmasters are often unpaid volunteers who “try to steer what they consider negative conversations in a positive direction with well-placed comments of their own” (French, 2006). ‘Negative conversations’ include political material, whereas an example of a positive discussion topic is “what celebrities make the best role models” (French, 2006).

The core of the Internet architecture is the Internet backbone. All Internet traffic to or from China is routed through a series of proxy gateways that interconnect China’s networks to the greater Internet backbone. It is at these proxy gateways that the main

component of China's Internet censorship mechanisms are implemented (Walton, 2001). Specific details are difficult to obtain, though empirical testing has revealed consistent filtering and blocking of access to Web sites and email messages which contain material deemed offensive by the Chinese authorities (Diebert & Villeneuve, 2005; OpenNet Initiative, 2005; Zittrain & Edelman, 2003). Topics which are consistently blocked include material relating to the Tiananmen Square massacre, Tibetan independence, Falun Gong, pro-democracy and human rights in China (OpenNet Initiative, 2005).

One of the criticisms of China is not just that it performs Internet censorship but the severe and unjust sentences imposed on some of its citizens as a result of breaching regulations on Internet expression. For example, Huang Qi was detained for three years prior to his sentencing to five years in prison in 2003 (Amnesty International, 2004). His 'crime' was to host a Web site on which 'cyber dissidents' outside China posted articles critical of the Chinese government. Journalist Shi Tao was arrested as a result of Yahoo! providing information to Chinese authorities after he sent an email message detailing a censorship crackdown by the government (Reporters Without Borders, 2004). Mr Tao was sentenced to ten years imprisonment for "divulging state secrets". There are many other similar examples in the literature.

The Chinese regime has been able to implement the system of Internet censorship and surveillance with the help of Western information technology companies such as Cisco Systems, Sun Microsystems and Nortel Networks, who have provided equipment and software (Walton, 2001). Companies including Yahoo!, MSN and Google aid the regime by filtering the results of their search engines hosted inside China. Microsoft implements automated censorship mechanisms in their China-based blog site (Human Rights Watch, 2006).

Such IT companies claim that they have no choice as they are subject to the rules and regulations of the Chinese Authorities (Boot, 2005). The senior vice president of Microsoft, Craig Mundie's cavalier statement of: "The companies that do business here have to deal with the legal environment as it is but I think it is, in my view, widely overstated to think that the Chinese citizen today isn't benefiting from access to the Internet" is indicative (AFX News Limited, 2006).

The "legal environment" referred to by Mr Mundie is not as clear as it may appear. The censorship and surveillance system is a violation of the Chinese peoples' basic human rights enshrined in the United Nations Universal Declaration of Human Rights. Of particular relevance are Articles 12 (protection of privacy), 18 (freedom of thought, conscience and religion) and 20 (freedom of association). Article 19 of the International Covenant on Civil and Political Rights (ICCPR) is particularly relevant, defining freedom of opinion and expression. China is a signatory to the ICCPR. As a signatory, they have "an obligation to refrain, in good faith, from acts that would defeat the object and the purpose of the treaty" (Thompson, 2006; United Nations). Fundamental freedoms such as "freedom of speech, of the press, of assembly, of association, of procession and of demonstration", as well as freedom of religion and the right to privacy are expressly protected in China's constitution ("Constitution of the People's Republic of China," 1982).

The wave of negative publicity surrounding Google's operations in China in the western media, particularly the information technology specific media, frequently mentioned the ethical dilemma that faced Google. Specifically, the central question asked was whether Google was, on balance, aiding the Chinese people by providing a limited access to their services or was simply part of the problem by aiding a regime of censorship and control. Human rights organisations such as Human Rights Watch and Amnesty International were quite strident in their criticism of Google being part of the

problem and adding legitimacy to the system of censorship through their participation (Amnesty International, 2006; Human Rights Watch, 2006).

