Government Control Of Communications Technology

Evan Peterson, University of Detroit Mercy, USA
Gregory W. Ulferts, University of Detroit Mercy, USA

ABSTRACT

The internet allows for the sharing of knowledge, communications, and business transactions on a global scale. Governmental regulation of the internet varies among different countries and regions of the world. The benefits and burdens of such regulatory policies should be considered.

Keywords: Internet regulation, government control, user accountability

INTRODUCTION

Advances in technology have enabled citizens in all areas of the world to interact with each other on an unprecedented scale in human history. In the tech savvy world of the 21st century, information, knowledge, wealth, and people are in a constant state of motion from one point of the globe to the next. While a variety of factors have contributed to this global interconnectivity, perhaps the most pervasive driving force centers around the growth of the internet. In the countries where internet use has seemingly become part of daily life, the internet has opened up a vast array of opportunities, from the discovery of new information to global communications.

Despite being hailed as a triumph by many and the dawn of a new age in global interconnectedness, access to the internet is regulated to one degree or another in nearly every country. The purpose of this paper is to examine the effects of government control on internet user accountability by an examination of countries in four geographic areas throughout the world: the Middle East, Asia, Europe, and North America.

BACKGROUND

The Kingdom of Saudi Arabia was introduced to the internet in 1994, but initial use was restricted to state academic, medical, and research institutions.[1] In 1997 the internet became officially available, but local internet service providers did not begin the process of connecting ordinary citizens until 1999. The King Abdul-Aziz City for Science and Technology (KACST) was established by the state to coordinate internet policy. A 1998 statement by the president of KACST, Saleh Abdulrahman Al-'Adhel, acknowledged that a standing committee had been created to protect the country's society from internet materials that violate Islam or infringe upon Saudi traditions and culture.[2]

In 2001, the Council of Ministers enacted a Resolution that forbade all users in the country from publishing or accessing various categories of internet content.[3] Under the Resolution, citizens are prohibited from accessing or publishing data in several categories, which include among others:

[1] "The Internet in the Mideast and North Africa: Free Expression and Censorship – Saudi Arabia" (Oct. 7, 2008) at www.hrw.org/advocacy/internet/mena/saudi.htm.
[2] "The Internet in the Mideast and North Africa: Free Expression and Censorship – Saudi Arabia" at 1.
[3] Council of Ministers Resolution 12 February 2001 (Oct. 7, 2008) at http://www.al-bab.com/media/docs/saudi.htm.

- Anything contravening a fundamental principle or legislation, or infringing the sanctity of Islam and its benevolent Shari'ah, or breaching public decency
- Anything contrary to the state or its system
- Anything damaging to the dignity of heads of states or heads of credited diplomatic missions in the Kingdom, or harm in relations with those countries
- The propagation of subversive ideas or the disruption of public order or dispute among citizens

In essence, the main goal of the government in enacting this policy is to ensure the country and its citizens are protected from any foreign influences it deems immoral.[4]

Despite the extensive regulation, there is an element of transparency to the filtering system. The state, via its resolution, promulgated publicly the limits regarding what types of content can be accessed and what types of content are blocked. When an internet user attempts to access a prohibited site, he or she receives a notice stating the site is blocked and explaining why it is filtered. While the blocked page displays a link to a form that would allow the user to suggest other sites that the government should block, there is also a link that provides a means for the internet user to request the site be unblocked.[5]

Like Saudi Arabia, China too has undertaken a massive effort to control the flow of information on the internet to its citizens. The initial steps taken by the Chinese government to regulate internet use occurred in 1997 when, acting pursuant to its authority under State Council Order No. 147, the Ministry of Public Security enacted extensive regulations restricting internet use. The stated purpose for enacting the regulations was to solidify the security of computer networks and the internet, and also to preserve social order.[6] Under Article 5 of the regulations, individuals may not, among other things, retrieve information that:

- Incites resistance to the Constitution, laws, or administrative regulations
- Incites division of the country or harms national unification
- Distorts the truth, spreads rumors, or destroys social order
- Injures the reputation of state entities

The media channels within China are closely scrutinized and it is not an uncommon occurrence for a journalist to be punished for disseminating information at odds with the official doctrine of the Communist Party. The Party seeks to restrict publication of information related to topics or movements that are subversive to the state, and also suppresses material it deems inappropriate for internet users, such as materials on pornography and obscenity.[7] Unlike the filtering system in Saudi Arabia, when an internet user in China attempts to access a restricted page he or she generally receives a network timeout message as opposed to a message giving the reasons for the blocking and an opportunity to request blocking reconsideration. Furthermore, the state generally does not admit to the censorship of internet content, and citizens are unable to request that the blocking of a site be reconsidered.[8] In addition, internet service providers utilize policies of self-censorship. Certain ISP employees, known as "Big Mamas," guide volunteers in the patrol of chat rooms and bulletin boards with an eye to eliminating undesirable content.[9] There have even been instances where ordinary users have reported violations to authorities.[10]

