Minnesota Journal of Law, Science & Technology

Volume 13 | Issue 1 Article 6

2012

Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China

Jyh-An Lee

Ching-Yi Liu

Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China

Jyh-An Lee*

Ching-Yi Liu**

China's Internet filtering and censorship regime has received considerable global attention. The Chinese government has successfully regulated access to Internet content at the national level through technical means. Although some researchers optimistically viewed the Internet as a liberating force in China's democratic development, the Chinese government has actually been using network technologies to control online information and grafting its own ideology to the Net. Digital technologies have become the government's tool to tamp down political threats. The rise of the Chinese model of Internet control prompts many interesting questions associated with Internet law scholarship. This Article uses Lawrence Lessig's pronouncement "code is law" as a lens for understanding the Internet filtering system in China. Through the application of Lessig's theory to the great firewall of China, we aim to illus-

* Assistant Professor of Law, National Chengchi University, Taiwan; J.S.D., Stanford Law School; LL.M., Harvard Law School.

** Professor of Law, National Taiwan University, Taiwan; J.S.D., University of Chicago Law School; LL.M., Harvard Law School. The research underlying this Article was funded by a Fulbright research grant, National Taiwan University's Top University Project, and Taiwan's National Science Council.

The authors would like to thank Jian-Rong Li, Weiping Li, Kun Fan, Håkan Hydén, Anselm K. Sanders, and Kyu Ho Youm for their helpful comments. The authors are also grateful for the generous and valuable insights gleaned from the participants at the following events: the 7th Asian Law Institute Conference, Law in a Pluralist Asia: Challenges and Prospects, held at the International Islamic University in Kuala Lumpur, Malaysia (2010); the 2nd East Asian Law and Society Conference, Dialects and Dialectics: East Asian Dialogues in Law and Society, held at Yonsei University in Seoul, South Korea (2011); and the ILST Conference on Innovation, Competition, and Regulation at National Tsing Hwa University in Hsinchu, Taiwan (2011).

trate the theory's new implications and the government's policy options in cyberspace.

I. INTRODUCTION

Inspired by the successful Tunisian revolt in the spring of 2011, anonymous activists quickly emerged on the Internet calling for a "jasmine revolution" in China.[1] Completely intolerant of this radical appeal, Beijing orchestrated massive censorship of the Internet and phone services within the country in an attempt to prevent protesters from organizing demonstrations online.[2] The phrase "jasmine revolution" was filtered and could no longer be seen or searched for by Chinese end users.[3] This is just one of the numerous examples of how the Chinese government controlled citizens' behavior and online information via Internet filtering. In an environment where information flows pervasively, the most effective and efficient tool for government control is probably neither strict law nor military force, but technology itself.

There is no doubt that the Internet has unleashed vast information flows throughout global society. In the book *The World Is Flat*, Thomas Friedman notes that anyone with an Internet connection has the ability to find almost any information on the web.[4] A number of commentators have also asserted that the Internet enables a free flow of information and helps create a freer society.[5] This assertion has been true for some, but not all, countries in the world.[6] In China, the government has built

1. *See, e.g.,* Andrew Jacobs & Jonathan Ansfield, *Catching Scent of Revolution, China Moves to Snip Jasmine*, N.Y. TIMES, May 10, 2011, at A1; Austin Ramzy, *State Stamps Out Small "Jasmine" Protests in China*, TIME, Feb. 21, 2011, http://www.time.com/time/world/article/0,8599,2052860,00.html.

2. Andrew Jacobs, *Chinese Government Responds to Call for Protests*, N.Y. TIMES, Feb. 20, 2011, at A8; Ramzy, *supra* note 1.

3. Jacobs & Ansfield, *supra* note 1, at A1; Jacobs, *supra* note 2, at A8.

4. *See* THOMAS L. FRIEDMAN, THE WORLD IS FLAT: A BRIEF HISTORY OF THE TWENTY-FIRST CENTURY 75–77 (2007).

