A Taxonomy of Censors and Anti-Censors:
Part I–Impacts of Internet Censorship

Christopher S. Leberknight, Princeton University, USA

Mung Chiang, Princeton University, USA

Felix Ming Fai Wong, Princeton University, USA

ABSTRACT

The tug-of-war on the Internet between censor and anti-censor technologies is intensifying. With an aim to raise awareness on Internet censorship and its circumvention, this paper and its companion Part II present a conceptual study of Internet censorship and anti-censorship. This first paper focuses on Internet censorship. It outlines an historical account of censorship through the lens of news coverage in the past decade, and presents a taxonomy of the principles, techniques, and technologies of Internet censorship. The interplay between social, political, and technological factors is presented to highlight the challenges in anti-censorship. Part II of the paper focuses on anti-censorship.

Keywords: *Anti-Censorship, Circumvention Technology, Filtering, Internet Censorship, Taxonomy*

1. INTRODUCTION

The Internet provides access to increasingly indispensible sources of information, yet it is censored almost everywhere and severely censored in a few countries. *Censorship* is defined as the institution, system or practice of reading communication and deleting material considered sensitive or harmful ("Censor," 2011; "Censorship," 2011). Throughout history, various methods of censorship have been used to reinforce specific religious and political agendas. Even though technological advancement often ameliorates the inefficiencies and limitations of the past, it is often suppressed through advances in censoring methods. The invention of the printing press in Europe in the 15th century is a prime example. The printing press increased the spread of information and knowledge, but it also faced increased degree of censorship. The task of maintaining effective censorship policies is undergoing rapid change due to the growth and diversity of different devices and networks including:

- Web traffic, Email (e.g., Gmail)
- P2P file-sharing (e.g., BitTorrent)
- Video (e.g., YouTube)
- Texting and messaging (e.g., Twitter)

DOI: 10.4018/jep.2012040104

- VoIP (e.g., Skype)
- Social Networks (e.g., Facebook)

While various media have been used in the past to communicate and inform the public of current events, none is as formidable to oppressive regimes as the Internet. For example, the printing press helped to spread information by accelerating the publication and dissemination of books and newspapers, while radio and television broadcasting facilitated the rapid communication of events and helped to expand overall news coverage. However, the Internet enables a much more rapid generation and spread of information and ideas compared to previous technologies. In addition, the inherent characteristics of the Internet make controlling information on the network extremely challenging. One factor is that national borders are more permeable online: residents of a country that ban certain information can find it on websites hosted outside the country (Wikipedia, n. d.).

Another major factor that makes online information especially difficult to control has to do with the fundamental design and objective of the Internet. The initial requirement for the Internet was to design a distributed system that was secure and would be less susceptible to failure and damage from a single point of failure. The very nature and advantage of a distributed system is that in the event that there is some damage or failure in the network, transmission can be routed around the damage. In addition, to allow for communication between different systems a set of standard protocols had to be developed to ensure interoperability. As a result, characteristics such as robustness which make the Internet an ideal platform for communication and dissemination of information also make it very difficult medium on which to regulate the spread and access of information. The combination of the ability to rapidly generate and share new ideas coupled with the complexity of controlling information flow, creates a viral effect which can, for example, spur social change. This phenomenon is especially significant if the information being exchanged contains content that may induce collective action and free thought. As a result, Internet censorship, which is defined as the control or suppression of the publishing or accessing of information on the Internet (Wikipedia, n. d.) has been steadily increasing in several countries.

Even though censoring information on the Internet may be more difficult compared to other forms of media, several techniques have been developed and are in use in many societies such as China, Iran, and Syria. Some recent events involving Internet censorship have also occurred in Iran, Tunisia and Egypt. In June 2009, the Iranian government headed by President Mahmoud Ahmadinejad blocked several websites and text messages to deter protesters supporting Presidential candidate Mir Hussein Moussavi (Chen, 2011). The popular social networking site, Twitter, was widely used by Iranian citizens to circumvent censorship to communicate current events outside of Iran. In October 2010, the Chinese "Great Firewall" obstructed the spread of the news that Liu Xiaobo, imprisoned for his activities for democracy in the country, received the Nobel Peace Prize, in recognition of "his long and nonviolent struggle for fundamental human rights in China" ("Liu Xiaobo", 2010). Another case of Internet censorship that took place amidst presidential elections occurred in January 2011, when the Tunisian government selectively blocked many sites during the political uprising against existing President Zine el-Albidine Ben Aliin.