Unlike the previously discussed countries, the United States does not filter its citizens' access to the internet outright. Instead, the use by its citizens of the internet is regulated more after the fact. Despite opposition

[4] "Silenced – Saudi Arabia," Privacy International (Oct. 7, 2008) at www.privacyinternational.org.
[5] "Internet Filtering in Saudi Arabia in 2004," OpenNet Initiative (Dec. 20, 2008) at http://opennet.net/studies/saudi.
[6] "Internet Filtering in China in 2004-2005: A Country Study," OpenNet Initiative (Dec 20, 2008) at http://opennet.net/studies/china.
[7] "Internet Filtering in China in 2004-2005: A Country Study" at 5.
[8] "Internet Filtering in China in 2004-2005: A Country Study."
[9] "Review of China's Internet Regulations and Domestic Legislation," International Center for Human Rights and Democratic Development (Oct. 7, 2008) at http://www.ichrdd.ca.
[10] "Internet Filtering in China in 2004-2005: A Country Study" at 18.

from free speech advocates, the United States government heavily regulates internet use in four main areas: child protection, national security, intellectual property, and computer security.[11]

In the area of child protection, the Children's Internet Protection Act (CIPA) was created to address concerns about children accessing certain Internet content in libraries and schools. Under CIPA[12], in order for a library or school to receive certain funding to support communications technology, it must implement a policing addressing:

- Access by minors to Internet materials that are inappropriate
- Safety and security of minors who use email, chat rooms, and other direct electronic communication types
- Access that is unauthorized, such as hacking and other unlawful online activities
- Unauthorized disclosure, use, or dissemination of personal information of minors

It is argued that the extensive schemes of other countries have not taken as firm a hold in the United States due to the strong resistance to these policies on freedom of speech grounds.[13]

Despite democratic roots, filtering of the internet within Europe occurs in several ways. Such methods include filtering search engine results based on illegal content, blocking illegal content originating from abroad, and state-backed elimination of illegal content on domestic sites. The range of filtered material in Europe includes child pornography, racism, and hate speech.[14] However, research uncovered no examples in Europe of filtering based on intent to silence political opposition.

Over the past few years there have been efforts to craft common policies and procedures at the European Union level pertaining to regulation of the Internet. Such a set of common policies and procedures is considered vital in order to promote commerce and competition, respond to criminal activity, and promote best practices. In 2002[15], an Action Plan on Promoting Safe Use of the Internet went into effect. This plan discussed some of the following areas where action is required to curtail damaging and illegal internet content:

- Promoting voluntary self-regulation and content monitoring schemes by industries
- Providing filtering tools and rating systems allowing parents and teachers to regulate access by children to certain internet content
- Exploring law-related implications of promoting safe internet use
- Encouraging internal cooperation in regulation

In 2004[16], Britain's largest ISP initiated Project Cleanfeed, thereby filtering Internet content according to a blacklist of sites containing images of child abuse as defined in the Protection of Children Act. This blacklist is created by the Internet Watch Foundation, a not-for-profit, in consultation with the government, industry leaders, police, and the general public. Attempts to access illegal content hosted abroad are met with an error message, designating the page unavailable. Voluntary self-regulation is also conducted by search engines, such as Google, Yahoo, and Lycos Europe. In addition, in nineteen European countries the general public assists in the identification and reporting of illegal content through various hotlines.[17]

[11] "United States and Canada," OpenNet Initiative (Oct. 14, 2008) at http://opennet.net/research/regions/namerica.
[12] "Children's Internet Protection Act," Federal Communications Commission (Oct. 14, 2008) at http://www.fcc.gov/cgb/consumerfacts/cipa.html.
[13] "United States and Canada" at 1.
[14] "Europe," OpenNet Initiative (Oct. 14, 2008) at http://opennet.net/research/regions/europe.
[15] "Europe" at 7.
[16] "Europe" at 2.
[17] "Europe" at 3.

REFLECTIONS AND ANALYSIS

Determining which regulatory system takes the better approach is difficult because although each one regulates internet use, comparison is complicated because the ends sought are entirely different. The regulatory method employed by Saudi Arabia and China takes a "before the fact" stance to regulation in order to prevent misuse, whereas the system utilized in North America and Europe follows a more "after the fact" approach and largely punishes misuse only after it occurs. Instead, the critical inquiry should focus on what is the effect of these various regulatory policies in terms of access to information, global commerce, and overall technology accountability.

First and foremost, these policies can restrict the sharing of knowledge. The ability of individuals to share and receive useful information will be curtailed due to a fear of viewing or posting inappropriate materials. In addition, these policies have the potential to harm commerce. The internet opens up a wealth of opportunity for companies and individuals to conduct business globally, but the ability to undertake such transactions could be hampered if a party on either side of the transaction runs afoul of the regulation process imposed by its home country.

