Communications of the IIMA

Volume 11 | Issue 2 Article 6

2011

The Growth of Global Internet Censorship and Circumvention: A Survey

Ramesh Subramanian
Quinnipiac University

The Growth of Global Internet Censorship and Circumvention: A Survey

Ramesh Subramanian
Quinnipiac University, USA
ramesh.subramanian@quinnipiac.edu

ABSTRACT

The Internet has, within a period of twenty years, become the primary medium of information exchange in the world. It is also arguably the primary source of information in the world. Search engines such as Google and Yahoo have made the vast trove of information available and accessible to everybody. Email and social network applications such as Facebook and Twitter have enabled people all over the world to meet, collaborate and participate in joint activities. The Internet has also gradually become a tool of dissidence in repressed nations all over the world - to spread information, plan and organize activists and conduct protests. Not surprisingly, repressive regimes see the Internet as a threat. Under the guise of protecting their citizens from the negative effects of the Internet (such as pornography and hate speech), they have, and are, actively curbed Internet use by their citizens by adopting various censorship measures and blockades.

In this paper I have surveyed the history of Internet censorship by various countries, starting from 1991. Governments all over the world use various means – legal, political, technical, and coercive – to control and restrict Internet content. Cataloging all such efforts by all the countries would be beyond the scope of this paper. Despite that, I have tried to focus on the various methods of censorship and blockades used by various countries around the world. I have also provided a brief description of recent attempts by Myanmar and Egypt to completely block the Internet, with a discussion of the technique and methods involved. Finally, I have also briefly discussed the push-back efforts by citizens of the world, who are actively and innovatively finding ways to circumvent the most pernicious of these censorship efforts and blockades.

Keywords: Internet, government control, global censorship, blockade, control, global technology policy, circumvention

INTRODUCTION: THE "OPEN" DESIGN OF THE INTERNET

The Internet was conceived as an open communications system which would enable academics to collaborate and exchange ideas and information without being tied to organizational and hierarchical constraints (Leiner et al., 2003). The original designers conceived the Internet as a highly redundant and inter-connected "network of networks" in which data communications would not be completely disrupted even if parts of the network were to go down. If there was a disruption in any part of the network, data packets would simply take alternate routes and networks to reach their destinations. The Internet became a household word in the 1990s, thanks to the development of the world-wide web (Web) by Tim Berners-Lee (n.d.) in 1989. Since then, the Web's ease of use has made it the most preferred medium of global flows of communication

among government, citizens and commercial enterprises. Hundreds of thousands of Web-based applications have been developed over time, and are used by an immense range of users, such as academics, students, children, computer gamers, senior citizens, those working in government agencies and NGOs, and even activists, dissidents and terrorists, just to name a few.

As the Web rapidly gained in popularity and usage during the early 1990s, social activists saw it as a medium for unfettered communication. In fact, many proponents of free speech and unrestricted communications were of the belief that the very design of the Internet would prevent any individual government from exercising control over it. In 1994, Dyson, Gilder, Keyworth, and Toffler, of the *Progress and Freedom Foundation,* released a ***manifesto*** of cyberspace, in which they stated some fundamental ideas of the governance of such a space. Langdon Winner (1997) termed their cyberspace philosophy as ***cyber-libertarianism***, which he explained as "a collection of ideas that links ecstatic enthusiasm for electronically mediated forms of living with radical, right wing libertarian ideas about the proper definition of freedom, social life, economics, and politics in the years to come" (para. 4). Notable cyber-libertarian spokesmen of that time included Nicholas Negroponte (Director of the *MIT Media Lab*), Stewart Brand (founder of the *Whole Earth Catalog*), Kevin Kelley (*Wired* magazine editor) and John Perry Barlow (co-founder of the *Electronic Freedom Foundation* and lyricist for *The Grateful Dead),* as noted by Langdon Winner and Alan Liu (2002). The early cyber-libertarians believed that the Internet should be a place which adhered to a set of common values and beliefs that should be allowed to function without any sort of governmental intervention.

The 1990s saw the global citizenry increasingly using the Internet for communications and commerce. Many of these early adopters embraced the libertarian notions of control of the Internet. It was thought that the Internet could continue to grow without any oversight, rules or laws imposed upon it by world governments. Even global commerce conducted over the Internet was thought to be exempt from government rules. The Internet was considered to be a parallel world where anarchy ruled, where the only rules, if at all they existed, were the result of consensus.

However, these early notions of a free and ungoverned Internet have proven to be illusory. Gradually, many national governments have found ways to control, censor, and govern the Internet. The case of Yahoo versus the French Government is an illustrative example of controls imposed upon free and unfettered commerce by a national government[1]. In fact, much of the Internet today is under the control of governments around the world. Governments have imposed laws, blockades and censorship under various guises, in the name of protecting commercial, national security and in some cases, cultural interests. Internet activists have reacted by developing means to circumvent the laws, blockades and censorship.

[1] Early Internet entrepreneurs like Jerry Yang of Yahoo embraced the cyber-libertarian view and firmly believed at the non-jurisdictional characteristic of the Internet. The reasoning was that since content could be located on any server anywhere in the globe, individual nations could not control such content. Thus, when Yahoo! faced a lawsuit in a French court against its policy of auctioning and selling Nazi memorabilia in April, 2000, Jerry Yang simply declared his view that "The French tribunal wants to impose a judgment in an area over which it has no control. (Goldsmith & Wu, 2006). Yang's notion was however, was proven wrong when a French judge ruled that Yahoo! had to find ways to stop providing access to materials deemed to be illegal inside French territory or face severe fines (Goldsmith & Wu, 2006).

In this paper I focus on the rise of Internet censorship and circumvention. The main objectives are to trace the history of Internet censorship over the last twenty years. I survey technologies and strategies employed by various governments, especially repressive governments, for Internet censorship. I also discuss the rise of dissidence and circumvention employed against censorship (i.e. the North African and Arab uprisings of 2010-2011). Finally I conclude with an analysis and suggestions for future work in this area.

The main questions I focus on are:

- What are the developments in governments' blockade and censorship of the Internet from the 1990s to the present?
- What are some recent blockades?
    - How are blockades accomplished?
    - Are there variations to the theme?
- What are "kill switches?"
    - Example of a simple kill switch implementation
- How have citizens and activists reacted to this?
    - What are some of the circumvention techniques used?

The methodology I have adopted is qualitative. I use published materials, news media publications, interviews and technical documents in developing the main ideas in the paper. I include case-studies, published literature, news items and analyses. I analyze all these materials in developing responses to the above questions.

