Chapter 5
Filtering Online Content in China

Jyh-An Lee
National Chengchi University, Taiwan

ABSTRACT

This chapter focuses on the Internet filtering mechanism the Chinese government adopted in order to prevent individual users from accessing foreign online content. Based on the case of Internet filtering in China, the author argues that when citizens are regulated by code rather than by the law, they will experience and perceive such code-based controls as natural. From the Chinese case, it should also be noted that the Internet's effects on politics varies depending upon how its architecture is designed.

INTRODUCTION

Increasingly, commentators claim that the Internet enables free flow of information and contributes to the creation of a freer and more open society (Deibert, 2002; Stevenson, 2007). This situation might be true in many of the world's countries today, but in some nations, such as China, the diffusion of Internet access and use has not led to increased freedom for Internet users (Stevenson, 2007; Farrell, 2007). Rather, in the People's Republic of China (i.e., mainland China), the national government has built probably the world's most sophisticated Internet filtering system. It is a system designed to block a number of foreign Websites that the national government views as a threat to the Chinese state. Interestingly, these blocked Websites include those pages containing information associated with Tibetan Independence, Taiwanese Independence, human right, Falun Gong, and other movements the ruling Communist Party sees as a threat or a challenge to its control (Stevenson, 2007; Faris & Villeneuve, 2008). The government, moreover, argues that such widespread and common filtering is desirable, for it can prevent the Western world from "dumping" information on China. In sum, it is online protectionism based upon real-world nationalism.

DOI: 10.4018/978-1-60960-833-0.ch005

During the early days of Internet access in China, some individuals optimistically believed access to and use of the Internet would make that medium a librating force that could help democratize China by opening new venues for political debate and discussion. On the contrary, the Chinese government has actually used online networking technologies to control the dissemination of information within the nation's borders. The government has adeptly used the Internet as a medium for advocating its own ideologies and perspectives while actively blocking any expressions of dissent. Thus, digital technologies have become the government's tool to tamp down political threats (Yang, 2009). For example, the Chinese government has ordered Chinese Internet carriers, like China Telecom, to deploy Cisco's equipment to block unwanted materials from entering China. This practice has, in turn, significantly changed the open nature of the Internet.

While the government can choose to use the law to regulate people's online behavior, controlling access to online information via technical architecture seems to be a much more effective approach. In fact, the Chinese government has been attempting to control online content via several different targets, including Internet content providers, individual consumers, and content on foreign Websites (Wacker, 2003; Yang, 2009). An investigation of the complex dynamics involved in this process could fill an entire library. For this reason, understanding the nature of government control of the Internet in China often requires one to examine the overall puzzle one piece – or component – at a time. This chapter, therefore, focuses on the topic of filtering mechanism used to prevent individuals in China from accessing foreign online content.

In examining this topic, this chapter will use Lawrence Lessig's (2006) pronouncement "code is law" as a mechanism for examining and understanding the Internet filtering system used by China's government. According to Lessig's ideas, technology can often fulfill a regulatory function or can be used in a way that has the same effects as regulation. The essential characteristic of code-as-regulator, for example, is that "[a] rule is defined, not through a statute, but through the code that governs" (Lessig, 2006, p.24). Through the application of Lessig's theory to online filtering practices in China (i.e., the "great firewall of China"), the author illustrates the implications this approach has for a government's ability to regulate online information sharing. The aim of the chapter is not to criticize the Chinese Internet filtering system, but rather to illustrate how a government can regulate and shape human behavior via architecture. Such an examination can provide important insights that can be used to examine how other governments or agencies use similar approaches to control online information dissemination in other contexts.

INTERNET FILTERING IN CHINA

The use of information and communications technologies (ICTs), including the Internet, in China has grown rapidly over the last decade due, in large part, to strong support from the Chinese government (Wacker, 2003). The Internet infrastructure in China has, as a result, experienced extraordinary growth in terms of scale, scope, and quality (Wu, 1996; Zhu & Wang, 2005). At the same time, the Chinese government has endeavored to control the dissemination of online information via various approaches, such as regulations and the use of certain filtering and monitoring technologies.

