Internet Censorship in China

Treasa Nic Giolla Chomhaill
Computer Science Department, Letterkenny Institute of Technology, Ireland

Nigel McKelvey
Computer Science Department, Letterkenny Institute of Technology, Ireland

Kevin Curran
School of Computing and Intelligent Systems, University of Ulster, Northern Ireland

Nadarajah Subaginy
School of Computing and Intelligent Systems, University of Ulster, Northern Ireland

INTRODUCTION

Freedom of information is an internationally protected Human Right and the Internet is said to be unlike any other medium with it enabling us to search for, obtain and disperse ideas and information and it therefore an "enabler" of other human rights (Human Rights Council, 2011). It is written in the constitution of China that every citizen is granted the right to freedom of speech; however these censorship laws contradict this freedom of speech and freedom of information. It limits the information available to Chinese citizens and it indeed manipulates them by injecting pro-CCP information and messages throughout the Internet, and with the help of multinational corporations what chance do the people of China have to fight for their freedom of speech. With numerous court cases and sentences passed for this 'criminal activity', there does not seem to be any dramatic change in the future of Chinas Internet censorship, aside from an increase in their censorship laws and continuous co-operation from Internet companies.

Chinas oligarchy consists of the Chinese Communist Party (CCP), who has been in power for over 60 years. They have always had rules and regulations which control the amount of information that the Chinese people have access to. China's constitution states that every citizen is granted the right to freedom of speech yet their laws seem to contradict this by putting a restriction on the information that the people of China can share on the Internet. I intend to explore the censorship laws that the CCP have enforced online, the self-censorship of multinational companies who have made agreements with the CCP, and also some court cases that have seen Chinese citizens go to jail for lengthy periods of time because of 'criminal activity' online. With the help on online databases, and articles these hazy definitions, agreements and laws will hopefully become clearer.

A huge portion of Chinas censorship laws are based around self-censorship. This shifts a large portion of responsibility onto the Internet providers and Internet sites. These self-censorship laws have been working in favour of the Chinese Government with all sorts of worldwide companies obeying them and working with the Government to ensure the Chinese citizens themselves do not break these laws. To name but a few, Microsoft, Yahoo and Google have all agreed to these laws at one time or another. The intention of this chapter is to discuss Chinas Internet censorship laws, and highlight some of the issues that have arisen from these laws. Censorship has always been prevalent in China and with the introduction of the Internet in 1990 it was no different. Some would argue that regulating the Internet is a good thing if the intention is to prevent criminal activity. The problem in the case of China is the definition of criminal activity.

BACKGROUND

Censorship has always been prevalent in China and its media. The CCP introduced the people of China to the Internet in 1990. From the beginning of this introduction

DOI: 10.4018/978-1-4666-5888-2.ch137

the Internet was treated no different to any other form of media and so came with it. It is only set of censorship laws. Some would argue that regulating the Internet is a good thing if the intention is to prevent such crimes as child pornography, and other online criminal acts. It is written in the constitution of China that every citizen is granted the right to freedom of speech; however these censorship laws seem to contradict this right to freedom of speech (Bennett, 2013).

Before we look at the law a closer eye should be cast to the infrastructure which is described by Cherry (2005). Chinas Network is called CN2, and is made up of over 200 routers which an installed throughout the country. These routers, made by companies such as Juniper and Cisco, are of the best in the world and before this the technology at hand was limited in China, so too was the methods of censorship. But now that technology is no longer a constraint censorship is 'a matter of politics than of technology'. These routers will have access to a database of banned names, phrases and words. In total Zittrain, et al (2003) says that there are 4 filtering methods in total; Webserver IP address, DNS server IP address, keywords, DNS redirection. Although all these measures are put in place the government do not solely depend on this technology. There is a law in place whereby all Internet businesses and Internet providers must apply for a license to allow them to operate online. These licenses will not be given out so easily, and once gained the business must install their own censor-ware to screen for banned names, phrases and words. If they do not adhere to these rules then the license will be taken from them and their business shut down, according to Cherry (2005). There was a separate police force established in 2000, the Internet Police. Their job is to investigate online crimes; viruses, hacking, pornography and politically sensitive material. The main culprit of this 'criminal activity' is the politically sensitive material. The censorship laws themselves are written in such broad terms. For example, ”topics that damage the reputation of the State” are banned but this is so vague that it makes it difficult for the user to know which words, names, topics and phrase they can and cannot discuss (Human Rights Watch, 2001).

