Circumventing Internet Surveillance and Censorship

By Stephen Slaughter

Drexel University
Dr. Robert Allen
INFO 614
Certification

This paper is entirely my own work.
I have not quoted the words for any other person for a printed source or a website without indicating what has been quoted and providing an appropriate citation.
I have not submitted this paper/project to satisfy the requirements of any other course.
Certification (your name here): _Stephen W. Slaughter

Freedom of Opinion and Expression: A human right?

On December 10, 1948, the United Nations developed a standard of achievement for all governments and people around the world; this was called The Universal Declaration of Human Rights. It called on all member countries to adopt this standard, integrate it into legislation, and display it in schools and other public places. The intent of this Declaration was to infuse the public good with universally agreed upon human rights values. These values were comprehensive and covered most aspects of the rights thought by most people as crucial to freedom, dignity, and the pursuit of happiness. Article 19 of the Declaration is particularly germane to this research paper because it mandates that all people should have the human right to express their opinions and exchange information through any media without interference. Although the Internet was not developed until several decades later in history, the intent is thought to include exchanging information through the Internet (G.A.U.N., 1948). Although this document has been elaborated in many subsequent international treaties, and is binding for
all member states of the United Nations, it has been criticized by many Islamic countries. According to Islamic leaders, the declaration fails to take into account the religious and cultural context of Islamic society. Indeed, some of the most egregious violations of the universal right of freedom of expression in the form of Internet censorship that have occurred in recent history have occurred in Islamic countries.

Most people who have lived in democratic countries appreciate the inherent value of the right to expression without interference. We consider this an essential right which should be exercised to the maximum extent possible given its critical role in democracy; how else can the body politic engage in political discourse but through media? For the purposes of this research, we will assume the position that human rights as expressed in the Declaration produced by the UN in 1948 is valid, credible, and should be upheld; as such, article 19 and the right to freedom of expression without interference should be considered an inalienable human right. Consequently, this position implies that Internet censorship and some forms of surveillance is an abuse of human rights.

**Internet Censorship and Surveillance: Where does it occur?**

Recent events involving Internet censorship have been focused in the Middle East, but censorship also occurs in many far eastern countries. Mild forms of censorship and surveillance can even be found in Western democracies. In 2010, Reporters without Borders identified 13 nation states as the worst “enemies of the Internet.” This list of 13 includes Burma, China, Cuba, Egypt, Iran, North Korea, Saudi Arabia, Syria, Tunisia, Turkmenistan, Uzbekistan, and Vietnam. Up to 60 different countries have been identified as engaging in surveillance and censorship, albeit in less severe forms than what is found in this list of 13 worst violators. While the Internet offers many spaces for discussion and information sharing in social networks such as Twitter and Face book- which can and have facilitated the mobilization of protests- these repressive governments have engaged in ubiquitous surveillance and ID registration which compromises the ability of citizens to protest the repressive state of their governments. More and more states
are considering repressive laws which curtail use of the Internet, and this seems to occur most in states which are considered in the west to be less than “free” (Morillon, 2010). A few countries known worldwide as democracies are engaging in censorship tactics, namely, Australia and South Korea. Australia is planning to implement an ISP-level filtering system, and already has a regulatory regime which includes a “black-list” of overseas websites (Australia, 2000). In 2001, South Korea passed an Internet content-filtering ordinance, which censors the country’s Internet content. Indeed, even the United States, leader of the free world, conducts internet surveillance. The occurrence of internet censorship and surveillance in democratic nation states is particularly disturbing, but pales in comparison to China’s massive effort at censoring the internet through its $700B Golden Shield Project, which is colloquially known around the world as, “The Great Firewall of China.” China’s censorship effort represents the largest network firewall in the world; it includes a technical layer which the government invested billions into building routers and other infrastructure to filter, monitor, and block websites and look into how people communicate (and determine what they are talking about). The second layer of this firewall system is a social layer, which is composed of thousands of human censors who work in large warehouse buildings, constantly monitoring and tracking people’s activities online. Some suggest a third layer is implemented to censor the internet, namely, a psychological layer which is induced in ordinary citizens through their awareness of internet monitoring and policing, and results in people self-censoring their own opinions and discussions on the internet due to fear of being tracked by the censorship system (Nie, 2010).

Internet Surveillance and Censorship: methods and tactics.

More often than not, the governments which prove to be the worst offenders in terms of censorship tend to be rather authoritarian, and they use powerful and compelling arguments such as “protecting the welfare of children,” “preserving intellectual property rights,” and “protecting national security,” as the impetus for employing extensive filtering practices to fight the perceived chaos of the internet. Indeed, without filters of any kind, the internet can be seen as
the virtual wild-wild West of the early United States. While some forms of censorship and surveillance on behalf of the government are universally agreed to be justified and ethical (e.g. monitoring for terrorist activities or child pornography), other forms of censorship can be quite controversial.