Within this context, the term "filter" generally refers to programming a router in such a way as to block data from entering or leaving a network (Human Rights Watch, 2006). The original objective of such programming is to give Internet service providers (ISPs) the means to control malicious or destructive programs such as viruses, worms, and spam (Human Rights Watch, 2006). Governments, however, can use the same technologies to selectively block certain kinds of online

information from being transmitted or received (Human Rights Watch, 2006). Such organized and coordinated blocking efforts by a government becomes "Internet filtering," which represents a technical approach to preventing Internet users from accessing specific Internet Protocol ("IP") addresses, Websites, or Web pages (Nawyn, 2007, p.505, 510). The reason for such filtering (i.e., blocking the access citizens have to certain online information) is, in most cases, because such blocked information is deemed too sensitive or too inflammatory by a particular government or agency (Zittrain & Palfrey, 2008).

In recent years, a number of countries have developed their own Internet filtering systems in response to a variety of political, moral, or security concerns (Zittrain & Palfrey, 2008; Faris & Villeneuve, 2008). In most of these cases, one of two types of Internet filtering techniques is used: the inclusion filter and/or the exclusion filter (Nawyn, 2007). The inclusion filter typically uses a "white list" to indentify Websites a government has deemed acceptable for its citizens to access online. An exclusion filter, by contrast, employs a "blacklist," which specifies Websites a government deems as "suspect" and thus uses technology to prohibit its citizens from accessing sites containing that information (Nawyn, 2007). In the case of exclusion filtering, the governments wishing to block online access to certain Websites usually request or require Internet service providers (ISPs) to implement the filtering task, for this approach is often the cheapest method to filter online information (Faris & Villeneuve, 2008).

The Chinese government has adopted the exclusion filter approach and has enacted this approach by requesting carriers/ISPs such as China Telecom to install Cisco's apparatus, which can drop information from at least three hundred IP addresses (Goldsmith &Wu, 2006;Faris & Villeneuve, 2008). Under this system, the Chinese government provided the carriers with a list of forbidden Websites and the addresses of those sites. The government then orders the ISP to use Cisco's equipment to block or prevent Chinese citizens from being able to access those sites (Goldsmith & Wu, 2006). These blocked sites include those for Amnesty International's (www.amnesty.org), Reporters without Borders (www.rsf.org), the BBC (news.bbc.co.uk), the Economist (http://www.economist.com), and the New York Times (http://www.nytimes.com) (Deibert, 2002; Farrell, 2007). Through this approach, certain online information gets dropped/cut off and can never reach end users located in the People's Republic of China.

From the government's perspective, the fact that new Websites are continuously and rapidly emerging means inclusion filters are seen as including/blocking too few Websites, while exclusion might block/exclude too few sites (Nawyn, 2007). In order to avoid potential over-blocking or under-blocking related to filtering, governments have started to employ the "content-analysis" technique as a new tool for Internet filtering (Nawyn, 2007, p.511). The content-analysis approach prevents users from accessing any Website or any URL path that contains or uses certain keywords the government has designated as suspicious or problematic (Nawyn, 2007; Faris & Villeneuve, 2008). One advantage to this content-analysis approach is that it does not require a government to incessantly update the white list or the blacklist used to filter online content. In China, for example, keywords for content analysis might include politically "hot button" issues such as Tibetan Independence, Taiwanese Independence, discussions of human rights violations, comments on the treatment of Falun Gong practitioners, etc. (Goldsmith &Wu, 2006).

In order to filter online information, the Chinese government has been continually installing a complicated technical system into the Internet ever since the initial days of online access in China (Nawyn, 2007; Stevenson, 2007). In 2002, Jonathan Zittrain and Ben Eldman (2003) worked with an end user in China to produce a list of foreign Websites blocked by the Chinese government.

The resulting list covered a range of organizations and topics the Chinese government blocked based on the perspective these subjects were a threat to the Chinese state. Of course, China is not the only country that filters away politically sensitive content. A number of other nations use this same approach, and these nations include Bahrain, Ethiopia, Libya, Iran, Myanmar, Thailand, Pakistan, Saudi Arabia, Syria, Tunisia, Uzbekistan, and Vietnam (Faris & Villeneuve, 2008).