While these three examples underscore the impact of using the Internet to precipitate social change, perhaps the most prominent and extreme form of Internet censorship occurred in Egypt on January 28, 2011. In response to political unrest, the Egyptian government shut down Internet connections for several days "…Citizens in Egypt were able to use satellite communications, Twitter feeds, and land lines to continue to communicate outside of the country" (Chen, 2011). While this event marks one of the most recent drastic measures to control the flow of information, many oppressive regimes that have blocked Internet services for political purposes are continuing to investigate new approaches to censoring the Internet.

Currently, the debate on Internet censorship continues as citizens in countries such as Turkey have begun to protest their government's new Internet filtering policy which would require Internet service providers to offer consumers four choices for filtering the Internet that would limit access to many sites, beginning in August. The policy also extends to banning the use of dozens of casual words on the Internet, like "girl," "partner" and "animal (Arsu, 2011).

The United States is taking a several measures to promote Internet freedom throughout the world. In response to the 2009 Iranian protests, the U.S. State Department asked Twitter to delay an upgrade in support of Iranians using the service to protest the presidential election. Events of such magnitude involving online censorship that limits the freedom of expression have prompted the U.S State Department to make unrestricted access to the Internet a top foreign-policy priority (Gorman, 2010). This move by the U.S. State Department marks a critical turning point in U.S. foreign policy which has taken several years to emerge due in part to many technological efforts.

To highlight the interplay between technology and policy relating to online censorship a list of U.S. polices (Ultrareach Internet Corporation, 2008) and the release of popular circumvention technologies is presented in Table 1. The data in Table 1 provides a timeline and side-by-side comparison of different technological advancements and efforts to crystallize political support. Based on the data in Table 1, significant political support and funding addressing online censorship issues was not achieved until 2009. This is a major milestone because even though there have been previous policies addressing censorship, adequate funding had yet to be awarded. This suggests that in 2009 Internet censorship became an important part of the U.S. political agenda. Consequently, government backed funding for anti-censorship projects and technologies will greatly improve the success and sustainability for efforts and technologies aimed at defeating online censorship. Most recently, in February 2011, the U.S. State Department announced a new policy to finance circumvention services (Landler & Knowlton, 2011).

The interplay between the technological forces that promote anti-censorship and the policies used to enforce censorship is the main focus of this paper. Specifically, the objective of this work is to increase awareness of the ramifications and negative consequences of Internet censorship and to advance the state of the art of circumvention technologies. The rest of this paper is organized as follows. First, in Section 2, an historical account of censorship policies and a discussion of the impact of censorship on international trade are presented. Second, an analysis of current trends and news coverage of Internet censorship is provided in Section 3.

Third, a taxonomy of Internet censorship technologies followed by concluding remarks are discussed in Sections 4 and 5, respectively. Discussion of anti-censorship is presented in the second part of the paper. Through the discussion of these four main points we present two open questions.

1. What metrics can be used to quantify the efficacy of current Internet censorship technologies?
2. Are there fundamental limits to existing Internet censorship technologies?

Among the three main steps of censorship and its circumvention, (1) monitoring and surveillance, (2) blocking, filtering, and modifying content, (3) recording events, we will focus mostly on blocking, filtering, and modifying content in this paper.

2. PREVIOUS RESEARCH

Censorship has affected many facets of social, political, and religious life. It has served as a vehicle to enforce segregation during the Apartheid in South Africa and as an instrument to promote racism and extremism by Nazi Germany during WWII. Several policies have been developed to regulate the flow of information.