GOVERNMENTAL CENSORSHIP OF THE INTERNET

The 1990s: Internet Control in its Nascent Stage

Today, there is evidence of at least some form of Internet censorship or blockade in most countries. The OpenNet Initiative (ONI), a collaborative partnership of the Citizen Lab at the Munk School of Global Affairs, University of Toronto; the Berkman Center for Internet & Society at Harvard University; and the SecDev Group (Ottawa), researches Internet filtering and surveillance practices in countries all over the world. The ONI (n.d.b) website provides country profiles of fifty countries with respect to Internet filtering. A complete discussion of all of these censorship efforts is beyond the scope of this paper. In the following, I narrow the scope and focus on some of the early attempts to regulate the Internet (i.e. in the 1990s), and then move to more recent attempts at blockading in countries around the world.

Early Attempts at Internet Censorship

Singapore

Active government censorship of the Internet began almost as soon as the Web came into existence. It is striking that as early as 1991, Singapore's National Computer Board began a study on how to effectively harness the power of the Information Technology for national development and improving the quality of life in Singapore. But in the same year, Singapore's

Ministry of Information and the Arts started a review of its censorship laws, with a view to including all media, including the nascent information and communications technologies (i.e. Internet) (Ang & Nadarajan, 1995). Singapore's censors decided to implement differentiated censorship levels: one level for the home, and one for commercial enterprises; one that differentiated access between the young and the old; and one that differentiated access between private and public use. The censoring authorities created a review board to review and censor, if necessary the contents of various USENET newsgroups[2]. An interesting aspect of the Singaporean censorship of the Internet is that, according to Ang and Nadarajan, the censorship seemed to have support from a majority of the general populace.

Comment: During the early years of the Web, it was quite common for Western commentators to look at Internet censorship efforts in Asian countries like Singapore as well as other countries in South-East Asia and conclude that citizens of these countries culturally preferred a certain level of censorship of communication media. This was no doubt perpetuated by the local media commentators of these countries, as well as clearly enunciated by the political leaders of these countries. It was the feeling of those times that the unregulated Internet presented a "wild West" that might have a corrupting influence on the developing countries in South-East Asia. Thus, most of the censorship was focused on pornography. Amy Knoll noted that the Singaporean censorship authorities read every e-mail and monitored USENET newsgroups (Knoll, 1996). *Individuals caught as a result of such monitoring were warned.*

China

Even during the nascent stages of the Internet, China was clearly conscious of the disruptive potential of the Internet. China looked up to Singapore's model to control the Internet content and eventually followed even stricter norms in exercising control. Right from the beginning, China allowed access only to certain newsgroups on the Usenet, namely the SCI and COMP newsgroups that dealt with science and computing subjects. Only a handful of government-approved Internet service providers could operate in the Chinese market. They were required to use filters to prevent pornography, as well as issues that were political and cultural (Ang, 1997).

Legal Scholar Amy Knoll noted that unlike Singapore, China did not have the advantage of having an English-speaking population. The language of the Internet was English, and provision for incorporating Mandarin characters was low. However, like Singapore, China realized the importance of the Internet, albeit for internal uses. In 1995, China started the China Education Research Network (CERNET). CERNET's main nodes were located at Tsinghua University, and regional network centers were located at the top-ten Chinese universities. In April, 1995, China opened the Internet to its citizens. However, the Chinese government was very particular to restrict general access to the Internet. The reasoning was that the government did not want its citizens to be too influenced by Western ideology and Western culture. The government also wanted to discourage public activism tending towards transition to a more democratic society. Finally, the government was also very concerned about the spread of and access to pornography spread through the Internet (Knoll, 1996).Therefore the Chinese government created several layers of bureaucratic control. First, the government tried to create an "Intranet" – i.e. internal access to all its citizens, while blocking external access. Second, the government strictly

[2] Ibid.

restricted flow of information from the outside through the China Internet Corporation, the first Chinese ISP, and a subsidiary of the official news agency Xinhua. All Internet providers, users and e-mail account holders were required to register with the police (Knoll, 1996). On January 2, 1996, the Xinhua News Agency published the "Interim Internet Management Rules" which laid out the conditions of and restrictions in Internet usage among citizens and businesses (Feir, 1997).

Myanmar (Burma)

Myanmar has been ruled by various authoritarian regimes since attaining independence from British rule in 1948. As early as 1996, *Financial Times* reporter Ted Bardacke noted the highly restrictive approaches taken by the military government with regards to access to the Internet. The regime's State Law and Order Restoration Council (SLORC) outlawed the possession of a computer with networking capability without proper authorization. Lengthy prison sentences of seven to fifteen years were imposed on anybody who obtained or sent information pertaining to state security, economy and national culture (Bardacke, 1996). However, Bardacke also noted that the impact of these rules on the Myanmar citizens was minimal, as almost nobody in the country could afford the extremely high costs of Internet connectivity (US $ 5/per minute). Moreover, Myanmar had (and continues to have) only two Internet service providers, Myanmar Teleport and the Ministry of Post and Telecommunication (MPT), both controlled by the government.

South Korea

South Korea (arguably a democracy) also took a very strong stance in controlling the Internet in the early 1990s. According to Ang (1997), South Korea was probably the first country to pass laws that controlled access to the Internet. The Electronic Communication and Business Law encompassed bulletin board services (BBSs), chat rooms, and other public domain services. Any material that was deemed to encroach on public morals, cause loss of national sovereignty, and harm youths' character, emotions and the sense of value was actively blocked. More importantly, contact with North Koreans, or expressions of sympathy towards North Korea on the Internet was prohibited.

The Middle-East

Iran opened to the Internet in 1992, when the Institute for Theoretical Physics and Mathematics was connected to Vienna through a link. This was earlier than other countries in the developing world (Sorensen, 1996). By 1995, many universities in Iran had Internet connectivity. However, the rulers of Iran soon saw the threat posed by unrestricted Internet access and in 1995, the Telecommunications Company of Iran disconnected Iran's only private Internet service provider (Wavell, 1995). Since that time, restrictions and censorship have increased exponentially, as noted in the next section.

With regards to Saudi Arabia, legal scholar Ari Staiman (1996) noted that the kingdom channeled all Internet access through one service provider, and also provided restricted access to hospitals and universities. Sorensen also noted that while Saudi Arabia cautiously opened up

Internet connectivity, it also closely watched its users, recording the site visits made by them, and scrutinizing those who downloaded or visited pornographic sites or participated in religious or political discussions deemed inappropriate by the rulers. The government also created a panel to study how the Internet could be regulated.

Other countries in the middle-east, such as Bahrain, Kuwait, the UAE and Morocco also joined the band-wagon of getting connected to the Internet, albeit with limitations. These countries provided Internet access only through government-run telecommunications companies, and also used filtering systems to restrict access to various sites (i.e. those with pornographic content, and those that discussed politics and religion) that were not approved.

Western Governments and Censorship

Attempts to exercise censorship of the Internet are not restricted only to authoritarian regimes or developing countries. During the early growth period of the Internet, many Western governments also seriously considered imposing certain restrictions. The objective was to restrict objectionable materials such as pornography and hate speech.