Numerous Web logs, newspaper articles and Web sites in the information technology area have mentioned how difficult it was for Google's executives to make the decision to operate inside mainland China and by doing so, becoming part of the censorship regime (Baker, 2006; Kirkpatrick, 2006; Maich, 2006; Thompson, 2006). Their justification is summed up by one of the co-founders of Google, Serge Brin:

> "We ultimately made a difficult decision, but we felt that by participating there, and making our services more available, even if not to the 100 percent that we ideally would like, that it will be better for Chinese Web users, because ultimately they would get more information, though not quite all of it." quoted in (Kirkpatrick, 2006).

Amid all the apparent hand-wringing there is no indication that the ethical question of doing business with a totalitarian regime with a significant history of human rights abuses was considered, quite apart from censorship and surveillance practices. Even if Google was not censoring its search results, the fact that it is a very high profile example of the importance of doing business in China lends legitimacy to the regime. It also reinforces the perception that many corporations' overriding responsibility rests with making a profit regardless of the broader implications for society.

Hacktivism and Cyberterrorism

The modern use of the term "hack" as an activity of a technical nature, dates back to the activities of students at the Massachusetts Institute of Technology in the 1960s (Anonymous, 2006). A hack was used to describe a simple, clever, solution to a problem, not necessarily involving computers. The person who created and performed the hack was therefore described as a hacker. In the 1980s the term hacker began to be used to describe a person gaining unauthorised access to a computer system, denoting a criminal activity involving the use of computers. For many computer enthusiasts however, the use of the term "hacking" to describe a criminal act is a misuse of the term and "cracking" should be used instead (Stallman, 2002). This distinction is almost universally ignored, even by authors who are aware of the controversy over the terminology.

Hacktivism is defined by Manion and Goodrum as "the (sometimes) clandestine use of computer hacking to help advance political causes" (Manion & Goodrum, 2000). As it is a combination of the terms 'hacking' and 'activism' it is not surprising that the context in which the term 'hacktivism' is used varies broadly between having positive or negative connotations. One of the fundamental principles of hacktivism is that it should be non-violent in nature (Manion & Goodrum, 2000).

Language has tremendous power. The labelling of hacktivist activities as 'cyberterrorism' blurs the distinction between an act of electronic civil disobedience and a malicious act designed to cause harm. Denning defines cyberterrorism as "politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage" (Denning, 2001). In the current climate of fear and loathing surrounding the imminent threat of terrorism, any linking of activist activities with terrorism can be extremely damaging to the hacktivist cause.

In Australian legislation the distinction between acts which could be described as hacktivism and those that could be described as cyberterrorism is not clear. The Criminal Code Act 1995 defines an action or threat of action as terrorism if it "is made with the intention of advancing a political, religious or ideological cause" and where the

action: "…(f) seriously interferes with, seriously disrupts, or destroys, an electronic system including, but not limited to: (i) an information system; or (ii) a telecommunications system; or (iii) a financial system; or (iv) a system used for the delivery of essential government services; or (v) a system used for, or by, an essential public utility; or (vi) a system used for, or by, a transport system" ("An Act relating to the criminal law", 1995).

The use of the terms "seriously interferes with" and "information system" is sufficiently broad and vague that they could be easily used to describe acts of civil disobedience such as 'electronic sit-ins'. Traditionally the term 'sit-in' described an act of civil disobedience in which one or more people occupied a public space in protest, often with the intention of causing disruption to normal operations of activities carried out in that space. The sit-ins conducted by African-American students in segregated restaurants in the early days of the civil rights movement in the United States are well-known examples of this non-violent form of protest.

Protest actions of a similar intent as sit-ins, conducted via the Internet with Web sites as the target are known as 'electronic sit-ins' or 'virtual sit-ins'. One of the first examples of electronic sit-ins was carried out against various Web sites of the French government in December 1995 (Denning, 2001). The electronic sit-in was conducted to protest against French government policies on nuclear and social issues. It was carried out by the protest organisers encouraging people around the world to simultaneously attempt to access the Web sites of the target government agencies via users' Web browsers.