Table 1. US policies and release of circumvention technologies

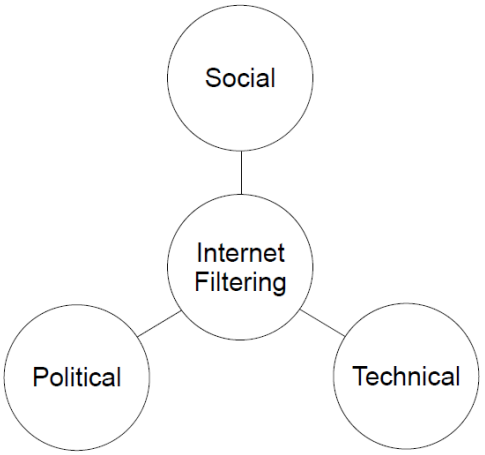
U.S. Policy (US Congress)	Year	Technology (Initial Release)
• US House Policy: Bipartisan, Bicameral Bill Stops Internet Jamming- October 2, 2002	2002	Anonymizer Anonymous Surfing, **UltraSurf**, Dynaweb
• US House Policy: Tear Down This Firewall - September 19, 2002	2002	Anonymizer Anonymous Surfing, UltraSurf, Dynaweb
• US House Representative Cox: House Passes Global Internet Freedom - July 16, 2003 •	2006	**GPass**, **Firephoenix**, Psiphon, Twitter
• US-China Economic and Security Review Commission: SARS in China: Implications for Information Control, Internet Censorship, and The Economy - June 5, 2003 •	2007	JAP, **GTunnel**
• 108th US Senate: Global Internet Freedom Act of 2003 - June 4, 2003	2008	
• 108th US House: Global Internet Freedom Act - HR 48 - January 7, 2003	2003	Circumventor
• Secretary of State Establishes New Global Internet Freedom Task Force - Feb 14, 2006	2006	GPass, Firephoenix, Psiphon, Twitter
• Global Online Freedom Act of 2007 - Dec 10, 2007	2007	JAP, GTunnel
• Testimony of GIFC in the US Senate Hearing on Global Internet Freedom (2008-05-20)	2008	
• U.S. State Department speaks to Twitter over Iran | Reuters - Jun 16, 2009		
• Senators Push Digital Code of Conduct Forbes – Jun 25, 2009		
• US to increase funding for 'hackivists' aiding Iranians - The Boston…Boston Globe – Jul 26, 2010		
• US Supreme Court backs free speech on the Internet Seattle Times – Jan 22, 2009	2009	
• POLITICS BLOG: Senators announce formation of Global Internet Freedom Caucus-Mar 24, 2010		
• US Government Works to Break Down Virtual Walls-Mar 19, 2010	2010	AnonymizerUniversal, Xi Xang Project (first anti-censorship technology software developed in China)

However, the globalization or democratization of information and the growing number of censorship-related issues raises concern for international trade. This section addresses these two issues, providing a brief review of censorship policies followed by a discussion of some of the implications of censorship on international trade.

A. Public Policy

No government allows free communication of *all* information. But the crucial differences between oppressive regimes and democratic ones are many, including the following factors: (1) the government is legitimately elected by the people, (2) there is a fundamental respect for freedom of expression, and (3) the laws concerning the regulation of information are

Figure 1. Three aspects of Internet censorship



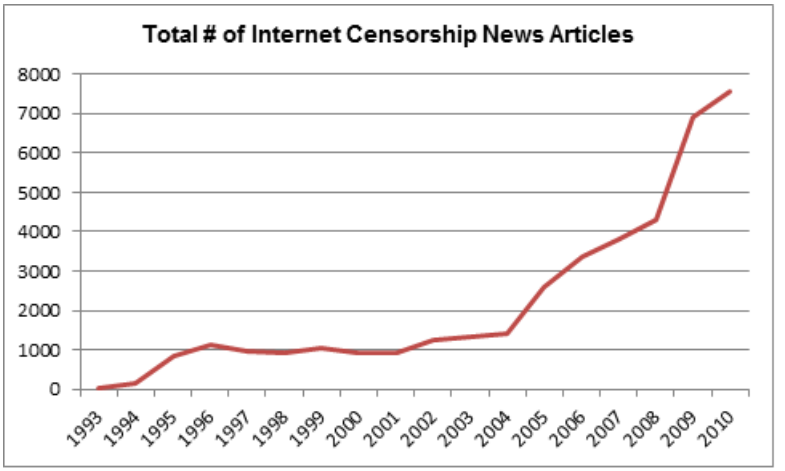
results of a check-and-balance system and enforced through the rule of law.

In the U.S., the Freedom of Information Act was intended to limit government control of information, but the statute has not ensured disclosure of all important governmental practices and decisions (Davis, 1978). Claims that the first amendment guarantees a right of access to information held by government have usually been rejected (Pell vs. Pecunier, 1974). The practice of withholding information when important public policies so require is nothing new; however, an important strand in American tradition leads in the opposite direction. Woodrow Wilson, for example, wrote that "government ought to be all outside and no inside.... [T]here ought to be no place where anything can be done that everybody does not know about." (Sunstein, 1996; Wilson, 1913) Woodrow Wilson's statement signified a shift to a more open government and many societies in the world have adopted and are in favor of Article 19 in the Universal Declaration of Human Rights (United Nations Declaration of Human Rights, 1948), which proclaims that everyone has the right of freedom of opinion and expression. However, many countries are in violation of Article 19 and actively engage in censoring information to control free exchange of ideas. The rise of the Internet has only heightened this activity. Just as the printing press may have been the catalyst for increased censorship in the past, the Internet is the modern day equivalent.