United States

On February 8, 1996, the Communications Decency Act (CDA) was signed into law by President Clinton. The CDA prohibits networked computer users from sending or displaying any material that was patently offensive and deemed indecent by community standards. However, activists decried the law as a violation of the right to free speech, and the potential for censorship that the law afforded. These included the Electronic Frontier Foundation (EFF) and the American Civil Liberties Union (ACLU). On June 12, 1996, a panel of Federal judges in Philadelphia blocked a part of the CDA. The American Civil Liberties Union followed soon with a lawsuit, and on June 26, 1997, the U.S. Supreme Court upheld the Philadelphia court's decision in *Reno v. ACLU* (Cornell University, 1997). The CDA was followed by the Child Online Protection Act (COPA), which was passed in 1998. Again, the focus was on trying to keep Internet pornography from the reach of minors. But this law was also challenged by speech rights activists. Many rulings, injunctions and appeals followed. Finally, that law was also declared unconstitutional in 2009 by the U. S. Supreme Court.

The above do not prove that Internet censorship was the objective behind CDA and COPA, but suggest that attempts to create a legal environment for such censorship were made. The terrorist attacks of September 11, 2001, gave much more impetus to law-makers and the security establishment to monitor Internet traffic and communications, through the USA PATRIOT Act.

In May 1996, *Human Rights Watch* issued a report titled "Silencing the Net: The Threat to Freedom of Expression On-line," authored by Karen Sorensen (Sorensen, 1996). The report listed various countries around the world, including those in the West, that were actively attempting to curb Internet freedom by claiming to protect citizens from pornography, terrorism, and hate speech.

Germany

In Munich, Germany, a task force was set up in 1994 to detect child pornography on the Internet. Based on the report of the task group, in December 1995, the German operation of the Compuserve on-line service based in Columbus, Ohio, was pressured into removing two hundred Usenet discussion groups along with picture databases, by a federal prosecutor in Munich, Germany. While Compuserve complied, later study showed that at least some of the sites that were censored did not contain objectionable materials. In December 1996, Deutsche Telekom censored sites that carried hate speech. In March 1996, the German Justice Minister announced that Germany would introduce Internet censorship legislation.

France

In October 1996, France tried to regulate its famous Minitel[3] system by proposing that inspectors be used to inspect Minitel to spot content that did not fall within the acceptance range provided in the French Telecom's terms of contract. In the same year, the French government also set up a Commission to study regulating the Internet. The Commission proposed *self-regulation* rather than regulating the source of content. But this was super-ceded by a more stringent proposal by the French Minister of Telecommunications, François Fillon. Under his proposal, a "code of conduct" would be drawn up by the Conseil Supérieur de la Télématique (CST). Internet providers were free to *not* abide by the code. However, those who followed the code voluntarily would be absolved of future legal proceedings (Ang, 1997).

United Kingdom, Australia and New Zealand

In March 1996, British Trade and Industry Minister stated that the government would encourage ISPs to exercise *voluntary control* on the content that they provided to the end-users, failing which the government would have to consider legislation to control Internet content (Sorensen, 1996).

Even as early as 1994, Australia considered imposing some restrictions on the content of the Internet. In August 1994, a report by the Department of Communications and the Arts titled "Regulation of Computer Bulletin Board Systems" was released. The report called for certain regulations. While acknowledging the need to protect the rights of free communications among adults, the report detailed a large list of actions and content that was deemed to be harmful to minors and recommended that the corresponding types of content be restricted through self-regulation. Even while these issues were being debated at the national level, with comments and responses from the public and the Electronic Frontiers of Australia (EFA), a public interest group, various state governments started passing laws that sought to regulate and restrict content deemed inappropriate for minors (Sorensen, 1996).

In 1994, New Zealand's Parliament passed a very restrictive Internet-related bill. The bill, known as the Technology and Reforms Bill, empowered the government to remove all users from any

[3] The Minitel system was introduced in France in 1981. It was a Teletext system that provided various applications to its users via dumb-terminals connected to telephone lines. Applications included news, airline reservation and other ticket booking, banking, etc.

site or service if anybody in that site was found to be transmitting even a single piece of "objectionable material." Those individuals found in violation would also face heavy fines and would be cut-off from telephone services for up to five years. However, this bill swiftly died due to some other political developments that took place[4].

South Asia

This includes Afghanistan, Bangladesh, Bhutan, India, Maldives, Nepal, Pakistan and Sri Lanka. Various levels of Internet censorship have existed in almost all of these countries. Of these countries, India alone has a record of being a strong democracy where strong protections have been guaranteed for freedom of the Press. In this section I will primarily focus on the gradual increase in censorship of the Internet in India.

The ONI (2007b) tested several ISPs in India, and their 2007 report noted that even though there was no evidence of filtering political and social sites, there were indications of selective filtering of sites that were listed by the government as relating to national unity and/or national security. The earliest case of Internet blocking is traced to the unsuccessful attempt by the VSNL in July 1999 during the Kargil war with Pakistan. VSNL, the government owned, sole ISP of the time, attempted to block the online edition of the Pakistani newspaper Dawn. After the Telecommunications Act of 2000, India saw the arrival of many private ISPs.

The issue of Internet censorship hit the headlines, when in September 2003, the Indian government ordered the blocking of all Yahoo groups, because Yahoo refused to block access to a single group, http://groups.yahoo.com/group/kynhun. The Kynhun website was started by the some citizens of the North-eastern state of Meghalaya who espoused secession from India. On February 27, 2003, the Indian government designated the CERT-IN (Computer Emergency Response Team, Department of Telecommunication) as the single authority to issue instructions to block websites. On July 7, 2003, the government issued another notification, which stated, according to Pavn Duggal, "websites promoting hate content, slander or defamation of others, promoting gambling, promoting racism, violence and terrorism and other such material, in addition to promoting pornography, including child pornography, and violent sex can reasonably be blocked" (as cited in Tanna, 2004, para. 16).

Another prominent site that has been blocked over time include the Hindu Unity Web site (www.hinduunity.org), which was blocked on April 28, 2004 for adopting an extremist Hindu fundamentalist stance against Muslims. This spurred a lively public discussion in India, as the blocking of the site was ordered by the Commissioner of Police, Mumbai, rather than CERT-IN. One ISP, *Sify*, refused to comply, saying that the block- order should come from CERT-IN, rather than the state police. The Indian government's various attempts to censor or block websites have always encountered opposition and debate in India Press and various citizen groups, who have defended the citizen's right to freedom of expression.