The goal of the electronic sit-in is to generate so much protest traffic at the target Web site that it is difficult for legitimate traffic to get through. This technique is a type of 'denial of service' attack. When the source of the spurious traffic is distributed amongst many computing hosts the effect is greatly magnified and is known as a distributed denial of service attack or DDoS attack. Software tools to launch coordinated DDoS attacks are readily available on the Internet and easy to use. The first high-profile example of the use of DDoS tools occurred in February 2000 when eBay, Amazon and CNN Web sites were attacked and effectively disabled for a number of hours (Neumann, 2000). The tools used to launch these attacks were designed to cause as much disruption to the target as possible and to evade detection by spoofing (faking) the source of the attack traffic. DDoS attacks are commonplace on the Internet today but are now longer as effective at causing major disruptions to high-profile targets, largely as a result of defence mechanisms enacted since early 2000.

By comparison, software tools designed to conduct electronic sit-ins are usually not designed to cause the same level of disruption as DDoS tools and usually do not attempt to hide the source of the traffic (Denning, 2001). Electronic sit-ins are usually designed to draw attention to the issue behind the protest action rather than simply to cause havoc for havoc's sake. In the eyes of many in the hacktivist community this distinction is an important one. It could also be an important factor in any judicial proceedings brought against people carrying out electronic sit-ins, though this distinction is not reflected in Australian legislation.

Traditionally, the three most important information security principles are confidentiality, integrity and availability. Availability is the principle of making available a resource for legitimate use. When a computer system is the subject of a denial of service attack it is the availability of the resource which is compromised. It could be argued therefore, that an electronic sit-in which hampers or temporarily stops legitimate access to a government Web site could constitute an act of terrorism in the Australian legal context. This has serious implications for restrictions in a fundamental component of a participatory democracy; the right to protest. Even if the law itself is not actually applied

in criminal proceedings there is potential for the chilling effect of the legislation to silence dissent.

Biometrics

Biometrics is an application of information security technology which has enormous potential to adversely impact upon civil liberties, particularly the right to privacy. Examples of biometric measures include fingerprint, iris and retina patterns, and voice, gait and facial recognition. A number of empirical studies have shown serious problems with the accuracy of many biometric applications and their usability in real-world scenarios (Chandra & Calderon, 2005). A great deal of research into biometric systems is underway, with the US government in particular heavily sponsoring research in the application of biometrics for identification purposes.

The distinction between authentication and identification is crucial when examining biometrics from a privacy perspective. Authentication is the process of proving a claimed identity. It is a one-to-one matching process. Identification is attempting to recognise or establish an individual's identity. It is a one-to-many matching process.

A biometric process which is used for authentication purposes is generally less intrusive, in privacy terms, than an identification process. For example, a biometric identifier such as a fingerprint template can be stored on a passport. In such a system, when a person presents their passport for checking they also have their fingerprint scanned. If the live scan matches the fingerprint template stored on the passport there is a high probability that the two biometric measures come from the same person. There may also be a high probability that the passport holder is who they claim to be. This is completely dependent on the security and accuracy of the process of creating the passport, storage of the collected biometric templates and the live scanning of fingerprints.

Facial recognition with biometric technology is often used as an identification process to aid security applications. For example, facial recognition software could be linked with security cameras in a public space. The software compares the images captured by the cameras with a database of the images of criminal suspects. Theoretically, if the software matches a live image with a stored image then it has identified an individual. This process can be conducted without the knowledge or consent of individuals. There are significant challenges in the accuracy of the process due to differences in lighting, camera focal length and facial angle between the stored images and the live captured images. There are also issues with people intentionally disguising themselves to avoid recognition.

