Freedom Of Speech And Censorship In The Internet

Joon-Yeoul Oh, Texas A&M University-Kingsville, USA
Rick A. Aukerman, Texas A&M University-Kingsville, USA

ABSTRACT

Internet censorship or internet content filtering is used to protect people from harmful materials, such as child pornography, as well as defamation and fraud, which are easily perpetrated on the internet. However, implementing censorship creates technical and social issues, such as over-blocking or false detection, decreased network performance, and freedom of speech. This paper describes internet content filtering approaches and technical difficulties to implementation. This paper also discusses censorship and freedom of speech with actual examples.

Keywords: Internet Censorship; Internet Content Filtering; Filtering Techniques; Content Control Software; Freedom of Speech

INTRODUCTION

The advent of the internet has changed the way that people exchange information, and almost any digital resources are available instantaneously to anyone with a computer and internet connection. However, this accessibility and availability apply to both legal and illegal contents. In order to protect people from accessing illegal content, almost every country has laws against certain types of activities, such as child pornography, defamation, and fraud. Enforcing these laws against illegal content on the internet is significantly more difficult than regular law enforcement. Because the internet itself has no concept of legal boundaries or jurisdiction and sometimes the physical host is outside the country in which the law was enacted, law enforcement agencies often find themselves unable to take action against the vast majority of web sites which break their laws. Even if a similar law exists in the country where a service is hosted, the best that can be done is to notify to the local authorities and the law enforcement agencies to discourage the potential customers of these services while monitoring or filtering the system.

Even though internet content filtering programs are unpopular and ineffective, a large number of them, such as Net Nanny, Covenant Eyes, and Websense, are still in place around the world. Because the cost of implementing these programs is usually passed straight down to the consumer, the cost of internet access in those countries which have implemented filtering systems is higher than in other areas. The recent Australian filtering program is budgeted to cost as much as $128 million (Clarke, 2009). Other factors which contribute to the cost of filtering systems in addition to the initial layout include expenses such as extra help desk staff hired to take calls from customers who cannot access websites and the cost of maintaining an up-to-date list of blocked pages (Conklin et al., 2004). No data is available on the cost of wide-scale deployments such as the one in China, but it is quite likely an astronomical sum.

Aside from direct monetary amounts, one of the biggest costs incurred by content filters is in the form of decreased network performance. Some of the solutions proposed for the Australian filtering system slowed down regular internet browsing by as much as 87 percent (Pillion, 2009). Although not all filtering systems have such extreme performance penalties, offsetting performance problems increases the monetary cost considerably. Another item that needs to be considered when implementing content filtering systems is the cost of false positives. Even the best of the content filters being considered in the Australian operation still has a 1% false positive rate (Meloni, 2008). The economic costs of blocking traffic to many websites cannot be precisely determined, but it is certainly a factor that should not be ignored.

However, because the internet was built from the ground up as a decentralized network, it is able to reroute itself around physical damage or censorship easily. This poses a significant challenge to those organizations which are charged with policing the trafficking of illegal materials. While ISPs (Internet Service Providers) often physically implement internet content filtering systems, government and law enforcement agencies make up the primary proponents for their adoption. In general, public opinion regarding any kind of mandatory content filtering system is quite negative. The enormous backlash against the recently-proposed filtering scheme in Australia demonstrates this very well. According to a national telephone poll, only 5 percent of the Australian population wants ISPs to be responsible for protecting children from on-line predators, and only 4 percent want the responsibility to fall on the shoulders of the government (Moses, 2009). Netspace, an Australian ISP, conducted a survey of its customers regarding the issue. Over 60 percent of the people interviewed were strongly opposed to mandatory filtering, while only 6.3 percent of those interviewed agreed strongly with the policy (Moses, 2009). Another public issue is that internet content filtering restricts freedom of speech. This paper describes the way to control internet content and the technical difficulties of internet censorship. The misuses and drawbacks of content filtering are also discussed.

CONTENT RESTRICTIONS APPROACHES

Internet censorship can occur at any location in the network, such as internet backbone, ISP, organizations and individual computers. Figure 1 shows the content censorship points. A wide and national level of content filtering and blocking occurs at the internet backbone. The ISPs implement government-mandated filtering. An organization, such as a business, school, or government agency can block or filter unnecessary and harmful internet content at its own organizational level. Filtering for a home computer or other individual internet access device can be achieved by installing filtering software, so that the device cannot access certain sites (Opennet, 2009).