However, over time, the Indian government has slowly strengthened its powers to censor the Internet. This has gained momentum especially after terrorist attacks in Mumbai in July 2006 and November 2008. Investigations revealed that the terrorists used email, social media and

[4] Ibid.

websites to plot and carry out the attacks. The Indian government released a draft of a proposed amendment to the Telecommunications Act of 2000 in April 2011, which sought to impose stringent restrictions on online intermediaries – "defined as those who store, transmit or provide services related to electronic messages -- for protecting citizen privacy, ensuring cyber security and preventing incitement to violence (Murthy, 2011, para, 5)." The proposed amendment places the onus of blocking inflammatory content on search engine providers and ISPs. The proposed amendment also places stringent restrictions on cyber-cafes, requiring such cafes to maintain detailed records of customers. This has again led to objections by citizens' groups like the People's Union for Civil Liberties (PUCL) and even search engine providers like Google.

Comment: The above discussion cataloged the early stages of Internet spread around the world. In the initial years, the Internet was characterized by chaotic and even anarchist growth unfettered by government controls. However, the rapidness of the growth brought governmental scrutiny. Democratic governments were interested in preventing pornography and hate speech, while trying to promote the commercial possibilities of the new medium. Autocratic governments wanted to curb the Internet for the same reasons, but more importantly, for the possibilities it afforded to enhance free speech and access to information, and thus promote dissent. In recent times, even some democratic governments have attempted to impose censorship of certain content. In some cases, these moves have met with opposition from democratic citizens as well as Internet service providers.

2000s: Systematic Censorship Efforts Gain Ground

The last section discussed tentative steps taken by most countries in their attempts to control the Internet, the exceptions being some Asian countries such as Singapore, China, North Korea and Myanmar. However, during the first decade of the twenty-first century, governments gradually tightened their control of the Internet. This trend has been cataloged in detail by Goldsmith and Wu (2006) in their book, *Who controls the Internet? Illusions of a borderless world*. Governments used laws and framed policies to gain control over access to the Internet by citizens, as well as restrict and control commercial activities on the Internet.

The ONI (n.d.b) describes four methods adopted by states to censor and control the Internet:

1. **Technical blocking:** This is done by blocking certain IP addresses, by removing certain DNS entries, or by blocking certain URLs by using proxy servers. This family of techniques includes, in addition to DNS filtering, IP filtering, keyword blocking, and dynamic content blocking through sophisticated software.
2. **Search result removal:** Search companies often cooperate with authoritarian governments by agreeing to remove certain parts of search results in return for the license to operate in a country
3. **Take down:** This includes 'cease and desist' orders to content providers to remove material, web pages or entire web sites, citing inappropriate on illegal content. In some cases, an entire domain name can be treated as "property" and "seized" by the government.
4. **Induced self-censorship:** Countries such as China and many countries in the EU require that Internet content providers as well as service providers agree to self-regulate

themselves, i.e., agree to follow very strict strictures on various aspects, such as the content, access to consumer data, etc. as a condition for permission to operate.

The items on the list above are actually implemented through a variety of strategies, which I have categorized as follows: **Controlling the intermediary; controlling the financial intermediary; controlling the conduit; establishing gate-keeper systems; filtering and censorship; controlling the standards;** and **total blockade.** While these strategies and specific measures may at times overlap with ONI's list, together they form a comprehensive list of Internet censorship and blocking efforts.

In the following, I give examples of how certain use one or more of these systematic measures to control the Internet in the last decade.

Controlling the Intermediary

The Case of Yahoo

The first case important case was the April, 2000 case against Yahoo! filed by Marc Knobel representing the International League against Racism and Anti-Semitism in a French court. The case pertained to the neo-Nazi merchandize sold on-line by Yahoo. The lawyers of Yahoo argued that French jurisdiction did not apply to Yahoo, an American company which posted its merchandize on the Web, anywhere in the world. The French judge disagreed, and ruled that as long as Yahoo operated in France in any means, it had to obey French laws, which prohibited the advertisement and sale of neo-Nazi merchandize. The court ruled that Yahoo should make all efforts to comply, or else punitive fines would be imposed, or worse, Yahoo would be barred from operating in France. Finally, Yahoo agreed and pulled out the offending merchandize.

In 1999, Yahoo entered the Chinese market, with a view to giving Chinese Internet users access to a range of information and services. But the Chinese government insisted that Yahoo filter the Internet and provide only government-approved information to its citizens. In 2002, Yahoo agreed to the Chinese government's demands. In 2005, Chinese journalist Shi Tao sent an email to a democracy website, using Yahoo mail. The Chinese government discovered the mail at an American website, and asked Yahoo to identify the sender. Yahoo was forced to identify the sender of the mail, and Shi Tao was sentenced to ten years in prison.

Comment: In this case, Yahoo was the intermediary. The government controlled Yahoo by using as weapons threats of disruption as well as license to operate. By controlling the intermediary, the government did not need to control the source of information. In addition, the government could also place the target consumer under threat of being disclosed.

Controlling the Financial Intermediaries

Financial intermediaries are required in order to conduct online financial and commercial transactions, such as buying, selling, auctioning, etc. Examples of financial intermediaries are banking and credit card companies like Citibank and American Express, and others such as Paypal. Governments control certain Internet activities and transactions by controlling the

intermediaries and preventing them from completing or even allowing certain types of transactions from the "targets" i.e. the consumers, and the "sources" i.e. the service or content providers. Thus as noted by Goldsmith and Wu (2006), if the U.S. government wanted to stop off-shore Internet gambling sites, all it needs to do is to warn the financial intermediaries of prosecution, were they to enable such transactions to take place. Since on-line gambling or e-Commerce rely on credit-card based financial transactions, the end user is effectively stopped or curtailed from participating in such activities deemed inappropriate by the government. This type of coercion even happened recently in the case of Wikileaks. When Wikileaks published a vast number of confidential U.S. diplomatic cables, many government figures in the U.S. directly and indirectly made statements that banks and other financial institutions that handled Wikileaks donations, as well as those online services that sold Wikileaks-related merchandise would be prosecuted. This forced those institutions to stop dealing with Wikileaks.

Controlling the Conduit

In 2001 in the UK, the government threatened to criminally prosecute Internet Service Providers (ISPs) for distributing content that was deemed to be inappropriate. At the time, the government was targeting ISPs for distributing illegal adoption sites, including those located abroad. By 2005, the UK, Germany and France had all adopted laws that require ISPs to remove contents that are deemed illegal or inappropriate. Otherwise, they could be prosecuted.

Comment: It should be noted that in the mid 1990s, UK, Germany and France focused on self-regulation of content. But this was difficult to police or control, as content could exist in jurisdictions that were not under these countries' dominion. By mid-2000s, many countries had shifted tactics and moved aggressively to control the conduits – i.e. the ISPs instead. China has sought to control every aspect of the Internet. China actively controls the information sources inside China, and actively prohibits content from sources abroad either directly through filtering, or through the control of conduits.

