To appear: Brown, I. (2008). Internet censorship: be careful what you ask for, *forthcoming*

Internet censorship: be careful what you ask for

Ian Brown
E-mail: ian.brown [at] oii.ox.ac.uk
Oxford Internet Institute
University of Oxford
1 St. Giles'
Oxford OX1 3JS
United Kingdom

Introduction

A growing number of states worldwide are imposing mandatory requirements on Internet Service Providers (ISPs) to prevent their subscribers from accessing overseas content that would be banned under local laws. It is well known that undemocratic states such as China implement online censorship; but a number of democracies with constitutional guarantees of freedom of expression are also imposing digital filters. States have further put pressure on Web publishers to remove content hosted outside their jurisdiction (Anderson, 2006).

States' Internet censorship regimes vary in terms of the types of content blocked and (to a lesser extent) the technologies used. Repressive states block political debate (such as discussion of Tibet or the crushing of the Tiananmen Square protests in China); theocracies impose strict limits on "blasphemous" and "immoral" content, including information on women's rights and gay and lesbian issues (such as in Saudi Arabia and Iran); while many European states have targeted pornography and racist and xenophobic material (Deibert & Villeneuve, 2005). All of these states have used blocking technologies such as IP address-based packet filtering, DNS poisoning, cache filtering and keyword searches (Zittrain & Edelman, 2003a).

This article critically examines the Internet filtering regimes and technologies used in a range of democratic and undemocratic states. It considers the effectiveness of filters, their impact on newer distribution systems such as peer-to-peer networks, and their compatibility with principles of freedom of expression. It concludes by contrasting the very limited effect of filters on determined users outside totalitarian states with their potential to impose mass censorship on mainstream Internet users.

Existing Filtering Regimes

The Internet has allowed many hundreds of millions of citizens around the world to access information from outside their own country's borders much more easily than ever before. While most states control the import of printed materials, and have attempted to control audio and television broadcasts into their territories, the Internet is a new channel through which content from all over the globe can flow.

This has presented a challenge to states that implement extensive controls over the information that their citizens may access. While few are willing to forgo the economic benefits of interconnecting national networks to the global Internet, most have focused on attempting to create a digital analogue to their existing processes for restricting the import of certain types of printed and broadcast material, filtering Internet data as it travels onto local networks. Some states have also attempted to put pressure on overseas firms to block access to their own citizens.

China has the world's most extensive filtering system, caricatured online as the "Great Firewall of China." Nine Internet Access Providers licensed by the government provide international network access to regional Internet Service Providers. Routers

on the national backbone network are configured to drop packets carrying data to and from blocked websites (OpenNet Initiative, 2005a). National gateway routers are also configured to reset connections between web browsers and servers that carry data containing keywords such as "Falun Gong" (Clayton, Murdoch & Watson, 2006). The Chinese government has used threats to block sites such as Google and Microsoft's MSN Spaces to persuade those companies to self-censor search results and blog posts, and to discover the identity of Yahoo! user journalist Shi Tao who was subsequently given a ten-year prison sentence (Claeburn, 2006).

Iran operates a similarly extensive filtering regime, requiring ISPs to block access to over 10 million websites including "immoral" sites and "political sites which rudely make fun of religious and political figures in the country" (Reporters San Frontières, 2006; BBC News, 2003). At least 10 ISPs have been shut down for breaching this requirement (OpenNet Initiative, 2005b). More recently, Iran has reduced the speed of international connections to 128kbps, effectively blocking access to high-bandwidth video streams (Tait, 2006).

Saudi Arabia routes all Web access through a government proxy which blocks access to sites that "violate the tenants of the Islamic religion or societal norms" as directed by a Ministry of the Interior committee (Government of Saudi Arabia Internet Services Unit, 2006). Unlike in China and Iran, users are notified when access to pages are blocked, and may request that a specific page is blocked or unblocked (see figure 1).