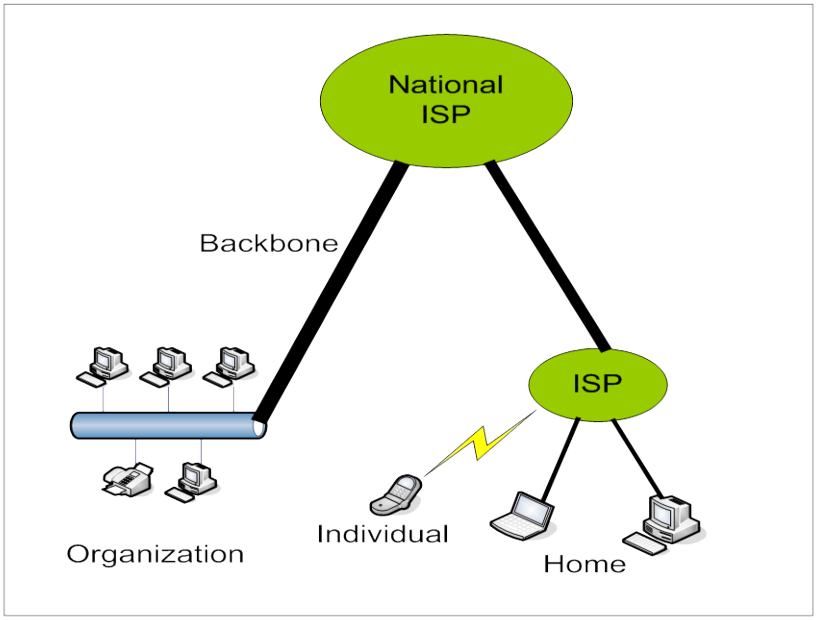

Figure 1: Content Censorship Points

There are several approaches for implementing internet censorship. One approach is technical blocking, such as IP (Internet Protocol) blocking, DNS (Domain Name System) tampering, and URL (Uniform Resource Locator) blocking, which are used to block specific WebPages, domains, and/or IP addresses. A second approach is search result removal. This approach is completed by an internet service provider cooperating with government to remove illegal materials from search results. Simply asking the web content hosts to remove the inappropriate or illegal content and not-accessing or not-posting illegal content, which is self-censorship, would be included in other forms of censorship approaches.

TECHNICAL DETAILS AND LIMITATIONS

While there are many disputes over whether internet content filtering should be performed at all, there is one point that can be almost universally agreed upon by anyone with experience in the field of Information Technology: Internet Content Filtering is completely ineffective at accomplishing its goals. Trying to prevent the flow of information on the internet is a costly arms-race at best, and is often simply a complete waste of time and money with very little chance of success. No matter what form of filtering approach is used, those who are determined to access the blocked content can almost always skirt around the restrictions with very little effort.

The simplest and cheapest method of content filtering is accomplished through manipulation of DNS records. Because most users receive their IP configuration through DHCP (Dynamic Host Configuration Protocol) from their ISP, it is easy to point them toward the desired DNS server. It is a trivial task for the ISP to configure its DNS servers to resolve undesirable addresses to a “block-page”, or simply to nothing at all. Some free DNS services such as OpenDNS allow private homes and businesses to easily manage this kind of filter with a few short clicks (Diehl, 2009). Of course, there is nothing stopping users from simply changing the computer settings to point toward a different, non-filtered DNS server of their choice. Another problem with DNS filtering is a tendency towards “scatter-shot” web site blocking. Since DNS resolution is not particularly granular, it is often required to block entire domain names at once, leading to large amounts of collateral damage in certain hosting arrangements. In essence, this approach is equivalent to erasing records out of a local phone book. The numbers are still there for you to call if you know what they are, and nothing is preventing someone from picking up a different phone book and looking up the number.

The next procedure in the filtering arms-race is to block unwanted websites by IP address instead of just filtering the FQDN (Fully Qualified Domain Name). This approach requires significantly more investment and overhead because of analyzing the headers of all packets that pass through your network, usually with a router, and comparing them to a list of filtered addresses. According to an interview of a policy chief from a peering cooperative, many smaller ISPs in Britain refuse to implement the “Cleanfeed” filtering system, the UK’s content locking system deployed by many of the larger ISPs, because “it would mean spending a lot of money on something that simply does not work” (Williams, 2009). One of the ISPs that has agreed to deploy the system has stated that it has only done so in order to prove to the politicians pushing for its adoption that it cannot work (Strover, 2009).