Aside from the social and economic issues engendered by these policies, two technical problems are created by the filtering process. Overblocking is the first technical problem, and as the name implies, it occurs when the filtering systems are so effective that they are, in fact, over effective.[18] A study conducted by OpenNet Initiative in Saudi Arabia found that the filtering system appeared to block sites falling outside the prohibited areas. For instance, it was found that the filtering system, SmartFilter, categorized some web sites incorrectly. While the system is largely effective, no system is perfect.

Another problem encountered relates to the use of proxy servers, which allow internet users to bypass the filtering system. The process is as follows: the user connects to an intermediary, which requests access to the blocked site and then forwards the ensuing page to the original user. The firewall imposed by the government is only able to see the user connect to the intermediary; it does not see the request by the intermediary to connect to the prohibited page, or the subsequent transfer of that page to the other party.[19] While this sneaky process can be subverted by adding the proxy site to the list of blocked sites, the proxy servers follow suit by merely changing their domain names and IP addresses to avoid the filtering.

One impression created by these regulatory schemes is that the internet can be a dangerous tool, a piece of technology that should be cautiously embraced only with numerous safeguards in place. They reflect concerns that the internet could be utilized as tool for malicious acts, as well as a tool that could upset or disturb the status quo of certain countries or areas of the world. Thus, it could be said that there is a slight element of trepidation as to how the internet may be used. If there is perhaps one universal truth, it is that change is an unavoidable. It occurs whether society is ready for it or not. Paradoxically, resistance to change can be deemed as much a certainty as change itself. Although society cannot prevent change per se, it does have the power to determine whether the change that does occur is beneficial or harmful. These regulatory policies are a means of adapting to the potential for change posed by the internet by regulating the effects of that change.

The fact remains that technological innovation is here to stay. Therefore, in addition to policing certain internet activities, the governments of these respective countries and all other countries may also benefit from encouraging responsible use of technology. An internet user who is educated as to good information practices, and is aware of the consequences for the internet's misuse, may likely be more responsible in his or her internet use. This might, in turn, help to slightly decrease the burden imposed upon the agencies charged with policing internet activity.

[18] "Internet Filtering in Saudi Arabia in 2004" at 16.
[19] "Internet Filtering in Saudi Arabia in 2004" at 9.

CONCLUSION

Advances in internet technology have enabled citizens in all areas of the world to interact with each other on a scale unprecedented in human history. More and more individuals from all parts of the world are logging on to the internet in ever increasing numbers. As a result of such widespread internet use, many countries have adopted regulatory schemes in order to monitor the types of information their citizens view on the internet. Some regulatory schemes are more extensive than others, involving complex filtering mechanisms and constant monitoring by ordinary, everyday citizens. While effective for the most part, these regulatory measures have practical flaws and possible negative effects in a variety of areas. Rather than trying to restrict and control technology, governments might be better served by embracing internet technology in a way that that will liven up the society and maximize the benefits that can be accrued from its use.

AUTHOR INFORMATION

Evan Peterson, JD, MBA teaches as an adjunct professor in the College of Business Administration at the University of Detroit Mercy. His areas of publication include scholarly articles on supply chain management, technology, decision making, innovative teaching methods, and the effects of legal the legal system on global business. He has been published in the *Journal of Business & Economics Research*, *American Journal of Business Education*, and the *College Teaching and Learning Journal*. His current research interests focus on the effects of securities law on transnational transactions

Dr. Gregory Ulferts is a Professor of Decision and Systems Sciences in the College of Business Administration. His scholarly activities have included research and publication on various topics related to management information systems, financial management, decision sciences, small business administration, and international business. Dr. Ulferts has served as a consultant in business and government in areas such as strategic and technology planning, operations and procurement management, analysis and design of systems, and business development.

REFERENCES

1. "Children's Internet Protection Act," Federal Communications Commission (Oct. 14, 2008) at http://www.fcc.gov/cgb/consumerfacts/cipa.html.
2. Council of Ministers Resolution 12 February 2001 (Oct. 7, 2008) at http://www.al-bab.com/media/docs/saudi.htm.
3. "Europe," OpenNet Initiative (Oct. 14, 2008) at http://opennet.net/research/regions/europe.
4. "Internet Filtering in China in 2004-2005: A Country Study," OpenNet Initiative (Dec 20, 2008) at http://opennet.net/studies/china.
5. "Internet Filtering in Saudi Arabia in 2004," OpenNet Initiative (Dec. 20, 2008) at http://opennet.net/studies/saudi.
6. "The Internet in the Mideast and North Africa: Free Expression and Censorship – Saudi Arabia" (Oct. 7, 2008) at www.hrw.org/advocacy/internet/mena/saudi.htm.
7. "Review of China's Internet Regulations and Domestic Legislation," International Center for Human Rights and Democratic Development (Oct. 7, 2008) at http://www.ichrdd.ca.
8. "Silenced – Saudi Arabia," Privacy International (Oct. 7, 2008) at www.privacyinternational.org.
9. "United States and Canada," OpenNet Initiative (Oct. 14, 2008) at http://opennet.net/research/regions/namerica.

NOTES