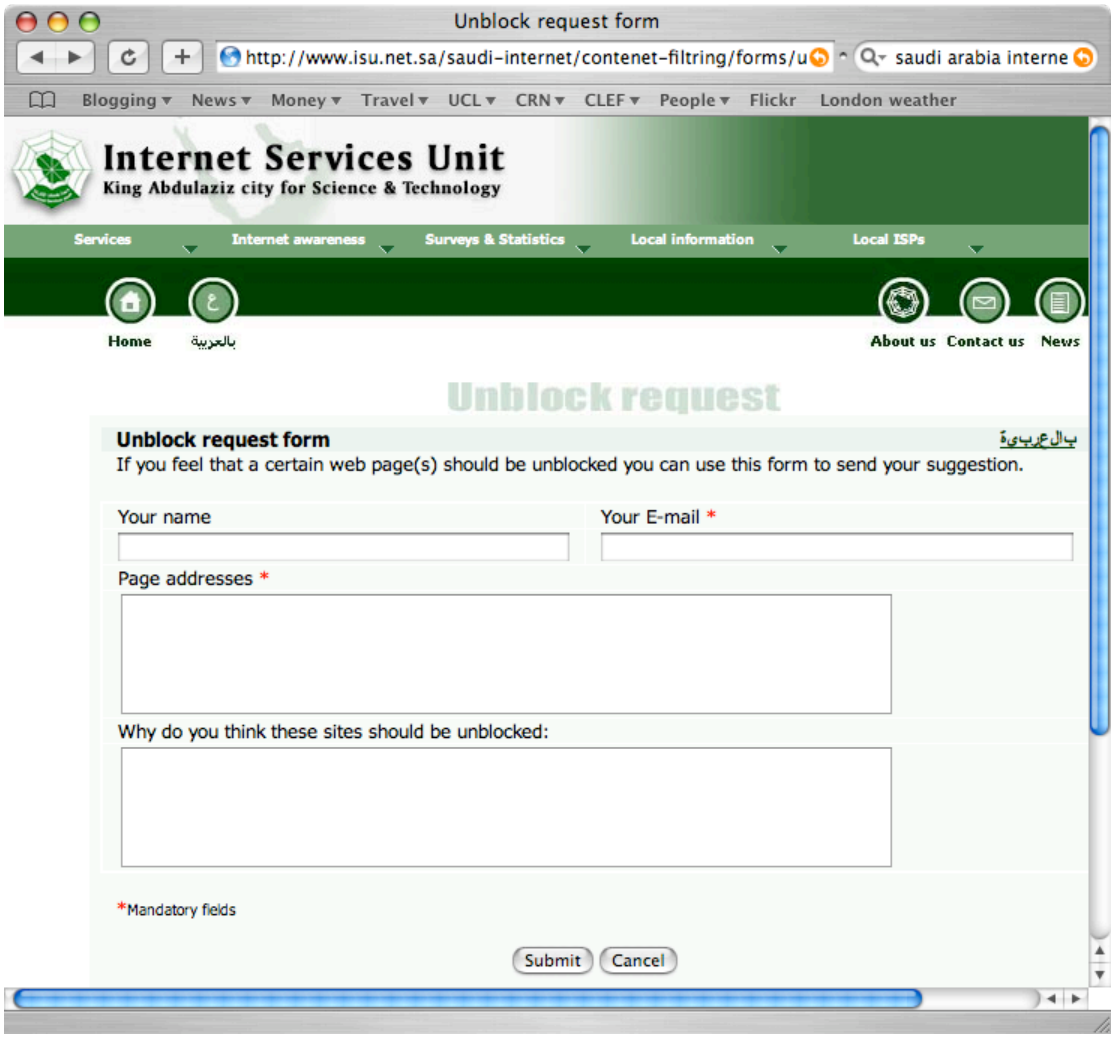

Figure 1: form to request unblocking of web pages by Saudi Arabian government

Other states filter access at ISPs and government-run networks, including Pakistan, Vietnam, Bahrain, Singapore, Syria, Cuba, Tunisia, Kazakhstan, UAE, Myanmar, Uzbekistan and Yemen. As well as pornography, these states target news, human rights and dissident websites (Deibert & Villeneuve, 2005, pp.121-122). Turkey, Taiwan and China require that Internet cafes install filters (Deibert & Villeneuve, 2005, p.116)

It is not however the case that states with stronger constitutional commitments to freedom of expression have rejected Internet filtering. In a piecemeal fashion, courts and governments in France, Germany, Switzerland, Finland, the UK and Italy have ordered ISPs to filter their users' access. While the US Supreme Court has struck down sections of two laws intended to censor websites within the US, federal funding to schools and libraries is conditioned upon the use of filtering software.

Several European states that suffered under the Nazi regime have laws against holocaust denial, while many ban materials promoting racial hatred. These prohibitions have been harmonised in a protocol to the Council of Europe's cybercrime treaty. Signatories must criminalise the making available of "any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as pretext for any of these factors" and "material which denies, minimises, approves of or justifies crimes of genocide or crimes against humanity" (Council of Europe, 2003). However, the application of such restrictions to Internet Service Providers has yet to be tested against European law that generally protects ISPs as "mere conduits" of information and limits EU member states' capacity to regulate ISPs (Hutty, 2007).