5. Ronald J. Deibert, *Dark Guests and Great Firewalls: The Internet and Chinese Security Policy*, 58 J. SOC. ISSUES 143, 143 (2002); Christopher Stevenson, *Breaching the Great Firewall: China's Internet Censorship and the Quest for Freedom of Expression in a Connected World*, 30 B. C. INT'L & COMP. L. REV. 531, 533–34 (2007).

6. Stevenson, *supra* note 5, at 534; *see also* Deibert, *supra* note 5, at 143 ("China . . . is a 'hard case' for those who argue that the Internet cannot be controlled"); Kristen Farrell, *The Big Mamas Are Watching: China's Censorship of the Internet and the Strain on Freedom of Expression*, 15 MICH. ST. J.

perhaps the world's most sophisticated Internet filtering system to block numerous foreign and domestic websites, which are viewed by the government as a threat to the Chinese state.[7] The blocked websites tend to be those containing information associated with Tibetan Independence, Taiwan Independence, human rights, Falun Gong, and other perceived threats to the Communist Party.[8] The government argues that such censorship practices are desirable, as they can prevent the Western world from "dumping" information on China. Maintaining social stability has become one of the most important goals of Internet filtering in China.[9] There should thus be little surprise when, in a public talk, Hu Jintao declared, "[w]hether [the government] can cope with the Internet is a matter that affects the development of socialist culture, the security of information, and the stability of the state."[10]

When the Internet was first introduced to China, some researchers optimistically viewed it as a liberating force in China's democratic development.[11] Researchers assumed that the free flow of information fostered by the Internet would ineluc-

---

INT'L L. 577, 590 (2007) ("The Internet has increasingly become a tool for security agencies to identify, monitor, arrest and imprison potential dissidents.").

7. *See, e.g.,* OPENNET INITIATIVE (ONI), *China*, *in* ACCESS CONTROLLED 449, 449 (Ronald Deibert et al., 2010) [hereinafter ONI CHINA]; Stevenson, *supra* note 5, at 536–37; Lijun Tang & Peidong Yang, *Symbolic Power and the Internet: The Power of a "Horse,"* 33 MEDIA, CULTURE & SOC'Y 675, 678 (2011). *See also* YUEZHI ZHAO, COMMUNICATION IN CHINA: POLITICAL, ECONOMY, POWER, AND CONFLICT 32 (2008) ("With the increasing sophistication of firewalls and filtering software, the survival time for offensive content in cyberspace has been progressively reduced.").

8. *See, e.g.,* Robert Faris & Nart Villeneuve, *Measuring Global Internet Filtering*, *in* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 5, 9, 12 (Ronald Deibert et al. eds., 2008); Stevenson, *supra* note 5, at 541; *see also* Farrell, *supra* note 6, at 587–88 ("China considers a wide range of topics sensitive and controversial . . . [I]ncluding the Tiananmen Square uprising, support for a free Tibet, the Falun Gong spiritual movement, criticism of China's human rights and social justice records, independent news media, and pro-democracy/pro-Western commentary.").

9. *See* ONI CHINA, *supra* note 7, at 456–67.

10. Xiao Qiang, *The Rise of Online Public Opinion and Its Political Impact*, *in* CHANGING MEDIA, CHANGING CHINA 202, 207–08 (Susan L. Shirk ed., 2011). For a different version of the English translation of this talk, see James F. Scotton, *The Impact of New Media*, *in* NEW MEDIA FOR A NEW CHINA 28, 41 (James F. Scotton & William A. Hachten eds., 2010).