Four commonly used tactics exist to censor internet communications: IP blocking, DNS tampering, keyword block filtering, and stateful traffic analysis. These methods are used to prevent access to specific web resources (i.e. web pages, IP addresses, and domains) considered to be subversive of the sociological, security, and economic interests stated above. The most direct way to prevent access to restricted content is to block the IP address of servers hosting this content. Alternatively, keyword blocking monitors the content of the traffic for certain keywords which identify the content as restricted. Stateful traffic analysis involves examining all the content which passes through a router and storing information about the state of this traffic, in order to piece together content which may be restricted and block it (Roberts, 2007). These methods are implemented most often when the server which hosts the offending website is located outside of the government's legal jurisdiction (e.g. Chinese government blocking access to Facebook, whose server farms are located outside of mainland China). However, when an offending site is located within the government's jurisdiction, the authorities use their legal authority to force the host to take the website containing sensitive content down. It also occurs that some companies (e.g. Google.cn) have worked with governments to remove websites they deem subversive from search results; this technique does not block access to the website (although the government may, in addition, block it using one of the methods mentioned above), but rather makes these websites more difficult to locate. If the authorities have jurisdiction over the domain name servers, they can force the host of the DNS servers to deregister the site hosting the illegal content. This effectively makes the site hosting the illegal content invisible to web browsers because they can not translate the host name to an IP address without its registration in the DNS system (Roberts, 2007). The possible points of control where a government can
implement filtering and surveillance occurs at the internet-backbone level, ISP-level, institutional level, and at the individual computer level. It appears that many countries implement filtering at all of these levels as part of a comprehensive strategy. In terms of surveillance, the main method employed by governments to examine message contents is Deep Packet Inspection (DPI). In the United States, DPI is what ISPs use to conform to CALEA, the U.S. government-ordered Internet wire-tapping directive (U.S Congress, 1994). DPI devices are able to inspect traffic at layers 2 through 7 of the OSI model which renders information beyond the protocol headers (i.e. the packet payload) visible and capable of being examined. When DPI devices are able to look past the protocol header information, into the actual content of packets, they can determine which type of application is being used and can inspect the payload to identify and read the type of content contained inside (e.g. copyrighted music, unencrypted email). Since encrypting data is one way to prevent DPI devices from reading packet payloads, many governments, including the U.S. plan to legislate that any web service which offers encrypted communication services (e.g. hushmail) provide the government with the technological means to unencrypt the data if necessary (Kassner, 2008).

**Circumventing government Interference online: tools and methods**

Several methods and tools are widely available to netizens for bypassing internet censorship and surveillance; the tool or method you choose depends on the type of censorship and eavesdropping being implemented. Furthermore, these tools and methods range from simple and requiring little skill, to advanced in nature and requiring more technical knowledge to implement.

If you are not concerned about anyone detecting and monitoring your circumvention, the simple approach of using secure HTTP (if the site has enabled this feature and HTTPS is not being blocked) may allow you to access a blocked site. For instance, the Burmese government blocks [http://www.twitter.com](http://www.twitter.com), but [https://www.twitter.com](https://www.twitter.com) remains unblocked. Another basic technique which may work is to access the alternative mobile website created for smartphones;
for example, http://m.flicker.com may be accessible, while http://flicker.com is blocked in your
country. Another simple technique which may yield access to a blocked website is to search for
the cached web page, instead of the official page located at a blocked URL. Since you are
retrieving the page from the search engine's servers instead of the blocked website itself, you
may be able to access the page. Obviously this approach will not work in the case where the
search engine is working with your government and has removed blocked sites from search
results. You may also use an RSS aggregator to access news feeds from blocked websites which
publish RSS feeds, since the RSS aggregator will be accessing the blocked site (not you).

Since small ISPs with few subscribers may be subject to less scrutiny than larger
providers, using one of these small, alternative ISPs can mean unfiltered access. In the 2011
Egyptian revolt, it is believed that Noor DSL was one of the last ISPs to comply with the
shutdown order because it only serviced eight percent of the market (and its noncompliance went
unnoticed for awhile). During the Egyptian revolt several citizens were able to hook up their
dial-up modems to foreign ISPs and broadcast news about the political situation (DeLeon, 2011).
Many ISPs offer free subscriptions to netizens living in countries with several social and political
unrest.