China uses an elaborate system for controlling and censoring content. The Chinese government use *Internet gateway routers* to drop incoming and outgoing packets that do not meet with official approval. Since typically there are only a few ISPs (and thus gateway routers) controlling entry into China, and since these are controlled by the Chinese government, this is a very simple but effective way of controlling content. Additionally, since the source and destination IP addresses are visible to the ISPs routers, the authorities can easily keep track of those within China who request or send offending materials. It is important to note that the predominant hardware used for such filtering are routers supplied by Cisco Systems, a U.S. company.

Filtering and Censorship

Test

Another, more expensive method of filtering used extensively in China is "search result filtering." In this method, certain search results that are returned by external search engines are simply blocked from being displayed, using a keyword search mechanism. This form of filtering

is even more effective, as the end user never knows the complete and un-censored list of query responses.

In 2005, the Microsoft admitted that its Chinese blog site "MSN Spaces," which allowed Chinese citizens to set up blog site in China, blocked titles like "democracy" and "freedom," under government pressure (Goldsmith & Wu, 2006). Both Microsoft and Yahoo were required to agree to a binding "self-discipline pact." Bloggers were required to register with the authorities, and Internet cafés are policed. These acts clearly demonstrate the power and determination of the Chinese government to control the Internet within China. China also routinely uses proxy servers to stop certain searches from leaving the Chinese methods to accomplish the same.

Second only to China, Iran practices the most extensive and organized censorship and control of the Internet. The ONI reports that over the years, Iran has greatly expanded and consolidated its technical filtering system (ONI, 2009a). The censorship efforts were applied in full force during the 2009 elections in Iran, when the government blocked several opposition web sites. When President Mahmoud Ahmedinejad was declared the winner, opposition parties and their supporters disputed the elections, and a vast majority of them participated in huge protests in Tehran. The Internet and social media were the preferred means to mobilize the protesters.

But shortly thereafter, the government fought back by blocking all social media systems such as YouTube, Skype, Flickr, Facebook and Twitter. According to Clothilde Le Coz, Director of Internet research for *Reporters Without Borders,* the Iranian government officials were openly bragging even in 2008 that the government was blocking five million websites (Abate, 2009).

The ONI and Abate of *Global Post* note that over the years, Iran has acquired and used filtering software and hardware from Secure Computing/McAfee and Nokia Siemens Networks, and has augmented them with locally produced filtering technologies.

In August 2006, The Berkman Center for the Internet and Society at Harvard University reported that the Socialist Republic of Vietnam was "actively censoring the Internet, focusing its filtering on sites considered threatening to its one-party system" (para. 2) The report also noted that the technical sophistication, breadth, and effectiveness of Vietnam's filtering were similar that that of China's with which Vietnam maintained close ties. Similar to China, Vietnam has taken a multi-layered approach to controlling the Internet; Vietnam applies technical controls, the law, and education to restrict its citizens' access to and use of information (Berkman Center, 2006). The censorship regimen has increased since then. In the last couple of years, there have been several articles in the news media that have reported on the increasing Internet censorship in Vietnam. On June 22, 2010, the *Asia News* reported that "In recent days, student and young people have complained that local authorities have partially or wholly blocked access to sites like *Facebook*, the *BBC* Vietnamese service and Vietnamese media based abroad. 'Many websites writing about democracy, freedom, justice and peace cannot be opened . . . '" (Asia News, 2010, para. 2)."

Establishing Gatekeeper Systems

Saudi Arabia controls content available to its citizens from Internet sites by establishing a proxy server which stands between the Saudi Arabian backbone network and external web sites. Any search that goes outside the country first goes to the proxy server, which then either passes on the query or summarily terminates it. The Internet Service Unit of the King Abdulaziz City for Science and Technology maintains the proxy server. The government is quite open about its filtering practices, and the role of the proxy server is published on its website (http://www.isu.net.sa/saudi-internet/contenet-filtring/filtring.htm):

"KACST maintains a central log and specialized proxy equipment, which processes all page requests from within the country and compares them to a black list of banned sites. If the requested page is included in the black list then it is dropped, otherwise it is executed, then the request is archived. These black lists are purchased from commercial companies and renewed on a continuous basis throughout the year. This commercial list is then enhanced with various sites added locally by trained staff" (Internet Service Unit, n.d., para. 3).

In addition to this explanation, the site also provides extensive religious (Islamic) justifications for filtering Internet content, and lists a number of software packages that citizens (i.e. parents, teachers, etc.) can use to further filter Internet contents (Internet Services Unit, n.d.).

Tunisia has one of the most developed telecommunications infrastructures in North Africa. It is well connected to the Internet, with over 33% of its citizens connected in 2009 (Internet World Stats, n.d.). In 2009, Tunisia had eleven ISPs (ONI Report, 2009b). However, the Tunisian government strictly policed Internet access by blocking numerous web sites thought to be anti-government in nature. The main ISP was the Tunisian Internet Agency (ATI), which was set up by the Tunisian Ministry of Telecommunications in 1996. The other ISPs leased bandwidth from the ATI. Thus the government maintained controlled over the Internet. As early as 2002, Zouhair Yahyaoui, a 35-year-old Tunisian, was jailed for two years in 2002 over criticism of the government in his web publication TUNeZINE (Lank, 2003). Over the years, numerous such instances of Internet censorship have been reported in the press. An ONI report in 2005 noted that Tunisia aggressively targeted and blocked "substantial on-line material on political opposition, human rights, methods of bypassing filtering, and pornography" (ONI, 2005a, para. 1).

Controlling the Standards

By controlling certain standards for wireless and other data communications standards, a state can effectively enhance surveillance of content passing from the content provider to the consumer, and thus control the Internet. In 2003, China released a new standard for wireless communications – WLAN Authentication and Privacy Infrastructure (WAPI), and mandated that this standard be included in all wireless devices sold in China starting in 2004. An interesting aspect of this new protocol was that it required both the sender and the WAP to register with a central WAPI server that would authenticate the connection. To many privacy activists, this was an overt attempt by the Chinese government to monitor wireless users through a standards based mechanism. The standard was to be licensed by eleven companies in China to all providers of

wireless equipment. However, the introduction and imposition of this new, closed standard was contested by the U.S. at the ISO, arguing that it imposed trade restrictions, and finally in 2006, the ISO rejected the new standard. This, however, is an example of how a government sought control by imposing computing and communications standard.

Total Blockade

While various governments have censored, filtered and used other means to control the content available to their citizens, as well as news emanating from within to the rest of the world, very rarely have governments attempted to completely shut off the Internet, thus completely blocking all access from any entity inside to any entity outside, and vice versa. But this was attempted September 29, 2007 by Myanmar's military junta and in January 28, 2011 by the Egyptian government.