11. *See, e.g.,* Yutian Ling, *Upholding Free Speech and Privacy Online: A Legal-based and Market-based Approach for Internet Companies in China*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 175, 215 (2011).

tably lead to a free society.[12] Nonetheless, the Chinese government has actually been using network technologies to control online information and grafting its own ideology to the Net. Such control has never been loosened, even during the 2008 Beijing Olympics.[13] Digital technologies have become a powerful tool with which the government tamps down political threats.[14] The Chinese government has ordered Chinese Internet carriers, like China Telecom, to deploy Cisco's equipment with the goal of blocking unwanted materials' entrance into China.[15] This practice has significantly changed the open nature of the Internet. Some researchers indicate that the Internet filtering in China "has become a paradigm of Internet censorship" for global society.[16]

The Chinese government has attempted to control online content via several different targets, including Internet content providers, individual consumers, and content on foreign websites.[17] Nonetheless, this Article focuses on the technological filtering mechanism that prevents Chinese Internet users from accessing unwanted online content. Lawrence Lessig's pronouncement "code is law" is particularly useful to our examination.[18] We use this idea as a lens through which to better understand the Internet filtering system in China. The essential characteristic of code-as-regulator is that "[a] rule is defined, not through a statute, but through the code that governs."[19]

---

12. *See, e.g.,* SHANTHI KALATHIL & TAYLOR C. BOAS, OPEN NETWORKS, CLOSED REGIMES: THE IMPACT OF THE INTERNET ON AUTHORITARIAN RULE 1–2 (2003); Stevenson, *supra* note 5, at 533–34.

13. ONI CHINA, *supra* note 7, at 468.

14. It is not easy to illustrate the relationships between the Internet and democracy because there are a number of complicated human experiences, institutions, and other factors in between. *See* GUOBIN YANG, THE POWER OF THE INTERNET IN CHINA 10 (2009).

15. *See, e.g.,* Derek E. Bambauer, *Cybersieves*, 59 DUKE L.J. 377, 379 (2009); Stevenson, *supra* note 5, at 542.

16. Ronald Deibert & Rafal Rohozinski, *Beyond Denial: Introducing Next-generation Information Access Controls*, *in* ACCESS CONTROLLED, *supra* note 7, at 3, 4.

17. *See, e.g.,* Gudrun Wacker, *The Internet and Censorship in China*, *in* CHINA AND THE INTERNET: POLITICS OF THE DIGITAL LEAP FORWARD 58, 69–70 (Christopher R. Hughes & Gudrun Wacker eds., 2003); Yang, *supra* note 14, at 48.

18. LAWRENCE LESSIG, CODE VERSION 2.0, 5 (2d ed. 2006) [hereinafter CODE VERSION 2.0].

19. *Id.* at 24.

The theory is that technology can fulfill a regulatory function or at least have the same effects as regulation does.[20] The Chinese case of Internet filtering elucidates the fact that although the government may 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. By applying Lessig's theory to the great firewall of China, we intend here to illustrate both some important novel implications of the theory and the Chinese government's policy options in cyberspace. Indeed, the Internet filtering practices in China have drawn considerable criticism, especially from the perspectives of democratic development and the value of an open Internet.[21] Nevertheless, the aim of our article is neither to evaluate the Chinese Internet filtering system nor to argue that technology can entirely replace the law. What we attempt to illustrate is how a government can shape human behavior via architecture design and the inimitable role played by code-based regulations in law enforcement.

II. INTERNET FILTERING IN CHINA

In China, information and communications technologies (ICTs), including the Internet, have been growing rapidly because of strong support from the government in recent years.[22] The Internet infrastructure in China has experienced extraordinary growth in terms of scale, technology, and quality.[23] The number of Internet users and its rate of growth have surpassed

---

20. *Id.*

21. *See* Robert Mackey, *Obama Walks China's "Great Firewall,"* N.Y. TIMES (Nov. 16, 2009), http://thelede.blogs.nytimes.com/2009/11/16/obama-on-chinas-great-firewall (quoting President Obama, "I am a big supporter of non-censorship . . . in the United States, the fact that we have free Internet—or unrestricted Internet access—is a source of strength, and I think [it] should be encouraged."). For other criticisms of Internet filtering, see William J. Cannici, Jr., *The Global Online Freedom Act: A Critique of Its Objectives, Methods, and Ultimate Effectiveness Combating American Businesses That Facilitate Internet Censorship in the People's Republic of China*, 32 SETON HALL LEGIS. J. 123, 147–54 (2007); Kevin Werbach, *The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing It Apart*, 42 U.C. DAVIS L. REV. 343, 367 (2008).