France and Germany saw the first restrictions imposed on Nazi and other racist materials hosted overseas. After an action brought by a group of Jewish students, the Superior Court of Paris in 2000 ordered Yahoo Inc. to block the sale of Nazi items to French users. The court found that by providing access to French citizens, Yahoo US was subject to French law; that nothing in the 1st amendment prevented Yahoo from being selective about its auctions; and that blocking access to French citizens was technically difficult but not impossible (Penfold, 2001). Yahoo has attempted to comply, but also obtained a Californian court declaration that ruling had no effect on a US corporation.

The district of Düsseldorf in Germany in 2002 ordered 78 Internet Service Providers in North Rhine-Westphalia to block access to two US-hosted Nazi websites (Privacy International, 2003, p.79). A series of contradictory rulings in lower courts led the higher court in Münster to uphold the order, which is being appealed to the German Supreme Court (Dornseif, 2003).

A Swiss magistrate in 2003 ordered ISPs to block access to three US-hosted websites that featured defamatory content. The Swiss government has also proposed fining ISPs up to 1 million Swiss francs for allowing users to access illegal gambling sites (Rauch, 2003).

Elsewhere in Europe and Canada, several governments are moving to require ISPs to block access to websites hosting child pornography. The Finnish government has encouraged ISPs to implement a "voluntary" system that blocks access to secret list maintained by the police of IP addresses hosting websites suspected to contain child pornography. Unlike similar systems in neighbouring Sweden and Norway, users will not have any choice whether their access is filtered; but the Finnish constitution

would make it difficult for an openly mandatory system to be imposed by the government (Lehdonvirta, 2005). Save the Children, ISPs and the Danish police have cooperated to set up a blacklist of sites which are "voluntarily" blocked once police validate that a site should be on the list and notify this fact to ISPs (Jorgenson, 2006).

In the UK, British Telecom and other large ISPs block customer access to sites that have been identified as containing child pornography by industry self-regulatory body the Internet Watch Foundation (Clayton, 2005). In May 2006 Home Office minister Vernon Croaker MP told the House of Commons that other ISPS would be required to implement similar controls:

> *Recently, it has become technically feasible for ISPs to block home users' access to websites irrespective of where in the world they are hosted. It is clear from the various meetings that Ministers have had with the ISPs, that the industry has the will to implement solutions to block these websites. Currently, all the 3G mobile network operators block their mobile customers from accessing these sites and the biggest ISPs (who between them provide over 90 per cent. of domestic broadband connections) are either currently blocking or have plans to by the end of 2006.*
>
> *We recognise the progress that has been made as a result of the industry's commitment and investment so far. However, 90 per cent. of connections is not enough and we are setting a target that by the end of 2007, all ISPs offering broadband internet connectivity to the UK general public put in place technical measures that prevent their customers accessing websites containing illegal images of child abuse identified by the IWF. For new ISPs or services, we would expect them to put in place measures within nine months of offering the service to the public. If it appears that we are not going to meet our target through co-operation, we will review the options for stopping UK residents accessing websites on the IWF list.* (Hansard, 2006)

The Home Office has stated that filters could be extended to other topics such as the "glorification" of terrorism:

> *At present, the government does not propose to require UK ISPs to block content and our policy is to pursue a self-regulatory approach wherever possible. However, our legislation as drafted provides the flexibility to accommodate a change in Government policy should the need ever arise.* (Hutty, 2006)

A number of large Canadian Internet Service Providers are implementing a similar system to British Telecom's "Cleanfeed". These ISPs are voluntarily blocking access to a list of sites containing child pornography maintained by charity Child Find Manitoba (Geist, 2006). The Italian government has recently introduced a requirement that ISPs block access to child pornography sites within six hours of being told to do so (Reuters, 2007a).

While federal and state US legislatures have been as aggressive as those in other democracies in attempting to censor the Internet, they have largely been restrained by US courts' application of the first amendment to the US constitution. In contrast courts in European states have so far given freedom of expression less weight in this regard; there is little relevant case law from the European Court of Human Rights.

Early attempts by the US Congress to censor US-hosted websites were repeatedly ruled unconstitutional during the 1990s. Sections of both the Communications Decency Act (CDA) and the Child Online Protection Act (COPA) were found by the US Supreme Court to go far beyond what was permitted by the first amendment. Justice John Paul Stevens wrote for the majority in the case of the CDA that:

> *As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship.* (Reno v. ACLU, 1997)

While Congress attempted to draw COPA more narrowly to meet these concerns, the Supreme Court found again in 2004 that the law still presented "a potential for extraordinary harm and a serious chill upon protected speech" (Ashcroft v. ACLU, 2004).