The Cleanfeed system first checks against a list of “suspect” IP addresses as they pass through a gateway router. If there is a match, it passes the packets on to a proxy server which then does more granular page-level checking and blocks only those pages which contain the blacklisted material. However, this method of filtering is bypassed just as easily as regular DNS filtering. Since there is no deep-packet inspection occurring, websites that wish to bypass the filter can simply be hosted on ports other than 80 to avoid the blocks by disguising themselves as something other than web traffic. Users can also connect to websites through proxy servers in another country outside of the filtering system, who will serve the web pages in their name to avoid the blacklist. Standard encryption also defeats this kind of filtering scheme.

Another logical approach in the filtering game is to perform deep-packet inspection on all traffic in order to stop web traffic to blacklisted sites which does not occur on the standard ports. Inspecting the entire packet in order to determine the type of traffic is a relatively simple, but expensive task (Strover, 2009 & Maiwald, 2004). It requires more processing time than simple header inspection since the payload contained in a packet is far longer than the header. This process vastly increases hardware costs and almost always decreases network performance significantly. Even after investing in the equipment required for filtering content in this manner, however, it is still bypassed very easily. All requirements to defeat this filtering mechanism are standard encryption, either via HTTPS (Hypertext Transfer Protocol Secure) or a VPN/SSH (Virtual Private Network/Secure Shell) tunnel. Blocking or forcing proxy use on all encrypted content to circumvent this breaks a significant portion of the internet, while also opening users up to potential security risks such as MITM (Man-in-the-middle, a form of eavesdropping) attacks.

Another issue to address is the ease of access to proxy servers which can be used to bypass many types of filters. There are so many proxy servers on the internet that adding all of them to the block list is essentially an impossible task. Although proxy servers are important for many legitimate uses and internet anonymity, we can assume that all of the customers are being treated like criminals, anyway, so this is unlikely to be a consideration. Although employing the number of people required to track down and block every proxy server on the internet is not feasible for most ISPs, the PRC (People's Republic of China) has worked hard at accomplishing this task. However, individuals are easily able to run personal or private non-indexed proxy servers outside the boundary of the firewall. It is effectively unfeasible to prevent private proxy servers from being used to circumvent nearly any firewall scheme without blocking all access to IP addresses outside of your control, which would be economically disastrous.

However, personal proxy servers are probably beyond the means of the average overly-curious internet user who might run afoul of internet Content Filters. Since packet headers have to remain unencrypted in order to remain usable by the ISP routers, and we now have a complete list of banned IP addresses from both websites and proxy servers, the battle seems essentially won against all but the most dedicated users. Of course, the internet has enabled the discovery of a number of ways to circumvent even a firewall as extensive as the one deployed in China. Programs such as Freenet have created a decentralized, encrypted peer-to-peer network which sits on top of the regular internet infrastructure that is almost impossible to block. Other programs such as Tor can be easily integrated into many web browsers such as Firefox in the form of plug-ins. This extension gives one-click anonymity through a distributed encrypted network. In order to block users from using these meta-networks to bypass content filtering, the filtering operation would have to block each and every computer on the planet that is running the software.

CENSORSHIP OR FREEDOM OF SPEECH

Over-blocking due to faulty categorization and transparency are often involved in the censorship debate. Many law enforcement agencies argue that if the list of blocked sites was made public, it would serve as nothing more than a phone book for those who wish to circumvent the system. The governmental body which manages the list of blocked child pornography sites in the Australian trials is the Australian Communications and Media Authority. While they refuse to disclose which sites are on the list, they have released some statistics regarding the makeup of the sites which are blocked. Of the 1370 websites blocked under the program, only 864 are in the same classification category as child pornography. Over 400 of the sites which are blocked by the program are still pornographic, but are classified as X18+ (hardcore non-violent pornography), which is legal within Australia with restricted access (Foo, 2009). Even at this early stage, the authority, which is responsible for maintaining the list openly, admits that it blocks perfectly legal sites which are not subject to the legislation authorizing the filtering system in the first place. The lack of oversight regarding this issue is troubling to many people.

The Australian filtering system is not the first internet content filtering system which suffers from a lack of transparency. In late 2008, six British ISPs simultaneously added Wikipedia.org to their child pornography block lists (Metz, 2008). Because one out of their millions of articles contained a controversial album cover with a picture of a nude girl on it, the entire website was labeled as child pornography. In addition, the filtering system routed almost all of the British traffic to Wikipedia through a small handful of IP addresses used by the proxy servers. This caused serious administration issues for websites such as Wikipedia. Since bans are performed via IP address, the administrators are forced to either ban the entire country from contributing to articles at all, or allow rampant defamation. Either choice has severe negative consequences for all users of Wikipedia.