The official battle between China and Google was launched by China in 2002 when the Chinese Government prevented local access to Google.com, needless to say Google were not pleased by this move. In February 2004 Google News China was blocked by the Chinese government, this spurred Google to invest in Baidu (the leading search engine in the Chinese cyber market) a mere 4 months later. Then came 2006 when Google officially made the move into the Chinese cyber market, with 384 million online users (in 2006, this figure has since grown to 538 million in 2013) it is the cyber market with the most potential in the world. When a company enters the Chinese cyber market it does so by agreeing to strictly obey by the Chinese Internet Censorship laws. It was a short lived partnership because after a mere 4 years in the Chinese cyber market, Google pulled out of China in 2010.

Google maintains that during its 4 years in China they were hacked, they blamed these hackings on the Chinese Government and stated that they are very capable of sophisticated cyber-attacks (Ho et al., 2011). Next Google stopped filtering their searches, this was a blatant breach of their agreement with the Government to which they responded by saying that Google have broken the written vow that had been made in 2006 by lifting their filtered searches and by blaming China for the so called hackings. A spokesperson stated, '… we express our discontent and indignation to Google for its unreasonable accusations and conduct'. Google now tend to speak out about the wrongful censorship of China, but are they in a position to condemn it when they adhered to the laws for 4 years. Most are of the opinion that Google are no better than the rest of the companies who filter their sites and block content from the people of China (Ingram, 2010).

There have been countless cases brought into the court room in China dealing specifically with the Internet censorship laws. The following are two which were convicted with the aid of the Yahoo Corporation. Wang Xiaoning, a 57 year old engineer, kept an online journal which he used to express his opinions on corruption and as an aid to promote democracy within China. In 1999 Xiaoning's belongings were seized, without warrant, by the Chinese Public Security Bureau while citing a “violation of administrative laws.” But Xiaoning did not stop there; he continued to post his journals online using Yahoo Groups, among other online methods, in order to circulate them. Yahoo soon took note of his Yahoo Group activity and banned him from using it for circulating his journals. Undeterred by this ban Xiaoning sent several copies of his journals to members of the Yahoo Group through private email address, as well as some foreign websites. Yahoo gave the Chinese police his email address along with evidence of his activities on Yahoo Group, afterward in 2002 Xiaoning had his email records and computer files taken from him by the Public Security Bureau. He was subsequently arrested and charged with "incitement to subvert state power," then sentenced to 10 years of imprisonment where he has been subject to physical torture . Xiaoning appealed his sentence in 2004 but it was rejected (Kwan, 2007).

2004 saw Shi Tao, a 37 year old journalist who worked for the Contemporary Business News, was arrested for giving away state secrets to an organization outside of China. He had sent an e-mail to various overseas websites a copy of a text message, which was originally from the Chinese police, informing them of the risks and outcomes of writing about the 15th anniversary of the Tiananmen Square Massacre. The information of this illegal activity came to light when Yahoo supplied the Chinese authorities with evidence which aided in his conviction. Tao was tried in court, found guilty and later sentenced to ten years in prison. (BBC News, 2005). According to BBC News (2005), in both cases the Yahoo Corporation aided the Chinese Government in the conviction of these men. Subsequently Yahoo was sued by the families of both men. With Congress critiquing them gravely, Yahoo eventually settled the cases outside of court. They have also vowed to assist in releasing Xiaoning and Tao from prison.