B. Implication for International Trade

While there are many examples of social inequities brought about by Internet censorship (Amnesty International, 2006; Freedom House, 2009; OpenNet Initiative, 2009) and even though all of these issues are causes for concern, one area that has received less coverage, and is becoming increasingly critical, is the implication of censorship on international trade. Essentially, by censoring online information domestic organizations can effectively discriminate against foreign suppliers (Erixon & Lee-Makiyama, 2010). For example, Google's decision to withdraw operations from China was due in part to non-compliance with Chinese censorship policies. Specifically, Google claimed that an organization which prides itself on being a source for information, cannot rightfully adopt a policy which enforces censorship. This clash between Google and Chinese authorities culminated with Google's decision to cease business operations in China on March 22, 2010 (Helft & Barboza, 2010). However,

Figure 2. Online news of Internet censorship



even though China insisted that Google must comply with Chinese censorship policies by blocking access to certain objectionable content, the Chinese search engine Baidu, often returns the same content as Google would have done. Therefore, it seems the use of online censorship to oust foreign competition may be another factor in play.

Furthermore a study published in 2009 by the European Centre for International Political Economy (ECIPE) concluded that after examining the World Trade Organization's (WTO) official regulations and the current status of Internet censorship in various countries, the WTO has a strong case against governments involved in blanket Internet censorship. Blanket Internet censorship, or disproportionate censorship, involves permanent bans and entire blockages of websites (Brian & Lee-Makiyama, 2009). The report by the ECIPE (Brian & Lee-Makiyama, 2009) and the events surrounding Google's withdraw from China underscores the increasing importance and impact of online censorship not only on international trade but also on foreign policy.

These two examples as well as the crackdown on Internet communications during the Iranian elections in 2009 have prompted the United States State Department to make unrestricted access to the Internet a top foreign-policy priority (Gorman, 2010). This new doctrine in addition to the surge in news coverage provides ample evidence that the future and spread of Internet censorship is a cause of great concern. This is not only a concern for citizens governed by authoritarian regimes, but there is also evidence which suggests online censorship is spreading to more liberal societies as well ("Joining China and Iran, Australia to filter Internet," 2009).

To further illustrate the prevalence of Internet censorship an analysis of news articles was extracted from http://news.google.com. The results in Section 3, Figure 2, depict the number of news articles containing the keyword "internet censorship" during a 17 year period from January 1993 to January 2010. The reports which indicate that China maintains the most advanced and sophisticated censorship network (Freedom House, 2009; OpenNet Initiative, 2009; Zittrain & Edelman, 2003) further underscore the broad reach and implication of Internet censorship. As the size of the Internet market grows and the contribution to the global economy becomes more pronounced online censorship will require both a technological and political solution.

While there have been many technological efforts and methods aimed at circumventing Internet censorship very few have had the ca-

pability to transform and influence public policy. That is, for circumvention or anti-censorship technologies to be truly effective it must be designed with the intention to not only provide free unrestricted access from a social perspective, but it must also be designed with the goal of transforming public policy. Internet censorship is a social, political and technical problem and each of these domains, depicted in Figure 1, interact in ways that can strongly reinforce one another. Therefore, some oppressive regimes have discovered that the successful implementation and sustainability of Internet censorship not only requires advanced technologies, but also requires social or self-censorship which can be enforced through harsh punishments and political ideologies which encourage acceptance of the status quo. Consequently, to defeat Internet censorship the same three structures must be attacked. The question is whether technology can serve as the catalyst to create a domino effect.

From a technological perspective there are two methods to destabilize information control. The first method requires that foreign supporters of anti-censorship lead in the technology evolution. However, this will only be a short term solution based on whether or not the anti-censorship community can financially sustain itself. This would be highly unlikely if not backed by government financing as Internet censorship is sponsored by oppressive regimes. Therefore, unless governments in favor of free speech and expression openly support and finance the destabilization of Internet censorship in foreign countries leading in the technology evolution will be difficult to realize because of the uneven playing field.

A more likely approach and technological solution may be to design technologies that maximize the cost to operate censorship networks or increase foreign awareness of the consequences of Internet censorship. This was accomplished during the Iranian elections in 2009 (Gorman, 2010) when Iranian citizens used YouTube and Twitter to bring images of violence and terror to the rest of world. With respect to increasing operational costs, based on the information in Figure 4, keyword censorship and stateful traffic analysis are the most expensive technologies to operate and therefore may lead to potential anti-censorship opportunities. Some underexplored anti-censorship technologies essential design characteristics will be discussed in Part II of this paper. However, to understand the role of technology as a vital part in the overall solution to Internet censorship a review of previous research is provided in the next section followed by a taxonomy of Internet censorship and anti-censorship technologies.