Myanmar

In August 2007, a sharp hike in fuel price in Myanmar led to widespread protests and rallies by its citizens. The military regime reacted by using harsh tactics to put down the protesters. A violent crackdown on September 26 left almost 200 dead. As the unrest spread, the citizens started using blogs, newsgroups and email to spread the message to others within the country, and relay messages, video clips and images of the harsh government response to the international media. Blow by blow accounts of the government crackdown, including videos were posted on YouTube. First, the government ordered a blackout of all local coverage, and tried to shut off access to foreign media organizations. Then on September 29, the government cut off all Internet connection with the outside world (ONI, 2007a). Until then, the "cyber-dissidents" of Myanmar maintained communications with the outside media and the blogging community through Internet chat, the use of proxy servers that penetrated the Internet, email, and free web hosting sites. The complete shutdown of the Internet lasted until October 4, 2007.

Egypt

Shortly after midnight on January 27, 2011, all Internet traffic entering and leaving Egypt abruptly dropped precipitously until it became just a trickle. Almost all of the twenty million people in Egypt who were connected online found themselves disconnected from the Internet (Glanz & Markoff, 2011). This was the Egyptian government's response to the anti-government protest movement that was rapidly spreading in the country. In the preceding days, pro-democracy and anti-government protesters had successfully leveraged the speed and reach of the Internet – especially social networks – to rapidly mobilize more supporters, organize protests in various locations, and transmit news of the protests to supporters and news media all over the world. The protest movement in Egypt followed in close succession a similar protest movement in Tunisia[5] just a few weeks earlier, which resulted in the ousting of Tunisia's government.

[5] The 2010 Tunisian revolt started when, on December 17, 2010, an unemployed Tunisian man named Mohammad Bouazizi immolated himself in protest when the police confiscated the fruits he was trying to sell, demanding a bribe. Even though this happened in the town of Sidi Bouzid in Central Tunisia, news of this act rapidly spread throughout Tunisia through the social-networking sites Facebook and Twitter[5]. Tunisian citizens began to protest the circumstances leading to Bauazizi's death. The protests morphed into a full-fledged revolt against corruption in the

Comment: The Internet blockade by the Egyptian government on January 28, 2011 shocked not just those who supported the freedom of expression, but also gave considerable pause to many in the technical community who simply had not thought that such a country-wide, near-complete shut-down of the Internet was even possible. Since the Egyptian Internet blockade, the idea that an "Internet Kill Switch" existed, and could be deployed quickly by governments, has gaining traction among citizens, activists and security professional alike. The Internet kill switch has interested technologists and non-technologists alike for some time now.

Technologies of Internet Censorship and Blockade

In the last section I discussed some of the standard techniques used in Internet censorship efforts. Much of these require the use of sophisticated software and hardware technologies.

As noted earlier, China uses router-based filtering, using the hardware and software supplied by Cisco Systems. In addition, China has gradually produced a collection of locally produced software that can be used for filtering the Internet. A well-known example is the "Green Dam" software developed in China (Lam, 2009).

Tunisia, which carried out elaborate Internet filtering, used the *SmartFilter* software, produced by the U.S. company Secure Computing. In 2008, Secure Computing was acquired by McAfee Inc. Tunisia's Internet infrastructure has a centralized hierarchy, with the government-owned ATI providing bandwidth to all the other ISPs. Therefore, all filtering of Internet content happens at ATI. Because of this, filtering is consistent throughout Tunisia. According to ONI, Tunisia's *SmartFilter* settings blocked anonymity, nudity, pornography and sexual themes. This was in addition to political views as well as human rights web sites. Also, the Internet blocking and filtering in Tunisia was secret, i.e. the users were not informed that a page was not accessible because of filtering.

In 2005, the ONI reported that initially, Bagan Cybertech of Myanmar (government-controlled ISP) used *DansGuardian* filtering software to block access to certain sites. The government also purchased the *Fortinet Fortiguard* firewall product in 2004. Fortinet is a U.S. company. The product comprises of a firewall and a database that categorizes web pages (ONI, 2005b). It was noted by the ONI that the filtering became more stringent and effective after the ISP started using Fortinet. This was perhaps due to the fact that the open source *DansGuardian* had a longer learning curve, combined with more effort required on the part of systems administrators.

Saudi Arabia uses the *SmartFilter* software to filter Internet Content. In addition, Saudi Arabia also provides its citizens a list of approved filtering software that can be used by individuals, families and schools. These are: Cybersitter, Netnanny, CyberPatrol, CyberSentinel, Cyber Snoop, SurfWatch, WebChaperone, and X-Stop.(Internet Services Unit, n.d.)

---

government, in a climate of high unemployment and food inflation. Many commentators including Tom Malinowski of Human Rights Watch have noted that the revolt was at least partly fueled by the whistle-blower website Wikileaks, which posted diplomatic cable exchanges between the American Embassy in Tunis and the U.S. State Department (Malinowski, 2011). The cables described the vast and corrupt dealings of the Tunisian president Mr. Zine el-Abidine Ben Ali and his family ("08Tunis679," 2010).

Iran uses the *SmartFilter*, and in addition, uses products from Nokia Siemens Networks to do "deep packet inspection" of data that is transmitted. Lately, Iran has, similar to China, started using domestically produced filtering software.

The "Kill Switch"

While it is easy to imagine that a total Internet blockade can be accomplished by simply shutting off all the border routers at the top level ISPs, this is not entirely practical. This is because a country will still need to be connected to international financial systems, and need to access systems used by the military. In addition, there may be international Internet traffic that may actually be passing through the country. Also, even repressive regimes need private access to emails and the Web. This means that a targeted and carefully planned shut-down has to be implemented. But this is also difficult to accomplish, as there is no guarantee that citizens within the country are completely blocked from proxy servers and anonymizers that hide the true source and destination IP addresses.

Burma

Nart Villeneuve, a security researcher at the ONI, did an analysis of the Burmese Autonomous System Border Gateway Protocol (BGP) advertisements. This data was available from the BGP monitors of the RIPE project (ONI, 2007a). Nart noted the following about the Burma Internet blockade:

> A high-level traffic analysis of the logs of NTP (Network Time Protocol) servers indicates that the border routers corresponding to the two ISPs were not turned off suddenly. Rather, our analysis indicates that this was a gradual process: traffic fell to 14 percent of the previous week's average on September 28, going down to 7 percent of the average on September 29 and zero traffic on September 30. This matches with the BGP data coming from AS 9988 and AS 18399 belonging to MPT and BaganNet respectively (Villeneuve, 2007, para. 3).

Egypt

Shortly after midnight, January 27, the Egyptian government apparently ordered all ISPs to shut down all international connections to the Internet. This was in response to the large-scale pro-democracy protests that were underway in Egypt at that time. James Cowie (2011) analyzed the blockade and noted the following sequence of events on the Renesys Blog:

- Telecom Egypt (AS8452), the national incumbent, starts the process at 22:12:43.
- Raya joins in a minute later, at 22:13:26.
- Link Egypt (AS24863) begins taking themselves down 4 minutes later, at 22:17:10.
- Etisalat Misr (AS32992) goes two minutes later, at 22:19:02
- Internet Egypt (AS5536) goes six minutes later, at 22:25:10.