The courts have similarly rejected state laws that have attempted to require Internet Service Providers to block access to certain overseas websites. A 2002 Pennsylvania statute was found to act as an unconstitutional prior restraint on speech (CDT v. Pappert, 2004). A Utah federal court has blocked the enforcement of a 2005 filtering law on first amendment grounds (The King's English v. Shurtleff, 2006).

The only filtering legislation that has so far passed constitutional muster is the Children's Internet Protection Act (CIPA). This requires US schools and libraries that receive federal funding under the "E-Rate" programme to install filtering software. Most use software from companies such as N2H2, which treat blocking lists as commercial secrets protected by intellectual property law (Deibert & Villeneuve, 2005, p.117). Parents and teachers rarely have control of lists of blocked content. Researchers interested in examining lists of filtered sites had to apply for a special exemption under the Digital Millennium Copyright Act before attempting to circumvent list access controls (US Copyright Office, 2003).

Problems with Filtering Technologies

The Internet was designed to allow the efficient transmission of information between networks around the world. Its basic functionality does not include censorship. Internet Service Providers required to block access to specific websites have therefore relied on three crude and ineffective mechanisms: IP address filtering, Domain Name System poisoning and keyword searching (Dornseif, 2003).

The simplest filtering mechanism is for ISPs to block traffic to and from lists of websites specified by their Internet Protocol address (a numerical identifier such as 128.16.64.1). Any packets of data with a destination or source address on this list will be dropped by the routers within ISP networks, especially those that exchange traffic with overseas networks.

With a little effort, users are able to evade such filters by accessing blocked sites using overseas Web proxies, intermediate machines that retrieve Web pages on behalf of users for a number of purposes such as increased efficiency and privacy protection. Even countries such as China that have made a concerted effort to block user access to such proxies find it difficult to locate and filter every single proxy machine. Anti-censorship activists have also developed proxies that individual users can run on their home and office PCs anywhere in the world, making it extremely difficult for governments to block access to every last proxy (Feamster et al., 2002).

While determined users are therefore able to work around filters, other users find their access severely curtailed by IP address filtering. Because Web servers typically host many (sometimes many thousands) of individual sites, a block on just one of those sites will mean none of the other sites hosted on that server will be accessible. When in 2003 the Indian government ordered ISPs to block access to a specific Yahoo! Group, many simply blocked access to the entire domain, cutting access to around 12,000 groups (Deibert and Villeneuve, 2005). Pennsylvania's Internet

filtering law was struck down in 2004 partially because of such overblocking. The blocking of 400 sites had prevented access to over 1.1 million other sites, whilst being easy circumvented. The Court found no evidence that the Act "has reduced child exploitation or abuse" (CDT v. Pappert, 2004).

Brazilian ISPs have recently been ordered by a Sao Paulo court to block access to YouTube until the company removes a video clip apparently showing two celebrities having sex on a Spanish beach (Reuters, 2007b). This will prevent many Brazilians from accessing over 6 million other videos hosted by the site (Gomes, 2006). India is considering a similar move over a YouTube-hosted video showing a parody of Mahatma Ghandi pole-dancing (see figure 2; Dhawan, 2007).

Figure 2: Gautham Prasad's parody of Mahatma Gandhi performing a pole dance

A second common mechanism used to obstruct access to websites introduces deliberate errors into the Internet's directory service, the Domain Name System (DNS). DNS servers translate human-readable domain names such as www.ucl.ac.uk into the numerical IP address equivalent (in this case, 144.82.108.183), allowing web browser software to connect directly to web servers. Internet Service Providers can remove or change the addresses for blocked sites on their own DNS servers, and block user attempts to connect to DNS servers elsewhere on the Internet (Zittrain & Edelman, 2003b).

Like IP address filtering, DNS poisoning will lead to overblocking of sites that share domain names (such as Yahoo! Groups and YouTube videos). It can also block access to non-Web services on the targeted domain such as e-mail and chat. It is trivially circumvented using proxies, and by users requesting web pages using IP addresses. Dornseif (2003) found that ISPs in Germany ordered to block access to hate sites had used DNS poisoning but almost all had made mistakes in their implementations.

IP address filtering and DNS poisoning both need government-compiled or backed lists of servers that should be blocked. Given the speed at which new content appears on the Internet, this is a time-consuming process. A third option is for routers and government-run Web proxies to filter individual pages based on lists of forbidden keywords such as "falun" in the case of China (Clayton, Murdoch & Watson, 2006). Search engines have also been pressured by China to filter search results that contain certain keywords such as "free Tibet" (OpenNet Initiative, 2004).