Another reason that many people are wary of internet content filtering systems is because they can so easily be used to squelch political opposition. This is not an unjustified fear, as there are many examples of this happening with existing filter implementations. Every single filtering system to date has blocked legitimate sites, either mistakenly or intentionally. One of the most startling examples of this occurred in early 2008, when M. Nikki (Nikki, 2008) began to protest against the web filter put in place in his country of Finland to stop child pornography. He conducted research on the filtering system and was able to discern which websites were blocked by the filter, as they were not disclosed to the public. He posted these results on his web site. A few weeks later, his own site was added to the block list. It is immediately obvious that the only reason his web site was censored was because of political reasons. Not only was his web site clearly not an example of child pornography, but it was also hosted locally in Finland. If any Finnish laws had actually been broken, local law enforcement could have easily stepped in and taken action. To this day, Nikki has not been charged with any kind of crime.

Another downside to a lack of transparency surrounding internet content filtering lists is the introduction of false positives. Any filtering system will understandably have a few web sites which fall through the cracks, but there have been examples of incredibly well-known and legitimate websites being blocked for little or no reason. The Finnish content filtering system erroneously blocked the World Wide Web Consortium (W3C) website late 2008 in a startling display of ineptitude (Lehto, 2008). The W3C is a standards body which maintains HTML, XML, and other important formats that comprise the backbone of the Web. There are only two possible explanations for this mistake. Websites which are reported to the system are either not reviewed at all, or the analysis is being done by a (malfunctioning) program and there is no human involvement. The URL for the W3C web site is embedded in the source code for all properly-written HTML pages. Because it is unlikely that anyone would intentionally submit the W3C web site to the block list, it seems probable that whatever system is analyzing the submissions stripped their URL out of the source code and added it to the list.

Filtering of non-illegal content is explicitly forbidden through freedoms of speech and press given in their constitutions and laws. However, these kinds of laws are not universal. While countries with freedom of speech are forced to add shady entries to their block lists behind closed doors, many of those without similar protections have no qualms about doing it in the open. By far, the most extensive internet content filtering system in place today is deployed by the PRC government. Nicknamed the “Great Firewall of China” by most westerners, the filtering system goes beyond simple website blocks and actively filters other internet services such as Instant Messaging and E-mail. The program has gone so far as to make a concerted effort to block all “lewd” content on the internet by employing thousands of workers to report offenders (Powell, 2009). While this is obviously a monstrous undertaking, the filtering is done on such a massive scale that this endeavor may actually succeed.

The Chinese filtering system is not limited to illegal or “immoral” content, however. Most western news sources, such as the *New York Times* web site, are inaccessible from behind the Chinese firewall (Bradsher, 2008). One of the primary goals of the filter is to prevent the flow of information which is “politically harmful”. They have even coerced outside companies such as Google to remove all references to events such as the Tiananmen Square massacre, the Dalai Lama, and Falun Gong. During the 2008 Olympics, the IOC (International Olympic Committee) forced the PRC to temporarily lift the filtering restrictions for the duration of the event (Taylor, 2008). During this period, the English-language version of Wikipedia was accessible to users in China, but not the Chinese-language version. These changes were only temporary, however, and the firewall has since returned to its previous state.

In the United States, there is no nationwide internet filtering, but public institutions block pornographic and harmful materials related to the sexual exploitation of children by law, the Children’s internet Protection Act (CIPA). However, researchers have found over-blocking of some content related to women’s health, gay and lesbian rights groups, and sexual education for teenagers (The citizen lab, 2007).

CONCLUSION

Internet content filtering systems have been employed by a number of countries and ISPs around the world. They all suffer from poor public support, high costs, and a lack of technical effectiveness. While there are some circumstances where a small-scale deployment of a filtering system may be appropriate, it is most certainly not yet feasible on a large scale. To implement a content filtering system generates negative consequences, such as decreased network performance, false detection, and restricted freedom of speech. These social and technical issues are very important and cannot be separated like both sides of coin. Even though current laws exist to prevent internet usage for activities that are deemed inappropriate, they are easily bypassed. The worldwide pervasiveness of internet usage has only served to “muddy the waters” of appropriate and socially acceptable communication and international legality.