Figure 3. Search results with largest number of related articles

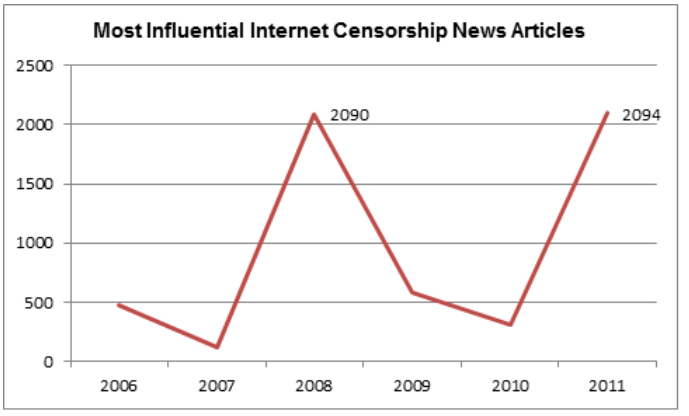
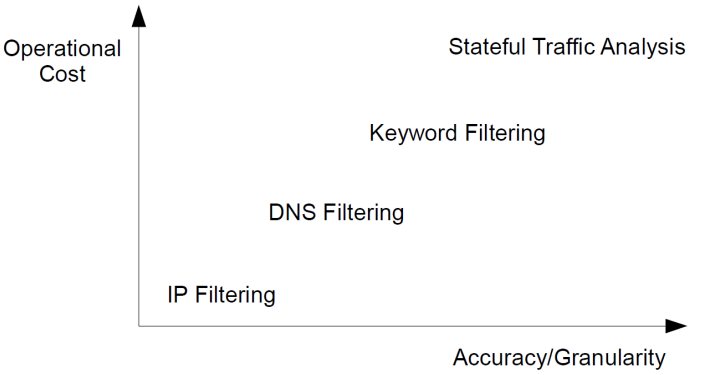


Figure 4. Internet filtering techniques



3. TRENDS IN INTERNET CENSORSHIP

To further illustrate the prevalence of Internet censorship an analysis of news articles was extracted from http://news.google.com. The results in Figure 2 depict the number of news articles containing the keyword "internet censorship" during an 18 1/2 year period from January 1993 to June 15 2011. The results illustrate that Internet censorship news coverage has been steadily increasing since 1993. Overall, it can be observed that the steepest ascent occurred between 2004 and 2011, which signifies the greatest impact of Internet censorship occurred within the last six years.

To examine this conjecture a bit deeper, the news articles which had the greatest number of related articles in the past 5 ½ years were extracted from the original data used to construct Figure 2. This data, depicted in Figure 3, was used to identify the most influential or popular topics on Internet censorship. Following similar techniques used to identify popular web sites based on the number of inbound links, we make the assumption that the articles with the greatest number of related articles are most likely more popular or influential compared to articles with less related articles. The diagram in Figure 3 and Table 2 provide deeper insight into the main topics of interest and the specific societies impacted by Internet censorship. A closer examination of these two figures combined with Table reveals some interesting results. First, based on the data in Table 2, it is clear that the overwhelming number of news articles on Internet censorship are all based on event in China.

Second, it can be observed that there are two measures of "importance" or "popularity". One is the number of articles during a given year and the other is the number of related articles. Even though the data in Figure 3 indicates a decline in the number of related articles for a given news story from 2008 to 2010, the data in Figure 2 suggests that overall more activity or articles on Internet censorship were published between 2006 and 2011 compared to any other previous time periods. Therefore, utilizing the data in both figures provides a means to understand the trend and identify impact on a case by case basis. For example, Figure 3 indicates that two peaks occurred in 2008 and 2011. These two data points correspond to Internet censorship news events in China. The first event describes the shift in Chinese policy to lift the imposed Internet censorship during the Olympic Games, while the second article describes how Google has been revealing government-backed cyber-warfare activities in China. According to the analysis based on news results obtained from news.google.com these two articles have captured more media attention than any other events in recent history. While

there may be some bias as to what Google reports based on their current relation with the Chinese government and it is also possible increase in the news coverage in recent years could be a by-product of an ever increasing digital world these results still do hint to many interesting conclusions.

