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