Biometric technology is not a security panacea but it is often marketed as such, especially in the area of airport security. Proponents often argue that accurate identification could stop some terrorist attacks but this argument fails to take into account the unknown attacker. If a person is not known to be a terrorist but has legitimate identification then biometrics will not stop an attack. The use of the technology may bring many innocent people under suspicion though. The infamous "No Fly" list maintained by the Transport Safety Authority in the US is a pertinent example of the dangers of errors in such systems. If an error occurs whereby a person who is not on a terrorist watch list has a biometric attribute which is matched by the system to a person on such a list, they could find it extremely difficult to prove their innocence with potentially serious consequences for civil liberties.

Civil Society Organisations and Information Security

The accurate and timely acquisition and dissemination of information is vital to the operations of civil society actors such as human rights, environmental and social justice NGOs and activists. Civil society organisations are a cornerstone of a participatory democracy. Such groups have made extensive and enthusiastic use of information technologies such as the Internet to aid their activities, though it is unclear if their information assets have had accompanying appropriate protection (Carey-Smith & May, 2006). Anecdotal evidence from conversations with an experienced information security consultant who wishes to remain anonymous clearly shows that many civil society NGOs have little idea of the importance of information security

Two of the most important assets of civil society organisations are their information resources and their reputation. The significant damage to these key resources that can accompany a serious information security incident could threaten the ongoing operations of such organisations. Due to the diverse and often dangerous operating conditions under which many civil society organisations operate, particularly their field-workers, they are often in positions of vulnerability.

The vulnerabilities faced may be of an information security nature and of a personal security nature. In an information security sense, civil society organisations that are oppositional to powerful interests such as corporations and state actors or their proxy agents such as militia groups are likely to be the subject of targeted attacks from their adversaries. These attacks may attempt to destroy information resources or they may conduct electronic wiretapping in an attempt to gain important and sensitive information that could be of direct benefit to them and of direct detriment to the NGO's field workers or clients.

Many civil society organisations are under increasing pressures to provide services for their clients. The Australian Council of Social Service Australian Community Sector Survey 2006 found that respondent organisations' increased expenditure outstripped their increased income and that more people in need were turned away during 2004-2005 than in the previous twelve months (171,366 people turned away, 29% more than 2003-2004), largely due to services operating at maximum capacity (Australian Council of Social Service, 2006). Our hypothesis is that the increasing pressures upon many civil society NGOs are contributing to a lack of knowledge of the importance of information security management and therefore a lack of application in securing important information resources. Future research will address the validity of this hypothesis.

Conclusion

Information security is inherently an ethically neutral technology. The manner in which this technology is deployed determines the effects on society. As national security concerns receive more and more priority from a range of state actors the potential effects of information security technology on society become broader. Governments in most societies are increasingly stressing the risks that terrorism presents to society. The danger of this emphasis is that governments effectively 'paint themselves into a corner' whereby they need to be seen to be taking action to counter the terrorist threat that they themselves have helped to promote.

One way of publicly taking action is to introduce measures which are presented as high-technology solutions to security problems, such as the deployment of facial

recognition biometrics to aid airport security. The decrease in civil liberties, as well as the false sense of security that that can result from such deployments needs to be carefully examined to ascertain, on balance, whether society is actually losing the freedoms that governments are meant to be protecting.

References

AFX News Limited. (2006, 23/4/2006). *China censorship impact on Internet freedom overstated - Microsoft executvie*. Retrieved May 28, 2006, from http://www.forbes.com/business/feeds/afx/2006/04/23/afx2689692.html

Agamben, G. (2002). Security and Terror. *Theory and Event, 5*(4).

Agamben, G. (2005). *State of Exception* (K. Attell, Trans.): The University of Chicago Press.