But how can the Chinese government, or any government, control the online flow of information into the country? The answer is that the government of China worked with the U.S. hardware vendor Cisco to create a great firewall between Chinese citizens and online information (Goldsmith & Wu, 2006; Stevenson, 2007). This firewall, in turn, has altered Internet access in China in such a way as to convert it into, essentially, a huge intranet within the nation's borders (Deibert, 2002; Stevenson, 2007). It is estimated that this conversion process earns Cisco some USD$500 million each year in China (Stevenson, 2007, p.542). But Cisco is not alone. Other companies that provide filtering software to China include the U.S.-based companies Sun Microsystems (acquired by Oracle in 2009), Websense, and Bay Networksboth (Stevenson, 2007; Deibert, 2002). Through working with these organizations, the Chinese government has created a filter that is constructed on different layers of China's Internet. The central backbone/foundation of this system, however, is the physical infrastructure that links the domestic Internet in China to global networks that exist outside of its borders (Farrell, 2007; Nawyn, 2007).

Different from the firewalls established to protect enterprises' information security, the Chinese great firewall is set around the whole country (Goldsmith & Wu, 2006). The country's Ministry of Information Industry (MII) alone is authorized to build the network used to connect China to the global Internet. This arrangement, thus, ensures government control over the network and thus what individuals can use that network to access or distribute (Farrell, 2007; Human Rights Watch, 2006). Because this approach means online information can only enter the country through a limited number of points, the Chinese government is able to control the information via controlling these points (Goldsmith & Wu, 2006). Under this system, government control over information flow is coordinated via several Internet access providers (IAPs), "each of which has at least one connection to a foreign Internet backbone" (Internet filtering in China, 2007; Faris & Villeneuve, 2008, p.14). In this system, IAPs peer at three Internet exchange points (IXPs) run by the Chinese government, and these IAPs "grant regional Internet service providers (ISPs) access to backbone connections" (Goldsmith & Wu, 2006, p.93). Put differently, individual Chinese end users purchase Internet access from several thousand ISPs, and those ISPs are, in effect, retail sellers of Internet access purchased wholesale from the few IAPs in the country. Thus, by effective managing the IAPs and IXPs, the Chinese government is able to control information flowing from abroad and to do so in a relatively manageable way.

CODE-IS-LAW IN THE CONTEXT OF INTERNET FILTERING

This section applies the code-is-law theory to Internet filtering practices in China. This application reveals how strategic uses of programming, or code, can achieve a regulatory function akin to focused legal oversight or legal intervention. It also reveals how architecture shapes human behavior.

Code-is-Law Theory

As Lawrence Lessig (2006) has argued, code — be it related to software or hardware — can be designed to perform a regulatory function. As a result, governments can use code in strategic ways to create many of the same effects as legal regulation (Lessig, 2006;Faris & Villeneuve, 2008).

According to Lessig, the "code"/programming that controls the Internet effectively creates the Internet's architecture and thus its "laws" (Lessig, 2006, p.5-6). Therefore, if and how the Internet is regulated depends upon the architecture or the design of code. In Lessig's words, "[a] rule is defined, not through a statute, but through the code that governs the space" (Lessig, 2006, p.24). He goes on to explain that

> The software and hardware that make cyberspace what it is constitute a set of constraints on how you can behave…The code or software or architecture or protocols set [certain] features, which are selected by code writers. They constrain some behavior by making other behavior possible or impossible. The code embeds certain values or makes certain values impossible. In this sense, it too is regulation. (Lessig, 2006, pp.124-125)

In commenting on this situation, Lessig observes "We can build, or architect, or code cyberspace to protect values that we believe are fundamental, or we can build, or architect, or code cyberspace to allow those values to disappear" (Lessig, 2006, p.6). From a policy perspective, Lessig reminds legislators and regulators that they need to carefully consider what law and architecture, or code, can best advance their goals (Lessig, 2006). Although Lessig explicitly recognizes the fundamental differences between the law (regulation via statute) and the code (regulation via programming/design) (Lessig, 2006), some commentators criticize his theory as a disingenuous representation of the role of technologies in regulation (Wagner, 2005).

Theory Application

By building one of the most complicated Internet filtering architecture in use today, the Chinese government has crafted a new Internet architecture according to its own nationalist ideology (MacKinnon, 2008). This architecture differs markedly from its counterpart in the Western world where Internet architecture has been characterized as open and free (Stevenson, 2007; MacKinnon, 2008). Comparing the differences between the Internet architectures of China and of the West, it is not difficult for the average observer to understand Lessig's argument that "some architectures enable better control than others" (Lessig, 2006, p.24).