For example, out of the top six articles in Table 2, it can be observed that the two main parties involved in the Internet technology revolution are the U.S. and China. In fact in approximately 50% of the most "influential" news articles, specifically in 2006, 2009 and 2010 the U.S. has either directly or indirectly responded to Internet censorship activities in China. The tug-of-war between U.S and Chinese policies on Internet freedom suggest that as the size of the Internet market grows and the contribution to the global economy becomes more pronounced, online censorship will require both a technological and political solution.

While there have been many technological efforts and methods aimed at circumventing Internet censorship very few have had the capability to transform and influence public policy. That is, for circumvention or anti-censorship technologies to be truly effective it must be designed with the intention to not only provide free unrestricted access from a social perspective, but it must also be designed with the goal of transforming public policy. Internet censorship is a social, political and technical problem and each of these domains, depicted in Figure 1, interact in ways that can strongly reinforce one another. Therefore, some oppressive regimes have discovered that the successful implementation and sustainability of Internet censorship not only requires advanced technologies, but also requires social or self-censorship which can be enforced through harsh punishments and political ideologies which encourage acceptance of the status quo. Consequently, to defeat Internet censorship the same three structures must be attacked. The question is whether technology can serve as the catalyst to create a domino effect.

4. INTERNET CENSORSHIP TAXONOMY

A. Principles

Internet censorship policies are primarily concerned with two main principles based on usability and censorship:

1. Limit the performance degradation
2. Enforce censors

The first principle is concerned with promoting usability. That is, the policy should attempt to censor information which may be disruptive to the status-quo without significant overhead or performance degradation. The second principle corresponds to achieving a certain level of accuracy with respect to restricting objectionable content. To achieve these

Table 2. Top news articles for 2006-2011

Title	Year	News Source	Related Articles
International: Bill Gates makes cryptic remark on internet rights	2006	MyBroadband	470
BBC Monitoring International Reports: China: Watchdog...	2007	BBC	117
Media Shift China Partially Lifts Great Firewall for…	2008	PBS	2090
Obama gives human rights, Internet censorship center stage	2009	Canada.com	582
Google executive calls for censorship trade rules	2010	MarketWatch	314
China Goes Phishing	2011	Wall Street Journal	2094

principles several the following eight criteria should be considered: "CCFFSSSR":

- *Cost:* both resource and opportunity cost, which directly impacts the availability of censors.
- *Circumventability:* how easily can the censors be disabled.
- *False negative:* the accuracy of censors.
- *False positive:* too high a false positive rate depletes the censor resources.
- *Scope:* the range of communication modes censored.
- *Scale:* the number of people and devices that can be simultaneously censored.
- *Speed:* the reaction time of censors.
- *Resolution:* the resolution at different levels, e.g., server, port, webpage, end user device, etc.

It is also important to realize that each bullet in the above list also presents an opportunity for the designers of anti-censorship systems.

B. Techniques

A review of relevant literature has revealed that the most prevalent use or practice of Internet censorship is primarily conducted in authoritarian regimes, such as China, Cuba, Iran, North Korea, Syria, and Tunisia (Palfrey, Roberts, & Zuckerman, 2009). Overall, it has been reported that China has the most advanced and sophisticated censor network (Palfrey, Roberts, & Zuckerman, 2009). These countries have employed several new policies and technologies aimed at controlling access to information on the Internet.

This section presents a taxonomy of Internet censorship technologies to help identify and explain the different strengths and weaknesses of various censorship strategies. The classification of existing censorship technologies can be used to explore new design opportunities for anti-censorship systems and stimulate future research to define the most appropriate metrics for quantifying performance an and stability. The taxonomy can be broadly categorized by attack mode, filtering method, and target which are used to achieve a certain level of digital censorship.

The attack mode defines the sources of interest within the network topology and an associated action. The source of interest within the network consists of (1) *nodes, (2) users, and (3) links*. The objective of a specific Internet censorship policy may identify an attack point and action within the network. For example, node attacks may consist of DoS, domain de-registrations or server takedown. To attack or censor a particular user the censorship organization may first decide to trace and record specific user activity prior to blocking any content. Therefore, there may be specific instances in which the operators of the censorship network wish to monitor and record activity as opposed to blocking or filtering specific content. Another mode of online censorship is to attack a link within the network, which can be accomplished using techniques such as IP blocking/filtering, DNS tampering, and/or HTTP proxy filtering.