American Civil Liberties Union. (2006a, 17/8/2006). *Federal Court Strikes Down NSA Warrantless Surveillance Program*. Retrieved August 26, 2006, from http://www.aclu.org/safefree/nsaspying/26489prs20060817.html

American Civil Liberties Union. (2006b, 20/4/2006). *Organizations and People Supporting the NSA Lawsuit*. Retrieved August 26, 2006, from http://www.aclu.org/safefree/nsaspying/25192res20060420.html

Amnesty International. (2004, 28/1/2004). *China: Controls Tighten as Internet activism grows - Amnesty International*. Retrieved May 2, 2006, from http://web.amnesty.org/library/index/ENGASA170052004

Amnesty International. (2006). *Business and Human Rights -- Internet Censorship*. Retrieved May 30, 2006, from http://www.amnestyusa.org/business/takeaction.html

Anonymous. (2006, 26/7/2006). *Hacker definition controversy - Wikipedia, the free encyclopedia*. Retrieved August 16, 2006, from http://en.wikipedia.org/wiki/Hacker_definition_controversy

Australian Council of Social Service. (2006). *Australian Community Sector Survey 2006* (Survey): Australian Council of Social Service.

Baker, L. (2006, 23/2/2006). *Breaking Google's Great Firewall of China*. Retrieved August 23, 2006, from http://www.searchenginejournal.com/index.php?p=2853

Boot, M. (2005). *Just Following Orders in China*. Retrieved May 12, 2006

Carey-Smith, M., & May, L. (2006). *Information Security and Civil Society Organisations.* Paper presented at the RNSA Security Technology Conference, Canberra, Australia.

Chandra, A., & Calderon, T. (2005). Challenges and constraints to the diffusion of biometrics in information systems. *Communications of the ACM, 48*(12), 101-106.

Constitution of the People's Republic of China. (1982).

Criminal Code Act 1995(1995).

Denning, D. (2001). Activism, Hacktivism and Cyberterrorism: The Internet As a Tool for Influencing Foreign Policy. In J. Arquilla & D. Ronfeldt (Eds.), *Networks and*

Netwars: The Future of Terror, Crime and Militancy (pp. 239-288): RAND Corporation.

Diebert, R. J., & Villeneuve, N. (2005). Firewalls and Power: An Overview of Global State Censorship of the Internet. In M. Klang & A. Murray (Eds.), *Human Rights in the Digital Age* (pp. 234): Cavendish Publishing.

Edelman, B. (2001). *Expert Report of Benjamin Edelman*. Retrieved May 15, 2006, from http://cyber.law.harvard.edu/people/edelman/pubs/aclu-101501.pdf

Electronic Frontier Foundation, T. (2006a, 16/6/2006). *EFF: Class Action Lawsuit Against AT&T*. Retrieved June 21, 2006, from http://www.eff.org/legal/cases/att/

Electronic Frontier Foundation, T. (2006b, 20/7/2006). *EFF's Spying Case Moves Forward - Judge Denies Government's Motion to Dismiss AT&T Case*. Retrieved August 18, 2006, from http://www.eff.org/news/archives/2006_07.php#004832

Electronic Frontier Foundation, T. (2006c, 15/5/2006). *Government Files Secret Motion to Dismiss AT&T Surveillance Case*. Retrieved August 18, 2006, from http://www.eff.org/news/archives/2006_05.php#004662

Electronic Frontier Foundation, T., & Online Policy Group, T. (2003, 26/6/2003). *Internet Blocking in Public Schools*. Retrieved April 25, 2006, from http://www.eff.org/Censorship/Censorware/net_block_report/

Fisher, D. (2006, Jan 30, 2006). *Google Fights for Your Rights; Search leader refuses to comply with DOJ's demand for data.* Retrieved August 18, 2006, from http://proquest.umi.com/pqdweb?did=978088781&Fmt=7&clientId=14394&RQT=309&VName=PQD

French, H. (2006, 9/5/2006). *As Chinese Students Go Online, Little Sister Is Watching*. Retrieved May 20, 2006, from http://www.nytimes.com/2006/05/09/world/asia/09internet.html?ex=1304827200&en=47cd8aa53c910466&ei=5090&partner=rssuserland&emc=rss

Greenfield, P., Rickwood, P., & Tran, H. C. (2002). *Effectiveness of Internet Filtering Software Products*: Commonwealth Scientific and Industrial Research Organisation (CSIRO).