Deployed in this fashion, the quantity of pages blocked by keyword filters is unlikely to be acceptable outside totalitarian states. However, they can also be used to block access to specific web pages (rather than entire websites, as with IP address filtering and DNS poisoning). This type of filtering is much more resource intensive than IP address filtering.

Keyword filters in routers can be circumvented using proxies that encrypt data sent back to the requesting user, avoiding their detection (Feamster et al., 2002). Clayton, Murdoch and Watson (2006) also found that the specific mechanism used in Chinese networks to block access to pages based on keywords could simply be ignored by Web browsers and servers.

Hybrid filtering systems have been developed that combine one or more of the filtering techniques described above. British Telecom's "Cleanfeed" system redirects requests for web pages on a list of specific servers to a keyword filter that blocks access to specific web pages hosted on those servers. This combines the efficiency of IP address filtering with the precision of keyword filtering applied to specific pages. However, Clayton (2005) showed that the BT system could be used to search out child pornography contained in pages on the secret filtering list.

Even when states are able to persuade overseas organisations hosting Web pages to limit access to their own citizens, the ability to determine the geographical origin of a web browser is still primitive and trivially fooled. Court experts gave evidence that Yahoo could block French users from certain auctions with 70-80% efficacy, but one of the three experts later amplified his reasoning as follows:

> *My answer was, in essence, this: no, compliance is impossible. But I was not allowed to leave it at that; remember that if it was not possible to comply completely, I was asked to say to what extent compliance is possible. The best that can be achieved is a rather flakey guess at nationality, using IP address or domain name (we estimated this was around 80% accurate for France, with some obvious huge exceptions, like AOL subscribers). Failing that, one can simply ask the websurfer whether she's French, and, if so, plant a cookie to that affect.*
>
> *Of course, both of these can be trivially circumvented. The first by using an anonymizer, for example http://www.anonymizer.com/ (note that I am in no way recommending this particular one, it just happens to be the first I found, after 10 seconds of searching), or by signing up for AOL. The second can be avoided simply by lying*. (Laurie, 2000)

The Decreasing Salience of the Web

A further problem with most filtering technology is that it is targeted at content distribution systems, particularly the Web, that are becoming decreasingly popular in terms of total Internet traffic. Peer-to-peer (P2P) systems such as BitTorrent and eDonkey are now estimated to carry up to 60% of data on large Internet networks (CacheLogic, 2006).

Many P2P systems are designed in response to music and movie industry attempts to block the sharing of copyrighted works, and are hence much more robust in the face of censorship. Other systems such as the Eternity Service (Anderson, 1996) and FreeNet (Clarke et al., 2000) are explicitly designed to resist censorship.

All of these systems avoid reliance on single machines that can be shut down or blocked, and on DNS names that can be poisoned; and are able to exchange encrypted files that cannot be keyword-filtered by intermediaries.

Conclusion

While China, Iran and Saudi Arabia have led the non-democratic world in filtering their citizens' access to overseas websites, democracies across Europe and North America are following in their wake.

The technologies being used are extremely imprecise, and often as a by-product block access to very large amounts of legitimate material. Ben Edelman found in 2001 that filtering systems in widespread use by US libraries and schools blocked many thousands of sites that did not come under the relevant definitions in the Children's Internet Protection Act (Edelman, 2001). Even where more precise hybrid systems such as BT's Cleanfeed are put in place, determined users can still bypass filters using proxies and peer-to-peer systems.

The lack of transparency, judicial oversight and ability to contest the inclusion of specific sites in such filtering lists are all extremely problematic for freedom of expression. Such mechanisms fall far below the scrutiny required by a decades-old US Supreme Court ruling:

> *Only a judicial determination in an adversary proceeding ensures the necessary sensitivity to freedom of expression, only a procedure requiring a judicial determination suffices to impose a valid final restraint.* (Freedman v. Maryland, 1965)

What all of these regimes have in common is that filtering technologies are difficult and expensive to impose for any reason; but once introduced can extremely easily encompass new areas of content. New websites and keywords can be blocked as easily as they can be typed into filtering lists. Blocks on access to child pornography can be trivially extended to restrictions on "hate speech," "glorification" of terrorism and from there to political debate and information on minority rights, alleged defamation (Rauch, 2003), purported copyright infringement (IFPI, 2007) and the "sacred texts" of cults such as Scientology (Lippard & Jacobsen, 1995).