Law vs. Code as Regulation

The code-is-law theory raises interesting questions regarding the role and the use of code or architecture as an alternative to law-based regulation. When policymakers have regulatory options of code or law, they often consider the effectiveness of each approach and evaluate the costs and benefits associated with each method (Kesan & Shah, 2005). In many cases, the deciding factor becomes a matter of breadth (the scope of the activities that can be regulated) and depth (the degree to which certain activities can be regulated).

In the case of China, the government has employed several mechanisms to regulate the amount and the kind of online information available to citizens. Such mechanisms include a mix of law and code. This mixed approach involves legislation (i.e., law) (Deibert, 2002; Farrell, 2007; Nawyn, 2007; Stevenson, 2007; Yang, 2009) and legal enforcement activities – based on existing statutes (i.e., law) – that force search engines to remove inappropriate content (Lessig, 2006; Stevenson, 2007). They also include a heavy focus on using technologies (i.e., code) that filter online content (Stevenson, 2007).

In comparison to being regulated exclusively by law, regulation by code – or by a mix of law and code –usually makes it more difficult for citizens to determine when they are being regulated and when their access to content is being actively blocked or controlled. When, for example, a Chinese Internet user is unable to open a forbidden/blocked Website, the message that appears on the computer screen does not read or note that the "Website has been blocked by the Government" (Goldsmith & Wu, 2006, p.94). Rather,

that individual receive the same "site not found" message they would encounter if the related site was no longer online, if an incorrect URL had been used, or if a technical problem had arisen (Goldsmith & Wu, 2006). This kind of ambiguity means Chinese Internet users can never be sure when their failure to access certain sites represents a conscious attempt by the government to filter online content vs. some form of error or problem on the part of the user or the Website's sponsor/sponsoring organization.

A variety of code-based options exist for creating such ambiguous messages when engaging in active blocking of online content. Countries such as Tunisia, for example, use U.S.-developed SmartFilter software as a proxy filter. This software (i.e., code) uses "a blockpage that looks like the… browser's default error page" (Faris & Villeneuve, 2008, p.15). Uzbekistan's Internet filtering practices similarly hide the government's blocking actions by redirecting users to Microsoft's search engine www.live.com (Faris & Villeneuve, 2008). The software/code-based approach used by China is similar to the SmartFilter and the Microsoft strategies, but the Chinese government relies on a software/code developed in China by Chinese programmers (Human Rights Watch, 2006, p.10; Internet filtering in Tunisia, 2005). In all of these cases, the software (code) involved helps conceal the fact that a government or government agency is actively attempting to block citizens' access to certain sites and specific online information. It is thus quite difficult for Internet users in these nations to know if the problems they experience when accessing certain Websites is a matter of government intervention and regulation or involve an actual technical problem (Goldsmith & Wu, 2006).

This difficulty proves that Lessig's (2006) concern over code-based regulation is not over-stated. Lessig has long warned us that because regulating by code is not as transparent as regulating by the law, the former may weaken the democratic values of a society. Or, more simply stated, when citizens are regulated by code rather than by the law, they will "experience these controls as nature" (Lessig, 2006, p.138). This situation is what is now happening in China. When citizens are more accustomed to the fact that a great number of Websites cannot be viewed via their computers, they will be more likely to take such intervention and control for granted.

Of course, governments implementing filtering system can choose not to disguise the fact that they are blocking a Website. The government of Saudi Arabia, for example, uses SmartFilter and has decided to provide citizens with a blockpage that notifies them when the online content they have requested has been blocked by the government (Faris & Villeneuve, 2008). Theses blockpages also inform users of how to lift the block on a particular site (Faris & Villeneuve, 2008). However, Saudi Arabia is just one of the few countries willing to disclose such blocking information and to provide users with a method for addressing that block (Faris & Villeneuve, 2008). Therefore, when regulating by code, a government has the option of whether to disclose its intent in constraining behavior or to leave that factor ambiguous.

Using law or code to regulate might bring about different costs to a society. Law regulates behavior through an *ex post* approach. That is, a law will not be enforced until a violation takes place (Lessig, 2006). Although law enforcement might threaten potential punitive actions in the future, doing so might incur significant costs for the regulator. From the perspective of the Chinese government, for example, jailing violators who use the Internet to disseminate prohibited content could draw considerable international attention and create negative public impression of China on the global stage. Such factors might even counteract China's relatively recent attempts to re-brand itself as an enticing location for foreign investors. Thus, the costs associated with direct legal action are extraordinarily high.