ACKNOWLEDGEMENT

The authors would like to acknowledge the contributions of Davis Gossett, an undergraduate Information Systems student assistant at the time this research was initiated.

AUTHOR INFORMATION

Joon-Yeoul Oh is an associate professor of the department of Mechanical and Industrial Engineering of the College of Engineering at Texas A&M University-Kingsville. Before joining the College of Engineering, he worked for the Information Systems Department for eight years. His research interest is in the areas of operation research, focusing on algorithm development, simulation, and the telecommunication and manufacturing network systems optimization. E-mail: kfjo000@tamuk.edu (Corresponding author)

Richard Aukerman is a Professor and Chair of the Information Systems Department and Associate Dean of the College of Business Administration at Texas A&M University-Kingsville. He received the Ph.D. from the University of North Dakota. His recent research has been in the areas of business ethics and the application of personal values in decision making. E-mail: kfraa00@tamuk.edu

REFERENCES

1. Clarke, T. (2009). Xenophon speaks out against internet content filtering, Retrieved March 8, 2009, from http://www.computerworld.com.au/article/278285/xenophon_speaks_against_internet_content_filtering?fp=4194304&fpid=1
2. Conklin, A. W., Williams, D., White B. G., Davis, L. R., Cothren, C., (2004). *Principles of Computer Security: Security and Beyond*. New York, New York: McGraw-Hill.
3. Pillion, A. (2009). Mandatory filtering won’t slow net access, Retrieved March 7, 2009, from http://www.australianit.news.com.au/story/0,24897,25040381-5013038,00.html
4. Meloni, M. (2008). The high price of internet filtering, Retrieved March 8, 2009, from http://www.abc.net.au/news/stories/2008/10/24/2399876.htm
5. Moses, A. (2009). Web Censorship Plan Heads Towards a Dead End, Retrieved March 6, 2009, from http://www.smh.com.au/articles/2009/02/26/1235237810486.html
6. Opennet (2009). About Filtering, Retrieved August 28, 2009, from http://opennet.net/about-filtering
7. Diehl, M. (2009). Web Content Filtering with OpenDNS, Retrieved March 8, 2009, from http://www.linuxjournal.com/content/web-content-filtering-opendns
8. Williams, C. (2009). Small ISPs reject call to filter out child abuse sites, Retrieved March 6, 2009, from http://www.theregister.co.uk/2009/02/25/iwf_small_isps/
9. Strover, R. (2009). Clean Feed, retrieved March 7, 2009, from http://www.melbpc.org.au/pcupdate/2902/2902article7.htm
10. Maiwald, E. (2004). *Fundamentals of Network Security*. New York, New York: McGraw-Hill.
11. Foo, F. (2009). Row Over Web Blacklist, Retrieved March 7, 2009, from http://www.australianit.news.com.au/story/0,24897,25096792-15306,00.html
12. Metz, C. (2008). British ISPs censor Wikipedia over ‘child porn’ album cover, Retrieved March 6, 2009, from http://www.theregister.co.uk/2008/12/07/brit_isps_censor_wikipedia/
13. Nikki, M. (2008). Lapsiporno.info and the Finnish internet censorship, Retrieved March 5, 2009, from http://lapsiporno.info/english-2008-02-15.html
14. Lehto, T. (2008). Virhe korjattiin nopeasti tänään, Retrieved March 7, 2009, from http://translate.google.com/translate?u=http%3A%2F%2Fwww.tietokone.fi%2Fuutta%2Fuutinen.asp%3Fnews_id%3D35075%26tyyppi%3D1&hl=en&ie=UTF-8&sl=fi&tl=en
15. Powell, G. (2009). China makes arrests to stop ‘vulgar’ content, Retrieved March 6, 2009, from http://tech.blorge.com/Structure:%20/2009/01/16/china-makes-arrests-to-stop-internet-porn/
16. Bradsher, K. (2008). China Blocks Access to the Time’s Website, Retrieved March 6, 2009, from http://www.nytimes.com/2008/12/20/world/asia/20china.html?_r=2&ref=todayspaper
17. Taylor, S. (2008). China allows access to English Wikipedia, Retrieved March 8, 2009, from http://in.reuters.com/article/technologyNews/idINIndia-32865420080405
18. The Citizen Lab, The University Toronto. (2007). Everyone’s Guide to By-passing Internet Censorship for Citizens Worldwide. [Electronic version]. A civisec Project, p. 6.