Such filters would doubtless catch the following piece of glorification:

> *"I do not, however, deny that I planned sabotage. I did not plan it in a spirit of recklessness, nor because I have any love of violence. I planned it as a result of a calm and sober assessment of the political situation that had arisen after many years of tyranny, exploitation, and oppression of my people by the Whites. . . . I, and some colleagues, came to the conclusion that as violence in this country was inevitable, it would be unrealistic and wrong for African leaders to continue preaching peace and non-violence at a time when the Government met our peaceful demands with force. This conclusion was not easily arrived at. It was only when all else had failed, when all channels of peaceful protest had been barred to us, that the decision was made to embark on violent forms of political struggle, and to form Umkhonto we Sizwe. We did so not because we desired such a course, but solely because the Government had left us with no other choice."*

South Africa and the rest of the world would however be much the worse without the leadership of Nelson Mandela, quoted here at his trial in 1964 during fruitless attempts to prevent "glorification" being made an offence in the UK (Lords Hansard, 2006). Governments such as Russia, China and Turkey are pursuing ongoing campaigns against minority groups in Chechnya, Tibet and Kurdistan (Human Rights Watch, 2007) and would appreciate both the moral support and technology development that would result from any mandatory introduction of filters in European Union states and Canada.

Absent the intimidation of a totalitarian state, the technically savvy and the determined are easily able to circumvent Internet filters, and content is increasingly being accessed using peer-to-peer systems that are even more difficult to police. It is mainstream Internet users whose access to information will be most affected by filtering systems.

Some governments have accepted this, and claim that their aim is merely to stop users "accidentally" viewing blocked information (Lehdonvirta, 2006). Regulators have rejected this broadcasting-era doctrine when considering Internet content regulation (Federal Communications Commission, 1997). Does such an aim justify striking a potentially fatal blow to "the most democratic speech technology yet invented, one with the greatest potential of allowing freedom of expression to those who do not own a printing press or a television station" (Boyle, 2004)?

If citizens are cut off from information sources and each other, the global network value (Briscoe, Odlyzko and Tilly, 2006) of the Internet will be reduced significantly. Civil society activists, who make extensive use of the Internet to carry out their work, could be particularly badly affected (Deibert & Villeneuve, 2005, p.123).

There is a danger that states with a commitment to freedom of expression are putting in place an unwieldy and ineffective censorship infrastructure that could easily be abused by future governments and repressive regimes. Have we learned nothing since Sigmund Freud made the following observation in 1933?

> *"What progress we are making. In the Middle Ages they would have burned me. Now they are content with burning my books."* (Jones, 1957)

Acknowledgements

The author would like to thank Douwe Korff for useful comments on a draft of this article.

References

Anderson, M. (2006). A Sneak Peek at a Fractured Web. *Wired News*, November 13, 2006. Retrieved January 12, 2007, from http://www.wired.com/news/technology/0,72104-0.html.

Anderson, R. J. (1996). The Eternity Service. *Proc. Pragocrypt '96.*

Ashcroft v. American Civil Liberties Union 542 U.S. 656 (2004).

BBC News (2003). Iran steps up net censorship. *BBC Online*, May 12, 2003. Retrieved January 13, 2007, from http://news.bbc.co.uk/2/hi/technology/3019695.stm.

Boyle, J. (2004). A Manifesto On WIPO And The Future Of Intellectual Property. Duke Law and Technology Review (9). Retrieved January 17, 2007, from http://www.law.duke.edu/journals/dltr/articles/2004dltr0009.html.

Briscoe, B., Odlyzko, A. & Tilly, B. (2006). Metcalfe's Law is Wrong. *IEEE Spectrum*, July 2006. Retrieved January 17, 2007, from http://www.spectrum.ieee.org/jul06/4109.

CacheLogic Research (2006). Peer-to-Peer in 2005. Retrieved January 16, 2007, from http://www.cachelogic.com/home/pages/research/p2p2005.php.

CDT v. Pappert, 337 F.Supp.2d 606 (E.D. Penn. 2004).

Clarke , I., Sandberg, O., Wiley, B. & Hong, T. W. (2000). A Distributed Anonymous Information Storage and Retrieval System. *Proc. Workshop on Design Issues in Anonymity and Unobservability*, Lecture Notes in Computer Science, 2009 pp.46—66.

Clayton, R. (2005). Failures in a Hybrid Content Blocking System. *Proc. 5th Workshop on Privacy Enhancing Technologies*, Dubrovnik, May 2005. Retrieved January 12, 2007, from http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf.

Clayton, R., Murdoch, S. J. & Watson, R. N. M. (2006). Ignoring the Great Firewall of China. *Proc. 6th Workshop on Privacy Enhancing Technologies*, Cambridge, June 2006. Retrieved January 12, 2007, from http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf.