Another basic approach used to circumvent censorship is performed using a web proxy.
A web proxy is like a web browser embedded inside a web page which displays a form where you
can input the URL of the site you'd like to visit. The web proxy then shows you the page,
without you having to access it directly (Calingaert, 2010.) Most of the links on the web page
will be rewritten by the proxy, so that when you click them, they will be accessed through the
proxy; however, some links will break out of the proxied connection due to design complexity.
Http://www.proxy.org contains a list of proxy websites, and you can find other lists of proxy
websites online. The problem with this approach is that many governments block the web pages
listing the proxies and/or the proxy websites themselves. Given this disadvantage, before a
proxy is identified by your government and blocked, the sensible approach is to use the proxy to
locate and learn how to use more advanced circumvention tools. Furthermore, unsecured proxies may leave your sensitive information visible to anyone eavesdropping on your packets (e.g. your passwords could be revealed).

Psiphon, an open-source web proxy platform was developed for people who have friends and family members living in countries whose governments censored the internet. Psiphon allowed these users to set up simple, home-based servers which provided encrypted, proxied access to blocked web pages. The design leveraged existing social and other trust relationships instead of publishing a public proxy list which can easily be found and blocked by the government. Only friends and family members of people who set up home-based psiphon servers would know the address of the proxy which reduced the odds it would be blocked. Psiphon's current cloud-based infrastructure allows its users to invite friends or family to use the service, without having to operate their own private proxy (Naone, 2007). Other proxy tools such as Sabzproxy, Freegate, Simurgh, and Ultrasurf provide similar circumvention.

One of the best options for circumvention is using a Virtual Private Network (VPN) to encrypt and tunnel internet traffic between yourself and another computer. A VPN can be used to tunnel all different kinds of internet services (e.g. email, IM, ftp, etc), and if the tunnel ends outside of the area being filtered, then your communication will appear to originate from the country where the VPN server is located to an outside observer (Lawson, 2010). SSL/TLS-based VPNs are simple to configure and provide a high-level of security. The main disadvantage of VPNs is that commercially available packages are well-known and may be blocked by your government. Every operating system on the PC market today offers a publicly available VPN system; one need only to download, install, and configure the client software, and then connect to the VPN server.

Re-routing systems such as Tor are effective tools for circumvention as well. The Tor second-generation onion routing network provides the means to anonymize your internet communications. Use of Tor makes tracing internet traffic—such as visiting a website or sending
an instant message- back to its origin more difficult. Tor is essentially a volunteer-run, open-source, free-of-charge network of relays which provide anonymity for its users by hiding the IP address of the sender and receiver at each intermediate step along the routing path. The messages you send through Tor are encrypted and passed through onion routing nodes; each node removes an encryption layer which reveals routing instructions, re-encrypts the message, and sends it to the next intermediate node (Dingeldine, 2004). The path taken to each node is unpredictable, sort of like how a person takes strange detours when he suspects a tail. Once a message exits the onion routing system and passes to the destination machine, the destination machine only knows the address of the exit node which passed the message to it- not the original sender's address. Onion routing is a great way to circumvent surveillance because an eavesdropper can not easily detect the sender and receiver of a message. The actual degree of anonymity provided by onion routing is increased as more participating routing nodes are added to the network while it is decreased by the number of compromised (i.e. nodes under the control of an eavesdropper) nodes (Dingeldine, 2004). While messages relayed through the Tor virtual circuit of intermediate onion routing nodes are encrypted, the plain-text message which passes from the exit node to the destination machine is not encrypted by design; thus, if encryption of the plain-text message once the communication exits the routing nodes is desired, end-to-end encryption such as TLS should be implemented. The Chinese government's Golden Shield firewall system successfully blocks the use of Tor within Chinese borders, but Tor is unblocked and can be used to anonymize communications in many countries. Compared to the VPN, Tor is less susceptible to analysis of the size and timing of encrypted data passing through its network (Lawson, 2010). One of the biggest disadvantages of Tor is that it slows down your internet connection speed dramatically; the same website which normally takes a split second to access without Tor running in the background can take 30 seconds to load in your browser when Tor is enabled.
Conclusion

While governments around the globe are working to censor and monitor internet communications, violating the basic human right of freedom of opinion and expression as defined by the United Nations in 1948, an independent movement of circumvention is growing in response which provides a myriad of methods and tools to bypass this interference. Governments use methods such as IP blocking, DNS tampering, keyword blocking, stateful traffic analysis, and Deep Packet Inspection to engage in censorship and surveillance. Netizens and internet activists have responded with proxies, VPNs, re-routing systems, and end-to-end encryption to circumvent government censorship and surveillance. Some observers note that even the highly sophisticated filtering and surveillance apparatus in China is largely unworkable, and is successfully being circumvented with counter-filtering practices by the decentralized movement of netizens (Lacharlie, 2002).

Bibliography