In contrast, regulating by code is an *ex ant* approach. That is, although the adoption of

infrastructure-based Internet filtering might lead to certain criticisms regarding citizens' rights to information, such practices create a relatively low cost for the government (i.e., domestic complaints by citizens – and complaints that are easy to dismiss as "technical errors") as opposed to regulating by law and addressing international concerns expressed over public trials or public arrests. This cost-benefit balance might explain why the Chinese government prefers to rely on the code-based approach to Internet control (Faris & Villeneuve, 2008).

Fulfilling Policy Goals via Architecture Design

As a number of commentators have noted, the Internet has historically represented freedom and openness (Lessig, 2006). The original architecture of the Internet was designed as a distributed network that had no central control. Thus, by its very design, the Internet is quite difficult to control. The values underlying the original design of the Internet, moreover, included interconnectivity, openness, flexibility, and the lack of a pervasive centralized authority (Naughton, 2000). Nonetheless, such attributes do not exist in full within the architecture of today's Internet in China as the Chinese government is weaving nationalist ideology into the design of the Internet itself.

In truth, the Chinese government has dominated the design of the Internet in that nation, and had controlled the development and dissemination of the Internet there since its inception (Nawyn, 2007). As a result, the Chinese government was able to create an Internet architecture that mapped its preferences onto that technology – an approach that made the Chinese Internet significantly different from its counterpart in the Western world. China, however, is not alone in creating such a system. The government of Saudi Arabia, for example, has also created its own unique network that governs how Internet traffic flows through three "choke points" overseen by its Communications and Internet Technology Commission (Internet and Saudi Arabia, 2010). Both China and Saudi Arabia have designed centralized control points in the international gateway of their Internet architecture, and these points were built in mid 1990. Therefore, the filtering systems used by these nations have been implemented at the international gateway level regardless the cooperation from ISPs (Faris & Villeneuve, 2008). This approach might partly explain why these filtering systems work so well in both nations.

In understanding this code-based approach to filtering, it can be helpful to balance the restrictive nature of China's Internet with that of filtering attempts tried by nations where Internet infrastructure developed in a different way. Australia can, in turn, provide a good contrastive example to the approach taken in China. The Australian government has attempted to build a filtering system into its existing Internet architecture (Bambauer, 2009). However, because the country's Internet is as decentralized as its counterpart in other Western countries, the government can hardly find a controlling point to use for deploying an effective filtering system (Bambauer, 2009). The case of Australia helps explain how the cost and difficulty of implementing an Internet filtering system are quite high if a government did not take such system into consideration when structuring the Internet architecture from the very beginning.

The difference between the Australian and the Chinese Internet filtering systems also illustrates how a government can decide to regulate the subject architecture and how an open architecture can constrain government's power. As Lessig (2006) points out

[W]hether [the Net] can be regulated depends on its architecture. Some architectures would be regulable, others would not. I have then argue that government could take a role in deciding an architecture would be regulable or not. (pp.151-52)

Therefore, if the Internet architecture in a nation has been crafted as an open and decentralized one since its inception, a government's power to regulate the network is greatly reduced. In other words, an open architecture represents a constraint on the power or a government. This situation echoes Lessig's suggestion that the architecture of the Internet often checks government control over the Internet and the ideas carried on it (or the values embedded in it)(Lessig, 2006).

Despite these factors, the Chinese government is also attempting to create an Internet with positive externalities in relation to business and economic development, education, and information exchange (Deibert, 2002; MacKinnon, 2008). Although such an intention and the open nature of the Internet are somehow conflicting with state's control over the network in these cases, the Chinese government has managed to carefully maintain the balance of openness and control associated with its Internet policy. One commentator cited a 2005 edition of *People's Daily* explains this approach as follows:

As long as we use more ways of properly looking at the Internet, we can make use of the best parts, we go for the good and stay away from the bad and we use it for our purposes, and we can turn it around on them…we won't be defeated in the huge Internet wars by the various intranational and international reactionary ideological trends in various areas. (MacKinnon, 2008, p.33)

Interestingly, according to the Chinese government, the purpose of filtering online information is to block "spiritual pollution" from the country (Deibert, 2002). In sum, the Chinese government encourages taking advantage of digital technologies, but such usage cannot be done to undermine the state's control.