Claeburn, T. (2006). Google, Microsoft, and Yahoo Urge Government Intervention Against Censorship. *Information Week*, February 1, 2006. Retrieved January 15, 2007, from http://www.informationweek.com/story/showArticle.jhtml?articleID=178600547.

Council of Europe (2003). Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Strasbourg, January 28, 2003. Retrieved January 13, 2007, from http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm.

Deibert, R. & 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.111—124). London: GlassHouse.

Dhawan, H. (2007). YouTube angers I&B with its tasteless Gandhi video. *The Times of India*, January 13, 2007. Retrieved January 16, 2007, from http://timesofindia.indiatimes.com/YouTube_angers_IB_with_its_tasteless_Gandhi_video/articleshow/1161665.cms.

Dornseif, M. (2003). Government mandated blocking of foreign Web content. In J. von Knop, W. Haverkamp & E. Jessen (Eds.). *Security,E-Learning,E-Services*: *Proceedings of the 17th DFN-Arbeitstagung uber Kommunikationsnetze*, Dusseldorf 2003, ISBN 3-88579-373-3, Lecture Notes in Informatics. ISSN 1617-5468, pp.617-648. Retrieved January 13, 2007, from http://arxiv.org/pdf/cs.CY/0404005.

Edelman, B. (2001). Expert Report of Benjamin Edelman in case of Multnomah County Public Library et al., vs. United States of America, et al. Retrieved January 17, 2007, from http://cyber.law.harvard.edu/people/edelman/mul-v-us.

Feamster, N., Balazinska, M., Harfst, G., Balakrishnan, H. & Karge, D. (2002). Infranet: Circumventing Web Censorship and Surveillance. Proc. USENIX Security 2002, pp.247—262. Retrieved January 16, 2007, from http://www.usenix.org/events/sec02/feamster/feamster_html/.

Federal Communications Commission (1997). Digital Tornado: The Internet and Telecommunications Policy. *FCC Office of Plans and Policy Working Paper*, March 1997. Retrieved January 31, 2007 from http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp29.txt

Freedman v. Maryland, 380 U.S. 51 (1965)

Geist, M. (2006). Child Porn Blocking Plan a Risk Worth Taking. *Toronto Star*, December 4, 2006. Retrieved January 13, 2007, from http://www.michaelgeist.ca/content/view/1560/159/.

Gomes, L. (2006). Will All of Us Get Our 15 Minutes On a YouTube Video? *Wall Street Journal*, August 30, 2006. Retrieved January 16, 2007, from http://online.wsj.com/public/article/SB115689298168048904-5wWyrSwyn6RfVfz9NwLk774VUWc_20070829.html.

Government of Saudi Arabia Internet Services Unit (2006). Introduction to Content Filtering. Retrieved January 12, 2007, from http://www.isu.net.sa/saudi-internet/contenet-filtring/filtring.htm.

House of Commons Hansard (2006). Written Answers for 15 May 2006 (pt 0107) col. 715W, 15 May 2006. Retrieved January 13, 2007, from http://www.publications.parliament.uk/pa/cm200506/cmhansrd/cm060515/text/60515w0111.htm#06051532000085.

Human Rights Watch (2007). World Report. ISBN 1-58322-740-7. Retrieved January 17, 2007, from http://www.hrw.org/wr2k7/wr2007master.pdf.

Hutty, M. (2006). Government sets deadline for universal network-level content blocking. London Internet Exchange Public Affairs blog, May 17, 2006. Retrieved January 13, 2007, from http://publicaffairs.linx.net/news/?p=497#more-497.

Hutty, M. (2007). Italian law mandates content blocking. London Internet Exchange Public Affairs blog, January 5, 2007. Retrieved January 13, 2007, from http://publicaffairs.linx.net/news/?p=622.Jones, E. (1957) *Sigmund Freud: Life and Work*, vol. 3, pt. 1, ch. 4. London: Hogarth Press.

IFPI (2007). Digital Music Report. International Federation of the Phonographic Industry. Retrieved January 19, 2007 from http://www.ifpi.org/content/library/digital-music-report-2007.pdf

Jorgensen, R. (2006). Blocking access to child pornography: The Danish Case. *European Commission Safer Internet Forum 2006*. Retrieved January 31, 2007 from http://europa.eu.int/information_society/activities/sip/docs/forum_june_2006/rikke_frank_joergenseng.pdf

The King's English v. Shurtleff, Civil Action No. 2:05-cv-00485-DB (D. Utah Aug. 25, 2006). (Stipulated Order)

Laurie, B. (2000). An Expert's Apology. Retrieved January 13, 2007, from http://www.apache-ssl.org/apology.html.