The 28th of December 2012 saw the passing of yet another legislation to strengthen the countries Internet censorship law. This particular law is aimed specifically at the companies and the Internet sites, and to prevent online anonymity. It states that telecommunication companies have now choice but to get a hold of the identification of its new clients, this is so that the government can keep track of each individuals activity and an activity dubbed as criminal can be immediately trace back to the customer of the 'abused' service. This is also extended to websites such as Sina Weibo, who are a micro-blogging site similar to twitter. Users of these sites would often register with a pseudonym in order to mask their identity in an attempt to avoid state penalties. Any activity which is deemed illegal is to be deleted, and immediately reported to the government alone with records of the offence along with detailed records of the offender. This crackdown has been related to the huge role the social networking played in the 2011 revolutionary commotions in Tunisia and Egypt (Morrow, 2013).

FUTURE RESEARCH DIRECTIONS

All of this bad international press toward the Chinese Government and multinational companies does not seem to bother the CCP in the slightest, and why would it when they can prevent their own citizens from knowing about it. The government not only prevents the people of China from having an unlimited search engine, they also employ ghost-writers who earn their pay by posting pro-CCP and pro-Chinese Government content online, none of which will be censored or filtered. It is not a fair statement to say that the Chinese Government are afraid of the Internet . They have made, and are continuing to make, efforts to spread broadband to the furthest corners of China. They have in fact moulded the Internet into a tool that they can use to their advantage. Although the Internet is generally thought of as a democratizing tool, the Chinese Government have certainly shown how this can be completely false (Lynch, 2011).

CONCLUSION

It seems evident that Internet censorship laws in China are continuing to grow. With the government having introduced new laws in 2013 which are there to be able to keep track online users, you might wonder if there is any sign of China's Internet censoring ending. Although large companies such as Cisco, Yahoo, Google are all complying with the countries regulations and aiding them in their increased monitoring and repression of their people, there is always hope. The Internet is such a great tool that no one government can deny an entire country its freedom of speech or freedom of information. Billions are pumped into the country's censorship every year yet people still manage to surf the web anonymously, they still manage to gain access to blocked sites with the use of proxy's. Alas for now the government of China have the upper hand and are winning the battle of Internet censorship.

REFERENCES

Bennett, I. (2013). Media Censorship in China. Retrieved from http://www.cfr.org/china/media-censorship-china/p11515.

Cherry, S. (2005). The Net Effect: as China's Internet gets a much-needed make over will the new network promote freedom or curtail it? *Spertrum, 42*(6), 38-44. IEEE. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1437036

Ho, J. C. Zhang, & Lee. (2011). Google's retreat from China: Two competing theories. In *Proceedings of Technology Management in the Energy Smart World (PICMET)* (pp. 1-8). Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6017804

Human Rights Watch. (2001). Freedom of Expression and the Internet in China.

Human Rights Watch Backgrounder. (2013). Retrieved from http://www.hrw.org/legacy/backgrounder/asia/china-bck-0701.htm

Ingram, M. (2010). Google and China: What You Need to Know. Retrieved from http://gigaom.com/2010/03/25/google-and-china-what-you-need-to-know/.

Kwan, V. (2007). Prisoner Profile: Wang Xiaoning. Retrieved from http://hrichina.org/sites/default/files/oldsite/PDFs/CRF.3.2006/CRF-2006-3_WangXiaoning.pdf

Lynch, E. M. (2011). This is Not Your Daddy's China – Or Is It? Retrieved from http://chinalawandpolicy.com/2011/11/24/this-is-not-your-daddy%E2%80%99s-china-%E2%80%93-or-is-it/

Morrow, W. (2013). Chinese government imposes new Internet censorship law. Retrieved from https://www.wsws.org/en/articles/2013/01/07/chin-j07.html

News, B. B. C. (2005). Yahoo 'helped jail China writer'. Retrieved from http://news.bbc.co.uk/2/hi/asia-pacific/4221538.stm.

Zittrain, J., & Edelman, B. (2003). Internet Filtering in China. *Internet Computing, 7*(2), 70-77. IEEE. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1189191

ADDITIONAL READING

Abbott, J. P. (2004). *The Political Economy of the Internet in Asia and the Pacific Digital Divides, Economic Competitiveness, and Security Challenges*. New York: Praeger.

Amnesty (2008) "What is Internet censorship? Amnesty International Australia. 28 March 2008.