With respect to filtering method, perhaps the most prevalent type of online censorship technology is a method known as IP filtering. IP filtering is used to block or filter objectionable content by restricting access to specific IP addresses. There are several different methods to filter content and while other oppressive regimes have utilized one or more methods, it has been reported that only China exercises all of them (Palfrey, Roberts, & Zuckerman, 2009). The most popular filtering methods are depicted in Figure 4, which contrasts the tradeoff between the different filtering techniques in terms of their accuracy versus their operational cost. For example, IP filtering is least costly to operate compared to stateful traffic analysis, but it does not provide a high degree of accuracy. Since many websites may be hosted on one IP address, blocking the IP address to restrict access to a particular website which contains objectionable content also blocks all other websites which may not contain objectionable content. IP blocking is simple and cheap to implement by providing routers with specific IP addresses to block.

However, it may unintentionally block websites containing valuable or useful information.

The next category in the taxonomy consists of the targets, which are comprised of the technological devices and networks to be censored. The decision to enforce a specific online censorship strategy is primarily influenced by the task to be performed on the device or network application. For example, depending on the specific context, the censorship organization may block a device or network based on whether it is used to access or publish digital content. Deciding which filtering method or strategy to employ is not only based on operational cost vs. accuracy as depicted in Figure 4, but it is also based on several other salient factors as summarized in the last section's bullet list.

C. Technologies

Unlike circumvention technologies there are not many commercially available censorship technologies. The technologies typically fall into two categories: hardware and software. Software based technologies are primarily used to filter and block content while hardware based technologies such as Deep Packet Inspection devices are used to classify network traffic and inspect packet headers and payloads. Much of the filtering software is proprietary and developed internally within organizations. However, there are some commercially available content filters such as Smartfilter which is developed by San Jose firm Secure Computing. In terms of hardware, several deep packet inspection devices are commercially available.

5. CONCLUSION

The two main objectives of this research are to provide an overview of online censorship including the interplay between technology and policy, and present a taxonomy of Internet censorship technologies. With respect to the first objective, a historical review of information control including the evolution into online censorship and the corresponding commercial applications demonstrates how censorship has been practiced and employed throughout the world as a social and political tool to control free thought and international trade. Many societies have reaped the benefits from technological advancements, however, in several totalitarian regimes, technology has often been perceived as a formidable opponent in the struggle to maintain the status quo. The intended benefits of new technologies are often met with unforeseen consequences. For example, technologies such as the printing press helped to streamline the publication and dissemination of information but it also inadvertently threatened closed societies who were intent on controlling which information should be allowed to proliferate. Throughout history there have been several other technologies which have improved communication and the spread of information. However, no single technology has posed as a great threat to authoritarian regimes as the Internet.

Second, in support of Internet freedom, this paper presents a taxonomy of censorship technologies along three dimensions: principles, techniques and technologies. This conceptual model can be used to design more robust and effective anti-censorship systems. Based on the analysis of online news articles in Section 3, Internet censorship has been steadily increasing since 1993 with the largest incline occurring between 2007 and 2010. While the U.S. has taken a strong position in promoting Internet freedom around the world, violations of basic human rights such as freedom of speech and expression still persists. In addition, the broader impact on international trade and associated policies underscores the criticality for interdisciplinary research which tackles Internet censorship on political, social, and technological levels.

REFERENCES

Amnesty International. (2006, July). *Undermining freedom of expression in China: The role of Yahoo! Microsoft and Google*. Retrieved from http://www.amnesty.org/en/library/info/POL30/026/2006

Arsu, S. (2011, May 15). Internet filters set off protests around Turkey. *The New York Times*. Retrieved from http://www.nytimes.com/2011/05/16/world/europe/16turkey.html

Brian, H., & Lee-Makiyama, H. (2009). *Protectionism online: Internet censorship and international trade law* (ECIPE Working Paper, No. 12/2009). Retrieved from http://www.ecipe.org/publications/ecipe-working-papers/protectionism-online-internet-censorship-and-international-trade-law/PDF

Censor. (n. d.). In *Merriam-Webster online dictionary*. Retrieved January 29, 2011, from http://www.merriam-webster.com/dictionary/censor

Censorship. (n. d.). In *Merriam-Webster online dictionary*. Retrieved January 29, 2011, from http://www.merriam-webster.com/dictionary/censorship

Chen, T. M. (2011). Governments and Executive "Internet Kill Switch." *IEEE Network*, *25*, 6–12. doi:10.1109/MNET.2011.5958002

Davis, K. C. (1978). *Administrative law treatise* (2nd ed.). San Diego, CA: K. C. Davis.