This sequence shows that there was no single "kill switch." Instead, this shows that the relatively few ISPs with unique Autonomous System numbers (ASNs) were being ordered to shut off all external advertisements. Once the "adjacent" AS's Border router noticed a lack of advertisement

from the (Egyptian) ISP, it took the IP prefix off its BGP list. In Egypt's case, most internal networks were also disconnected, except one, named Noor, which was connected to Egypt's financial market.

These analyses show that there is no single "switch" that can be used to shut of or block the Internet connectivity completely. However, in the case of smaller countries, with a relatively small number of ISPs, this can be accomplished with some planning.

Circumvention

As seen from the above discussion, many states around the world try to suppress information exchange and free speech by censoring or blockading the Internet using various methods and devices. However, these attempts have only succeeded up to a certain level. Citizens and activists have consistently found or developed methods and strategies to circumvent such attempts to block the Internet.

Many citizens in repressive states that seek to control access to the Internet make use of "anonymizers" and "proxy servers." Once a user connects to the proxy server's site, his/her source IP address as well as the destination IP address is "anonymized" so that a simple IP address or domain name filter can be circumvented. Examples include proxify.com, anonymizer.com and megaproxy.com proxy servers. There are also "translators" that translate or hide an original query to another. Examples are systransoft.com, Altavista/Babelfish, and dictionary.com.

The states have responded by blocking certain these specific domains and IP addresses so as to prevent citizens from reaching the sites. But in response, certain alternate proxy-servers are set up, usually in a foreign country. Then connection to these proxy servers can be made even by using dial-up connectivity, thus bypassing state censorship. Citizens of Myanmar used this technique to access proxy servers such as Glite.sayni.net during the country's Internet blockade (Crispin, 2001).

The University of Toronto's Citizen Lab has developed software called *psiphon* which acts as a tunnel through the firewall. Psiphon works through social networks. A net user in an uncensored country can download the program to their computer, which transforms it into an access point. They can then give contacts in censored countries a unique web address, login and password, which enable the restricted users to browse the web freely through an encrypted connection to the proxy server (Citizen Lab, 2009).

Kindle users can access banned websites in mainland China from the device. With Amazon's electronic book gadget, Kindle users can now visit Facebook and Twitter, both currently blocked by the Chinese government (Zhang, 2010).

In addition to activists, some democratic governments in the West have established programs to aid citizens from repressive regimes to more effectively and safely use Internet and social media technologies to organize their protests. The U.S. State Department has recently started funding certain activist organizations that focus on educating pro-democracy and anti-government

movements in repressive regimes. The training includes ways to avoid traps set by the repressive governments that enable tracking of the dissidents and their activities. It has been observed that during the 2010-2011 protests in Tunisia and Syria, the states' intelligence operatives increasing turned to social media such as Facebook, creating false identities and infiltrating the dissident groups. The State Department has already funded over $22 million in "Internet freedom" grants. One of the projects funded includes MobileActive.org, which build a "panic button" that allows activists, if pursued or arrested, to send a text message to a group of contacts in a way that does not appear in the phone's call-log (Greeley & Gaouette, 2011).

CONCLUSION

The Internet has, within a period of twenty years, become the primary medium of information exchange in the world. It is also arguably the primary source of information in the world. Search engines such as Google and Yahoo have made the vast trove of information available and accessible to everybody. Email and social network applications such as Facebook and Twitter have enabled people all over the world to meet, collaborate, and participate in joint activities. The Internet has also gradually become a tool of dissidence in repressed nations all over the world - to spread information, plan and organize activists and conduct protests. Not surprisingly, repressive regimes see the Internet as a threat. Under the guise of protecting their citizens from the negative effects of the Internet (such as pornography and hate speech), they have, and are, actively curbed Internet use by their citizens by adopting various censorship measures and blockades.

In this paper I have surveyed the history of Internet censorship by various countries, starting from 1991. It is seen that the urge to curb and control Internet content is not just a preoccupation of repressive societies. Even democratic countries such as the U.S. and many EU countries have sought to control the Internet for various reasons over time. Starting from the turn of the century, these attempts to control the Internet have become more and more sophisticated. Governments all over the world use various means – legal, political, technical, and coercive – to control and restrict Internet content. Cataloging all such efforts by all the countries would be beyond the scope of this paper. Despite that, I have tried to focus on the various methods of censorship and blockades used by various countries around the world. I have also provided a brief description of recent attempts by Myanmar and Egypt to completely block the Internet, with a discussion of the technique and methods involved. Finally, I have also briefly discussed the push-back efforts by citizens of the world, who are actively and innovatively finding ways to circumvent the most pernicious of these censorship efforts and blockades.

I believe that there will always be efforts to control and curb the Internet, and for that matter, any other means of communication. However, such efforts will only lead to an "arms race" between those who seek to control, and those who want free access. Just as newer technologies and methods will be developed to censor and control the Internet, there will also be simultaneous efforts to develop techniques and methods to overcome and circumvent such controls. Finally, I believe that it is important that the Internet remain free and open, and suggest that free and open access to the Internet should become a universal right, applicable to all the people of the world.

Future work would focus on legal and policy implications of Internet censorship, as well as study the emergence and gradual growth of the global movement that considers access to the Internet as no different from access to knowledge, and can thus be considered to be a human right.
Another shortcoming in studies of Internet censorship and circumvention is a lack of a framework to analyze such moves. A framework will bring in a standardization and uniformity of such studies and enable quantification of Internet censorship and circumvention, which will further enable more empirical, rather than descriptive studies. I propose to undertake further study in developing such a framework in the future.

REFERENCES

08Tunis679, Corruption in Tunisia: What's yours is mine. (2010, December 7). In *Wikileaks*. Retrieved March 25, 2011, from http://wikileaks.ch/cable/2008/06/08TUNIS679.html

Abate, T. (2009, July 7). *Iran stocks up on censorship tools*. Retrieved June 2, 2011, from http://www.globalpost.com/dispatch/technology/090706/iran-web-censorship

Ang, P. H. (1997). *How countries are regulating Internet content*. Paper presented at the INET97: The Seventh Annual Conference of the Internet Society, Kuala Lumpur, Malaysia. Retrieved from http://www.isoc.org/inet97/proceedings/B1/B1_3.HTM

Ang, P. H., & Nadarajan, B. (1995). *Censorship and Internet: A Singapore perspective*. Paper presented at the INET'95 - The Internet Society's 1995 International Networking Conference, Honolulu, Hawaii. Retrieved from http://www.isoc.org/inet95/proceedings/PAPER/132/txt/paper.txt

Asia News. (2010, June 22). *Internet censorship tightening in Vietnam*. Retrieved June 3, 2011, from http://www.asianews.it/news-en/Internet-censorship-tightening-in-Vietnam-18746.html