Haselton, B. (2000, 12/12/2000). *Amnesty Intercepted: Global human rights groups blocked by Web censoring software*. Retrieved May 15, 2006, from http://www.peacefire.org/amnesty-intercepted/

Haselton, B. (2004). *Circumventor Central*. Retrieved August 24, 2006, from http://www.peacefire.org/circumventor/

Holahan, C., & Kopecki, D. (2006, 18/8/2006). *Wiretap Ruling Threatens Telecoms*. Retrieved August 26, 2006, from http://www.businessweek.com/technology/content/aug2006/tc20060818_382622.htm?chan=top+news_top+news+index_businessweek+exclusives

Human Rights Watch. (2006, 1/2/2006). *US.: Put Pressure on Internet Companies to Uphold Freedom of Expression*. Retrieved May 21, 2006, from http://hrw.org/english/docs/2006/02/01/china12592.htm

Kaiser Family Foundation, T. (2002). *See No Evil: How Internet Filters Affest the Search for Online Health Information*.

Kirkpatrick, D. (2006, 25/1/2006). *Google founder defends China portal*. Retrieved August 24, 2006, from http://money.cnn.com/2006/01/25/news/international/davos_fortune/?cnn=yes

Klang, M. (2005). *Controlling Online Information: Censorship & Cultural Protection*. Retrieved April 23, 2006, from http://www.kus.uu.se/pdf/publications/ICT/klang_03_oct.pdf

Maich, S. (2006, 20/2/2006). *Yes, Master*. Retrieved August 17, 2006, from http://www.macleans.ca/topstories/business/article.jsp?content=20060220_121814_121814

Manion, M., & Goodrum, A. (2000). Terrorism or Civil Disobedience: Toward a Hacktivist Ethic. *SIGCAS Comput. Soc., 30*(2), 14-19.

Morgan, P. M. (2004). Information Warfare and Domestic Threats to American Security. In E. O. Morgan (Ed.), *National Security in the Information Age* (pp. 161-189): Frank Cass Publishers.

NetAlert Limited. (2006). *A Study on Server Based Internet Filters: Accuracy, Broadband Performance Degradation and some Effects on the User Experience*.

Neumann, P. G. (2000). Inside Risks: denial-of-service attacks. *Communications of the ACM, 43*(4), 136.

OpenNet Initiative, T. (2005, 14/04/2006). *Internet Filtering in China in 2004-2005: A Country Study*. Retrieved March 24, 2006, from http://www.opennetinitiative.net/studies/china/

Reporters Without Borders. (2003, 12/5/2003). *"Living dangerously on the Net" - Censorship and surveillance of Internet forums*. Retrieved May 26, 2006, from http://www.rsf.org/article.php3?id_article=6793

Reporters Without Borders. (2004, 6/12/2004). *Arrest of poet and journalist Shi Tao*. Retrieved April 20, 2006, from http://www.rsf.org/article.php3?id_article=12026

Stallman, R. (2002). *On Hacking - Richard Stallman*. Retrieved August 16, 2006

Thompson, C. (2006, 23/4/2006). *Google's China Problem (and China's Google Problem)*. Retrieved May 26, 2006, from http://www.nytimes.com/2006/04/23/magazine/23google.html?ex=1303444800&en=972002761056363f&ei=5090

United Nations.*United Nations Treaty Collection - Treaty Reference Guide*. Retrieved May 4, 2006, from http://untreaty.un.org/English/guide.asp

Walton, G. (2001). *China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China*. Retrieved March 21, 2006, from http://www.ichrdd.ca/english/commdoc/publications/globalization/goldenShieldEng.html

Zittrain, J., & Edelman, B. (2003). Internet filtering in China. *Internet Computing, IEEE, 7*(2), 70-77.