Lehdonvirta, W. (2006). Finnish ISPs must voluntarily block access. *EDRI-gram*, September 8, 2005. Retrieved January 13, 2007, from http://www.edri.org/edrigram/number3.18/censorshipFinland.

Lippard, J. & Jacobsen, J. (1995) Scientology v. the Internet: Free Speech & Copyright Infringement on the Information Super-Highway, 3 Skeptic 3, 35–41. Retrieved January 19, 2007 from http://www.discord.org/~lippard/skeptic/03.3.jl-jj-scientology.html

Lords Hansard (2006). 28 Feb 2006 : Column 152. Retrieved January 17, 2007, from http://www.publications.parliament.uk/pa/ld199697/ldhansrd/pdvn/lds06/text/60228-08.htm.

OpenNet Initiative (2004). Probing Chinese search engine filtering. Retrieved January 16, 2007, from http://www.opennetinitiative.net/bulletins/005/.

OpenNet Initiative (2005a). Internet Filtering in China in 2004-2005. Retrieved January 12, 2007, from http://www.opennetinitiative.net/studies/china/ONI_China_Country_Study.pdf.

OpenNet Initiative (2005b). Internet Filtering in Iran in 2004-2005. Retrieved January 12, 2007, from http://www.opennetinitiative.net/studies/iran/ONI_Country_Study_Iran.pdf.

OFCOM (2006). Office of Communications chairman's annual lecture, David Currie, November 1, 2006. Retrieved January 19, 2007 from http://www.ofcom.org.uk/media/speeches/2006/11/annual_lecture

Penfold, C. (2001). Nazis, Porn and Politics: Asserting Control Over Internet Content. *Journal of Information, Law and Technology*, 2001(2). Retrieved January 13, 2007, from http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_2/penfold/.

Privacy International (2003). Silenced: An International report on Censorship and Control of the Internet. Retrieved January 17, 2007, from http://www.privacyinternational.org/survey/censorship/silenced.pdf

Reno v. American Civil Liberties Union, 117 U.S. 2329 (1997).

Rauch, F. (2006). Internet censorship in Switzerland. *EDRI-gram*, February 12, 2003. Retrieved January 13, 2007, from http://www.edri.org/edrigram/number2/censor.

Reporters San Frontières (2006). Authorities boast of success in Internet filtering. Retrieved January 13, 2007, from http://www.rsf.org/article.php3?id_article=18864.

Reuters (2007a). Italy enacts law to block child porn Web sites. *Reuters Internet news*, January 2, 2007. Retrieved January 13, 2007, from http://today.reuters.com/news/articlenews.aspx?type=internetNews&storyID=2007-01-02T185905Z_01_L02273101_RTRUKOC_0_US-ITALY-INTERNET.xml.

Reuters (2007b). Phone companies in Brazil blocking YouTube, *Reuters Internet news*, January 8, 2007. Retrieved January 16, 2007, from http://today.reuters.com/news/articlenews.aspx?type=technologyNews&storyid=2007-01-09T005413Z_01_N08418109_RTRUKOC_0_US-BRAZIL-SEX-YOUTUBE.xml.

Tait, R. (2006). Iran bans fast internet to cut west's influence. *The Guardian*, October 18, 2006. Retrieved January 13, 2007, from http://technology.guardian.co.uk/news/story/0,,1924637,00.html.

US Copyright Office (2003). Rulemaking hearing under §1201 Digital Millennium Copyright Act, April 11, 2003. Retrieved January 16, 2007, from http://www.copyright.gov/1201/2003/hearings/transcript-apr11.pdf.

Zittrain, J. & Edelman, B. (2002). Documentation of Internet Filtering in Saudi Arabia. *Berkman Center for Internet & Society*, September 2002. Retrieved January 12, 2007, from http://cyber.law.harvard.edu/filtering/saudiarabia/.

Zittrain, J. & Edelman, B. (2003a). Documentation of Internet Filtering Worldwide. In C. Hardy and C. Moller (Eds.), *Spreading the Word on the Internet: reflections on freedom of the media and the Internet* (pp.137—148). Vienna: Organisation for Security and Cooperation in Europe. Retrieved January 12, 2007, from http://www.osce.org/publications/rfm/2003/06/12245_103_en.pdf.

Zittrain, J. & Edelman, B. (2003b). Internet filtering in China. IEEE Internet Computing, 7, 2 pp.70—77, March/April 2003.