22. *See, e.g.*, Wacker, *supra* note 17, at 58.

23. *See, e.g.,* Wei Wu, *Great Leap or Long March: Some Policy Issues of the Development of the Internet in China,* 20 TELECOMM. POL'Y 699, 699–701 (1996); Jonathan J.H. Zhu & Enhai Wang, *Diffusion, Use, and Effect of the Internet in China*, 48 COMM. ACM 49, 50–52 (2005).

those of any other country in the world.[24] All the while, the Chinese government has endeavored to control the Internet's flows of information through such approaches as regulations and technology applications.

Early on in the widespread use of the Internet, filters were programs that, by manipulating routers, blocked data from entering or leaving a network.[25] The initial aim was to provide Internet service providers (ISPs) with means to control viruses, worms, and spam.[26] The same technology has been employed by the Chinese government to filter online information.[27] This technology was harnessed by the Chinese government to prevent Internet users from accessing "objectionable" Internet Protocol (IP) addresses.[28] The government blocks online information from citizens it deems too sensitive or inappropriate.[29] A great number of countries have developed their own Internet filtering systems because of political, moral, religious, or security concerns.[30] Traditionally, there have been two types of Internet filtering techniques: the inclusion filter and the exclusion filter.[31] The inclusion filter typically uses a "white list" to include websites that are permitted for browsing, whereas the exclusion filter employs a "blacklist," which specifies websites that users are prohibited from visiting.[32] Countries blocking websites usually request ISPs to undertake a two-pronged approach in blocking.[33] Countries begin with general IP blocking because it is the cheapest way to filter online information and switch to domain name service (DNS) blocking in response to complaints of over blocking.[34]

24. ONI CHINA, *supra* note 7, at 453.

25. HUMAN RIGHTS WATCH, RACE TO THE BOTTOM: CORPORATE COMPLICITY IN CHINESE INTERNET CENSORSHIP 9–10 (2006).

26. *Id.*

27. *Id.*

28. Marc D. Nawyn, Survey, *Code Red: Responding to the Moral Hazards Facing U.S. Information Technology Companies in China*, 2007 COLUM. BUS. L. REV. 505, 510–13 (2007).

29. Jonathan Zittrain & John Palfrey, *Introduction*, *in* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING, *supra* note 8.

30. *See id*. at 3; Faris & Villeneuve, *supra* note 8, at 7, 9.

31. Nawyn, *supra* note 28, at 510.

32. *Id*.; Ling, *supra* note 11, at 184; Jennifer Shyu, Comment, *Speak No Evil: Circumventing Chinese Censorship*, 45 SAN DIEGO L. REV. 211, 227 (2008).

33. Faris & Villeneuve, *supra* note 8, at 13–14.

34. *Id.* at 14.

The Chinese government has adopted the exclusion filter by requesting carriers, such as China Telecom, to install Cisco's apparatus, which can drop information from at least three hundred IP addresses.[35] The Chinese government provided the carriers with a list of forbidden websites and their addresses, and ordered these carriers to block the sites through Cisco's equipment.[36] Among these sites are those of Amnesty International, Reporters without Borders, the BBC, the Economist, and the New York Times.[37] In this way, certain information has been dropped from the Internet, never reaching many of China's domestic end users.