Architecture's Impact on Human Behavior

Although sophisticated users can always circumvent Internet filtering technologies and reach the blocked foreign sites, it is perhaps the case that the filtering system employed by the Chinese government has effectively prevented most Chinese users from accessing foreign Websites deemed "inappropriate" by the authorities (Nawyn, 2007). This situation is just one aspect of how architecture (i.e., code) regulates online behavior. However, the most profound consequence of this architecture is not that it immediately stops citizens' access to sensitive foreign content. Rather, the major factor to consider is how such uses of code are gradually shaping human behavior in cyberspace.

Together with other regulations and monitoring techniques imposed by the government, the Chinese are using the Internet in the way that has been prescribed by the nation's government. According to a 2005 study conducted by the Chinese Academy of Social Science, most Chinese Internet users look for entertainment services and information rather than try to find political discussions when online (MacKinnon, 2008; Yang, 2009). Influenced by the filtering architecture and perhaps other factors, not many Chinese Internet users seem interested in seeking out political information online.[1] Even university students, users who are often aware of technologies such as proxy servers that can circumvention of Internet filtering, appear not to be widely interested in taking advantage of existing technologies to reach blocked foreign Websites (MacKinnon, 2008). For those technologically savvy Chinese youth who do access blocked Websites, such actions are just a game that often lacks much (if any) political interest (Wacker, 2003). This phenomenon also echoes Lessig's (2006) argument that we cannot conclude that effective control of code is not possible only because complete control or perfect control does not exist.

By shaping citizens' online behavior via Internet architecture, the Chinese government has slowed the Internet's impact as a tool for political change (MacKinnon, 2008). In so doing, the government of China has reinforced its political authority. Obviously, in the short run, the Internet's role in enabling a public discourse around political and policy debates in China will be limited because of governmental control. Nevertheless, it is difficult to assess if and how circumvention of Chinese Internet filtering will make a difference in the long run.

Regulating the Intermediaries

As mentioned, Chinese Internet filtering is primarily implemented at international gateways an on the level of IAPs, IXPs, and ISPs. This practice provides a good example of how governments can regulate the decentralized architecture of the Internet. Because of the open and decentralized nature of the Internet, it is extremely difficult and costly to directly regulate each Internet user's behavior. Therefore, as Lessig (2006) has argued, it is more difficult to regulate scattered individuals than to regulate a few large firms. In the case of online content control in China, it would be more effective for the government to indirectly regulate users by directly regulating intermediaries like IAPs or IXPs. A possible explanation for such indirect regulation is that intermediaries, such as IAPs or IXPS, are far more susceptible to pressures from the government than are individual Internet users. As Jack Goldsmith and Tim Wu (2006) argue, "[W]hen government practices control through code, it is practicing a commonplace form of intermediary control" (p.72). In sum, it would be much less effective to control individual Internet users' access to foreign Website than to directly mandating Internet filtering implemented by IAPs or IXPs.

CONCLUSION

The Internet might have the power to eliminate sovereign boundaries in certain scenario, but this potential does not mean the Internet exists in a social and political vacuum. Conventional wisdom states that the Internet provides almost anyone with near-perfect access to information. However, this belief turns out to be not true in many countries that implement Internet filtering systems. Like many other countries around the world, China filters Internet content that the government has deemed "too sensitive for ordinary citizens." And it has done so with precision and effectiveness for a number of years.

In the case of China, we learn that Internet's impact on politics varies depending upon how its architecture is designed. As China has changed the original nature of the Internet, it has become obsolete for commentators to claim that the Internet will democratize the country. This chapter claims that the Internet filtering technology in China verifies Lessig's (2006) code-is-law theory. When a person fails to open a prohibited Website in China, he or she might view this factor as a technique problem rather than consider it government intervention of some sort. In this way, a code-based regulation is not as transparent as law-based regulation. Moreover, from the government's perspective, regulating by code might occasionally lead to much less cost than regulating by law. This belief is seems to be especially true in the context of the Chinese government regulating online flows of information.

The history of the Chinese Internet has made it unique and effective in filtering online information. Like Saudi Arabia, the government of China designed the nation's Internet architecture from the very beginning and did so with the aim of controlling and blocking information flow from abroad. Therefore, the Chinese government is able to filter or block information much more effectively and efficiently than other countries with a traditional open and decentralized network. Together, with

other surveillance mechanisms, Internet filtering has to a certain degree shaped the online behavior of Chinese citizens and has done so according to the government's preferences.