Bardacke, T. (1996, October 5). High price to pay for Internet use in Burma. *The Financial Times*. Retrieved from http://www.burmanet.org/bnn_archives/1996/bnn1096n536.txt

Berkman Center. (2006, August 5). *OpenNet initiative Vietnam report: University research team finds an increase in Internet censorship in Vietnam*. Retrieved June 3, 2011, from http://cyber.law.harvard.edu/newsroom/opennet_vietnam

Berners-Lee, T. (n.d.). *Tim Berners-Lee: Bio.* Retrieved May 21, 2011, from http://www.w3.org/People/Berners-Lee/

Citizen Lab. (2009). *China's battle to police the web*. Retrieved June 2, 2011, from http://citizenlab.org/2008/03/chinas-battle-to-police-the-web/

Cornell University Legal Information Institute (LII). (1997, June 26). *Reno v. American Civil Liberrties Union (96-511) 521 U.S. 844 (1997).* Retrieved April 1, 2011, from http://www.law.cornell.edu/supct/html/historics/USSC_CR_0521_0844_ZS.html

Cowie, J. (2011, January 27). Egypt leaves the Internet. Retrieved February 17, 2011, from http://renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml

Crispin, S. W. (2001, September 21). Burning down Myanmar's Internet firewall. *Asia Times Online*. Retrieved May 27, 2011, from http://www.atimes.com/atimes/Southeast_Asia/ II21Ae01.html

Dyson, E., Gilder, G., Keyworth, G., & Toffler, A. (1994, August). Cyberspace and the American dream: A magna carta for the knowledge age. *Future Insight*. Retrieved from http://www.pff.org/issues-pubs/futureinsights/fi1.2magnacarta.html

Feir, S. E. (1997). Regulations restricting Internet access: Attempted repair of rupture in China's great wall restraining the free exchange of ideas. *Pacific Rim Law & Policy Journal*.

Glanz, J., & Markoff, J. (2011, February 15). Egypt leaders found "off" switch for Internet. Retrieved February 17, 2011, from http://www.nytimes.com/2011/02/16/technology/ 16internet.html?_r=1&sq=internet%20switch&st=cse&scp=1&pagewanted=all

Goldsmith, J., & Wu, T. (2006). *Who controls the Internet? Illusions of a borderless world*. New York, NY: Oxford University Press, USA.

Greeley, B., & Gaouette, N. (2011, April 28). Untangling dictators' webs: The State Dept. is funding tools to help online activists abroad. *BusinessWeek*. Retrieved June 3, 2011, from http://www.businessweek.com/magazine/content/11_19/b4227022810305.htm

Internet Services Unit. (n.d.). *Introduction to content filtering: What is this service?* Retrieved May 26, 2011, from http://www.isu.net.sa/saudi-internet/contenet-filtring/filtring.htm

Internet World Stats. (n.d.). *Tunisia: Internet usage and telecommunications market report.* Retrieved March 23, 2011, from http://www.internetworldstats.com/af/tn.htm

Knoll, A. (1996). Any which way but loose: Nations regulate the Internet. *Tulane Journal of International and Comparative Law, 4*, 275.

Lam, O. (2009, June 8). *China: Green dam PC filtering*. Retrieved June 3, 2011, from http://advocacy.globalvoicesonline.org/2009/06/08/china-green-dam-pc-filtering/

Lank, R. (2003, February 18). *Tunisia: Seven versions of Pravda*. Retrieved June 1, 2011, from http://worldpress.org/Mideast/957.cfm

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., . . . Wolf, S.. (2003). A brief history of the Internet. Retrieved from http://www.internetsociety.org/internet/internet-51/history-internet/brief-history-internet

Liu, A. (2002). *The culture of information*. Retrieved March 26, 2011, from http://www.english.ucsb.edu/faculty/ayliu/courses/english25/2002W/materials/class17notes.html

Malinowski, T. (2011, January 25). Whispering at autocrats. *Foreign Policy*. Retrieved from http://www.foreignpolicy.com/articles/2011/01/25/whispering_at_autocrats?page=0,0

Murthy, G. (2011, June 2). *Whither democracy/wither democracy: The rise of Internet censorship in India*. Retrieved September 14, 2011, from http://www.audiencescapes.org/india-democracy-internet-regulation-cyber-cafes-freedom-media-access

ONI. (2005a). *Internet filtering in Tunisia in 2005: A country study*. Retrieved June 1, 2011, from http://opennet.net/studies/tunisia

ONI. (2005b). *Internet filtering in Burma in 2005: A country study*. Retrieved June 2, 2011, from http://opennet.net/studies/burma

ONI. (2007a). *Pulling the plug: A technical review of the Internet shutdown in Burma*. Retrieved June 1, 2011, from http://opennet.net/research/bulletins/013

ONI. (2007b, May 9). *India*. Retrieved October 1, 2011, from http://opennet.net/research/profiles/india

ONI. (2009a, June 16). *Iran*. Retrieved June 2, 2011, from http://opennet.net/research/profiles/iran

ONI. (2009b, August 7). *Tunisia*. Retrieved June 1, 2011, from http://opennet.net/research/profiles/tunisia#footnote8_qi3bs7e

ONI. (n.d.a). *Research*. Retrieved May 22, 2011, from http://opennet.net/research

ONI. (n.d.b). *About filtering*. Retrieved May 26, 2011, from http://opennet.net/ about-filtering

Sorensen, K. (1996). Silencing the net: The threat to freedom of expression on-line. *Human Rights Watch, 8(2)*. Retrieved from http://epic.org/free_speech/intl/hrw_report_5_96.html

Staiman, A. (1996). Shielding Internet users from undesirable content: The advantages of a PICS based rating system. *Fordham Int'l L. J., 20*, 866.

Tanna, K. (2004). *Internet Censorship in India: Is it Necessary and does it work?* Retrieved from http://www.ketan.net/INTERNET_CENSORSHIP_IN_INDIA.html

Villeneuve, N. (2007, November 5). *ONI: Myanmar/Burma Internet closure*. Retrieved June 2, 2011, from http://www.nartv.org/2007/11/05/oni-myanmarburma-internet-closure/

Wavell, S. (1995, September 3). Closed societies opened by Internet genie. *The Sunday Times (London)*. Retrieved from http://www.lexisnexis.com/hottopics/lnacademic/?sfi= AC00 NBGenSrch&csi=332263&shr=t

Winner, L. (1997). Cyberlibertarian myths and the prospects for community. *ACM SIGCAS Computers and Society*, *27*(3). doi: 10.1145/270858.270864

Zhang, Q. (2010, November 1). *Amazon's Kindle bypasses the great firewall of China*. Retrieved June 2, 2011, from http://opennet.net/blog/2010/11/amazon%E2%80%99s-kindle-bypasses-great-firewall-china