From the Chinese government's perspective, the inclusion filter usually includes too few websites, as new websites continuously emerge and pose new threats; likewise, the exclusion filter may exclude too few.[38] In order to avoid such under-inclusion and under-blocking, governments have started to exercise the "content-analysis" technique as a new approach to Internet filtering.[39] The content-analysis technique prevents users from accessing any website or URL path containing certain keywords designated by the government.[40] One advantage to a government's adoption of the content-analysis technique is that the censors do not have to incessantly update a white list or blacklist. In China, keywords for content analysis include "Tibetan independence," "Taiwan independence," "human rights," and "Falun Gong."[41] The scope of filtering is continuously increasing and is far beyond the "three Ts: Tibet, Tiananmen, and Taiwan."[42]

The Chinese government has built a complicated technological system and has integrated it into the Internet to filter

35. *Id.*

36. JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET: ILLUSIONS OF A BORDERLESS WORLD 93–94 (2006).

37. ANDREW MURRAY, INFORMATION TECHNOLOGY LAW 74 (2010); Deibert, *supra* note 5, at 147; Farrell, *supra* note 6, at 588.

38. Nawyn, *supra* note 28, at 510–11.

39. *Id*. at 511.

40. *Id*.; Susan L. Shirk, *Changing Media, Changing China*, *in* CHANGING MEDIA, CHANGING CHINA, *supra* note 10, at 1, 14; Cannici, *supra* note 21, at 131; Faris & Villeneuve, *supra* note 8, at 15; Ling, *supra* note 11, at 185; Shyu, *supra* note 32, at 227; Andrew W. Lloyd, Note, *Increasing Global Demand for an Uncensored Internet—How the U.S. Can Help Defeat Online Censorship by Facilitating Private Action*, 41 VAND. J. TRANSNAT'L L. 299, 303 (2008).

41. *See* GOLDSMITH & WU, *supra* note 36, at 96; Stevenson, *supra* note 5, at 541.

42. ONI CHINA, *supra* note 7, at 471.

online information, a process that has been ongoing since the digital network was built.[43] Through the help of an end user living in China, Jonathan Zittrain and Ben Eldman produced a list in 2002 identifying foreign websites blocked by the Chinese government.[44] The Chinese government had deemed the sites a threat to the Chinese state.[45] As we mentioned, China is obviously not the only country that filters out politically sensitive content. Other countries with similar motives include Bahrain, Ethiopia, Libya, Iran, Indonesia, Malaysia, Myanmar, Thailand, Pakistan, Saudi Arabia, Singapore, Syria, Tunisia, Uzbekistan, and Vietnam.[46] For different purposes such as blocking pornography, some democratic countries, including Australia, Britain, Canada, France, Japan, and New Zealand, filter online content as well.[47]

How is it that the Chinese government developed and implemented a complex system for controlling the flow of information into the country? In fact, the government built a great firewall with direct assistance from the U.S. hardware vendor Cisco.[48] This assistance made it possible for the whole country's Internet to evolve into a huge intranet.[49] It is estimated that the company earns USD $500 million each year in China for services rendered.[50] Other companies that provide filtering software to China include Sun Microsystems (acquired by Oracle in 2010), Websense, and Bay Networks, all of which are U.S. companies.[51] The filter has been constructed on different layers

43. Nawyn, *supra* note 28, at 512; Stevenson, *supra* note 5, at 540.

44. Jonathan Zittrain & Benjamin Edelman, *Internet Filtering in China*, 7 IEEE INTERNET COMPUTING 70 (2003).

45. *See* Nawyn, *supra* note 28, at 519–20.

46. Bambauer, *supra* note 15, at 382; Faris & Villeneuve, *supra* note 8, at 9–10; Shaojung Sharon Wang & Junhao Hong, *Discourse Behind the Forbidden Realm: Internet Surveillance and Its Implications on China's Blogosphere*, 27 TELEMATICS & INFORMATICS 67, 74 (2010).

47. Bambauer, *supra* note 15 at 382; Derek E. Bambauer, *Filtering in Oz: Australia's Foray into Internet Censorship*, 31 U. PA. J. INT'L L. 493, 516–17 (2009) [hereinafter *Filtering in Oz*].

48. *See, e.g.*, GOLDSMITH & WU, *supra* note 36, at 93; Lloyd, *supra* note 40, at 312; Cannici, *supra* note 21, at 132; Stevenson, *supra* note 5, at 541–42.