Bradsher, K. (2008). "China Blocks Access to the Times's Web Site." The New York Times.

Goldman, M. G. Gu, Edward X. (2004). Chinese Intellectuals between State and Market. Routledge publishing. ISBN 0-415-32597-8

Goldsmith, J. L., & Wu, T. (2006). *Who Controls the Internet? Illusions of a Borderless World* (p. 91). Oxford University Press.

Guan, S. (1995). *Intercultural communication*. Beijing: Beijing University Press. (in Chinese)

Jackob, D. (2008). *Background: Firewall of Shame*. Global Internet Freedom Consortium.

MacKinnon, R. (2008). Flatter world and thicker walls? Blogs, censorship and civic discourse in China [Springer]. *Public Choice*, *134*, 31–46. doi:10.1007/s11127-007-9199-0

Qiu, J. L. (1999). Virtual Censorship in China:Keeping the Gate Between the Cyberspaces. *International Journal of Communications Law and Policy.*, *4*, 1999.

Taubman, G. (1998). A not-so world wide web: the Internet, China, and the challenges to non- democratic rule. *Political Communication*, *15*, 255–272. doi:10.1080/10584609809342369

Wu, Z. (2012) "Chinese Laws and Regulations Regarding Internet." Chinaeclaw.com.

Yu, M. (2012) "Inside China," Washington Times, 8 February 2012.

KEY TERMS AND DEFINITIONS

Computer Network Attacks: Denial-of-service attacks and attacks that deface opposition websites can produce the same result as other blocking techniques, preventing or limiting access to certain websites or other online services, although only for a limited period of time. This technique might be used during the lead up to an election or some other sensitive period. It is more frequently used by non-state actors seeking to disrupt services.

Connection Reset: If a previous TCP connection is blocked by the filter, future connection attempts from both sides can also be blocked for some variable amount of time. Depending on the location of the block, other users or websites may also be blocked, if the communication is routed through the blocking location. A circumvention method is to ignore the reset packet sent by the firewall.

Domain Name System (DNS) Filtering and Redirection: Blocked domain names are not resolved, or an incorrect IP address is returned via DNS hijacking or other means. This affects all IP-based protocols such as HTTP, FTP and POP. A typical circumvention method is to find an Alternative DNS root that resolves domain names correctly, but domain name servers are subject to blockage as well, especially IP address blocking.

Internet Censorship: The control or suppression of what can be accessed, published, or viewed on the Internet. It may be carried out by governments or by private organizations at the behest of government, regulators, or on their own initiative. Individuals and organizations may engage in self-censorship for moral, religious, or business reasons, to conform to societal norms, due to intimidation, or out of fear of legal or other consequence.

Internet Protocol (IP) Address Blocking: Access to a certain IP address is denied. If the target Web site is hosted in a shared hosting server, all websites on the same server will be blocked. This affects IP-based protocols such as HTTP, FTP and POP.

Network Disconnection: A technically simpler method of Internet censorship is to completely cut off all routers, either by software or by hardware (turning off machines, pulling out cables) e.g. Egypt in 2011.

Over- and Under-Blocking: Technical censorship techniques are subject to both over- and under-blocking since it is often impossible to always block exactly the targeted content without blocking other permissible material or allowing some access to targeted material and so providing more or less protection than desired.

Packet Filtering: Terminate TCP packet transmissions when a certain number of controversial keywords are detected. This affects all TCP-based protocols such as HTTP, FTP and POP, but Search engine results pages are more likely to be censored.

Portal Censorship and Search Result Removal: Major portals, including search engines, may exclude web sites that they would ordinarily include. This renders a site invisible to people who do not know where to find it.

Splinternet: The term sometimes used to describe the effects of national firewalls. The verb “rivercrab” colloquially refers to censorship of the Internet, particularly in Asia.

Uniform Resource Locator Filtering: URL strings are scanned for target keywords regardless of the domain name specified in the URL. This affects the HTTP protocol. Typical circumvention methods are to use escaped characters in the URL, or to use encrypted protocols such as VPN and TLS/SSL.