REFERENCES

Bambauer, D. E. (2009). Filtering in Oz: Australia's foray into Internet censorship. *The University of Pennsylvania Journal of International Law*, *31*, 493–513.

Deibert, R. J. (2002). Dark guests and great firewalls: The Internet and Chinese security policy. *The Journal of Social Issues*, *58*, 143–159. doi:10.1111/1540-4560.00253

Faris, R., & Villeneuve, N. (2008). Measuring global Internet filtering. In Deibert, R. (Eds.), *Access denied: The practice and policy of global Internet filtering* (pp. 5–27). Cambridge, MA: The MIT Press.

Farrell, K. (2007). The big mamas are watching: China's censorship of the Internet and the strain on freedom of expression. *Michigan State Journal of International Law*, *15*, 577–603.

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

Human Rights Watch. (2006). *Race to the bottom: Corporate complicity in Chinese Internet Censorship*. New York, NY: Human Rights Watch.

Internet.gov.sa. (2010). *Internet in Saudi Arabia*. Retrieved November 15, 2010, from http://www.internet.gov.sa/ learn-the-web/guides/ internet-in-saudi-arabia

Kesan, J. P., & Shah, R. C. (2005). Shaping code. *Harvard Journal of Law & Technology*, *18*, 319–399.

Lessig, L. (2006). *Code and other laws of cyberspace version*. New York, NY: Basic Books.

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

Naughton, J. (2000). *A brief history of the future*. Woodstock, NY: The Overlook Press.

Nawyn, M. D. (2007). *Code red: Responding to the moral hazards facing U*. S. Information.

October 10, 2010, from http://www.opennetinitiative.net/ studies/tunisia/ONI_Tunisia_ Country_Study.pdf.

OpenNet Initiative. (2005). *Internet filtering in Tunisia in 2005: A country study*. Retrieved

OpenNet Initiative. (2007). *Internet filtering in China: 2006-2007*. Retrieved March 26, 2010, from http://opennet.net/studies/china2007

Stevenson, C. (2007). Breaching the great firewall: China's Internet censorship and the quest for freedom of expression in a connected world. *Boston College International and Comparative Law Review*, *30*, 531–558.

Technology companies in China. *Columbia Business Law Review,2007*, 505-564.

Wacker, G. (2003). The Internet and censorship in China. In Hughes, C. R., & Wacker, G. (Eds.), *China and the Internet: Politics of the digital leap forward* (pp. 58–82). New York, NY: Routledge.

Wagner, R. P. (2005). On software regulation. *Southern California Law Review*, *78*, 457–516.

Wu, W. (1996). Great leap or long march: Some policy issues of the development of the Internet in China. *Telecommunications Policy*, *20*, 699–711. doi:10.1016/S0308-5961(96)00050-X

Yang, G. (2009). *The power of the internet in China. New York*. NY: Columbia University Press.

Zhu, J. J. H., & Wang, E. (2005). Diffusion, use, and effect of the Internet in China. *Communications of the ACM*, *48*, 49–53. doi:10.1145/1053291.1053317

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

Zittrain, J., & Palfrey, J. (2008). Internet filtering: The politics and mechanisms of control. In Deibert, R. (Eds.), *Access denied: The practice and policy of global Internet filtering* (pp. 29–56). Cambridge, MA: The MIT Press.

KEY TERMS AND DEFINITIONS

Content-Analysis Filter: An Internet filtering approach preventing users from accessing any Website or any URL path that contains or uses certain keywords the government has designated as suspicious or problematic.

Exclusion Filter: An Internet filtering approach employing a "blacklist," which specifies Websites a government deems as "suspect" and thus uses technology to prohibit its citizens from accessing sites containing that information.

Internet Exchange Point (IXP): A physical infrastructure through which Internet service providers (ISPs) exchange Internet traffic between their networks.

Internet Filtering: A technical approach to preventing Internet users from accessing specific Internet Protocol ("IP") addresses, Websites, or Web pages.

Internet Service Provider (ISP): An entity that provide its customers with access to the Internet.

Inclusion Filter: An Internet filtering approach using a "white list" to indentify Websites a government has deemed acceptable for its citizens to access online.

Router: A device that connects two or more computer networks, and selectively interchanges packets of data between them.

ENDNOTE

[1] In making this argument, I do not mean that Chinese citizens in the People's Republic of China are not interested in engaging in online political discussions. I only wish to point out that many of them might lose interested in finding sensitive political information online.