Erixon, F., & Lee-Makiyama, L. (2010, January 6). Chinese censorship equals protectionism. *The Wall Street Journal*. Retrieved from http://online.wsj.com/article/SB10001424052748704840426045746416209426685 90.html

Freedom House. (2009, April 1). *Freedom on the net: A global assessment of Internet and digital media*. Retrieved from http://www.freedomhouse.org/uploads/specialreports/NetFreedom2009/FreedomOnTheNet_FullReport.pdf

Gorman, S. (2010, January 20). Web access is new Clinton doctrine. *The Wall Street Journal*. Retrieved from http://online.wsj.com/article/SB10001424052748703405704575015461404882830.html

Helft, M., & Barboza, D. (2010, March 22). Google shuts China site in dispute over censorship. *The New York Times*. Retrieved from http://www.nytimes.com/2010/03/23/technology/23google.html

Joining China and Iran. Australia to filter Internet. (2009, December 15). *SkyNews*. Retrieved from http://www.foxnews.com/scitech/2009/12/15/like-china-iran-australia-filter-internet/

Krippendorff, K. (2004). *Content analysis: an introduction to its methodology* (2nd ed.). Thousand Oaks, CA: Sage.

Landler, M., & Knowlton, B. (2011, February 14). US policy to address Internet freedom. *The New York Times*. Retrieved from http://www.nytimes.com/2011/02/15/world/15clinton.html

Liu Xiaobo. (2010, December 10). *The New York Times*. Retrieved from http://topics.nytimes.com/top/reference/timestopics/people/l/liu_xiaobo/index.html

OpenNet Initiative. (2009, June 15). *Internet filtering in China*. Retrieved from http://opennet.net/sites/opennet.net/files/ONI_China_2009.pdf

Palfrey, J., Roberts, H., & Zuckerman, E. (2009, March). *2007 Circumvention landscape report: Methods, uses, and tools*. Retrieved from http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2007_Circumvention_Landscape.pdf

Pell v. Procunier, 417 U.S. 817 (1974).

Sunstein, C. R. (1986). Government control of information. *California Law Review*, *74*(3), 889–921. doi:10.2307/3480399

Ultrareach Internet Corporation. (2008, July 2). *Privacy, security and freedom: Background information*. Retrieved June 28, 2009, from http://www.ultrareach.com/background_en.htm

United Nations. (1948). *The universal declaration of human rights*. Retrieved January 31, 2011, from http://www.un.org/en/documents/udhr/index.shtml

Wikipedia. (n. d.). *Internet censorship*. Retrieved January 31, 2011, from http://en.wikipedia.org/wiki/Internet_censorship

Wilson, W. (1913). *The new freedom: A call for the emancipation of the generous energies of a people*. New York, NY: Doubleday, Page. Retrieved January 29, 2011, from Project Gutenberg website: http://www.gutenberg.org/files/14811/14811-h/14811-h.htm

Zittrain, J., & Ben, E. (2003). Internet filtering in China. *IEEE Internet Computing*, *7*(2), 70–77. doi:10.1109/MIC.2003.1189191

Christopher S. Leberknight - received the BA degree in Computer Science from Rutgers University, New Brunswick, NJ, the MS degree in Computer Science and the PhD degree in Information Systems from the New Jersey Institute of Technology (NJIT), Newark, NJ. He is currently a Postdoctoral Research Associate in the Department of Electrical Engineering at Princeton University. His primary research interests are in the technological applications and computational methods for modeling human behavior and decision making. In addition to his academic experience he also has over 10 years of industry experience as a systems engineer and technical systems manager. Dr. Leberknight is a member of the Association of Computing Machinery and the Association for Information Systems.

*Mung Chiang is a Professor of Electrical Engineering at Princeton University, and an affiliated faculty in Applied and Computational Mathematics, and in Computer Science. He received his BS (Hons.), MS, and PhD degrees from Stanford University in 1999, 2000, and 2003, respectively, and was an Assistant Professor 2003-2008 and an Associate Professor 2008-2011 at Princeton University. Chiang's research in networking received awards such as the IEEE Tomiyasu Award, PECASE, TR35, ONR YIP, NSF CAREER, Princeton Wentz Faculty Award, and several best paper awards. His inventions resulted in seven issued patents and several technology transfers to commercial adoption, and he founded the Princeton EDGE Lab in 2009. He is currently writing an undergraduate textbook "*20 Questions About the Networked Life*".*

Felix Ming Fai Wong received the B.Eng. degree in computer engineering from the Chinese University of Hong Kong, in 2007, and the MSc degree in computer science from the University of Toronto, in 2009. He is currently a PhD student in electrical engineering at Princeton University. His research interests are in computer networks and online social networks.