49. Deibert, *supra* note 5, at 147; Stevenson, *supra* note 5, at 540–41.

50. Stevenson, *supra* note 5, at 542.

51. *Id*; Deibert, *supra* note 5, at 148; *see also* Farrell, *supra* note 6, at 587 ("American engineers aided the Chinese in censorship by developing special routers, integrators, and special firewall boxes"); Wacker, *supra* note 17, at 69 ("It is ironic, therefore, that while the Western media frequently criticise Chi-

of China's Internet, but it has been constructed primarily at the "backbone level of China's network," the physical infrastructure that links the domestic Internet to global networks.[52]

The metaphor most frequently used in describing the Internet filtering in China is "the great firewall," an obvious play on the words 'the Great Wall' and 'firewall.'[53] The Great Wall of China was built by the ancient Chinese state to keep foreign invaders at bay; in an analogous way, the great firewall denotes China's attempt to block undesirable content from its "netizens." Different from the firewalls established to protect enterprises' information systems, the great firewall of China, as it were, forms a virtual ring around an entire country.[54] Authorized to build the firewall, the country's Ministry of Information Industry (MII) has had an extraordinary opportunity to ensure government control over China's overall Internet network.[55] Because online information enters the country through a limited number of connection points, the Chinese government can control the information by controlling these connection points.[56] Government control over information flow takes place via several Internet access providers (IAPs), "each of which has

---

na for obstructing the development of the Internet, it is Western firms that are supplying the technological means which enable China to carry out surveillance."). Some literature focuses on the legality of those U.S. companies' support of the Chinese filtering regime, especially on whether the companies are in violation of the Global Online Freedom Act of 2006. *See, e.g.,* Cannici, *supra* note 21, at 134–47; Ling, *supra* note 11, at 192–94; Nawyn, *supra* note 28, at 544–554; Shyu, *supra* note 32, at 230–31; Stevenson, *supra* note 5, at 545–58. In the meantime, human-rights supporters have publicly criticized Cisco's involvement with the Chinese filtering regime. *See, e.g., Tell Cisco: Stop Helping China Abuse Human Rights!*, ELECTRONIC FRONTIER FOUND., https://secure.eff.org/site/Advocacy?cmd=display&page=UserAction&id=504 (last visited Aug. 10, 2011).

52. *See* Farrell, *supra* note 6, at 587; s*ee also* Nawyn, *supra* note 28, at 511–12.

53. *See, e.g.,* Ling, *supra* note 11, at 177, 180, 184; ONI CHINA, *supra* note 7, at 460; Scotton, *supra* note 10, at 30–32; Shyu, *supra* note, 32, at 227; Katherine Tsai, *How to Create International Law: The Case of Internet Freedom in China*, 21 DUKE J. COMP. & INT'L L. 401, 415 (2011); Ethan Zuckerman, *Intermediary Censorship*, *in* ACCESS CONTROLLED, *supra* note 7, at 71, 73; David Pierson, *Great Firewall's Fall Opens the Web to China Briefly; Outage of Strict Internet Controls Lasts Several Hours*, WASH. POST, Jan. 5, 2010, at A9.

54. GOLDSMITH & WU, *supra* note 36, at 92.

55. Farrell, *supra* note 6, at 585; HUMAN RIGHTS WATCH, *supra* note 25, at 9.

56. YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM 267 (2006); GOLDSMITH & WU, *supra* note 36, at 93.

at least one connection to a foreign Internet backbone."[57] "IAPs peer at three Internet exchange points (IXPs) run by the state. IAPs grant regional Internet service providers (ISPs) access to backbone connections"[58] under the control of Chinese government. Under this regime, individual Chinese end users purchase Internet access from one of several thousand ISPs, and those ISPs are in effect retail sellers of Internet access provided wholesale by the small number of IAPs. Different from the decentralized Internet architecture in most countries around the world, most ISPs in China need to connect to the global network through one of the four state-controlled companies operating the IAPs and IXPs.[59] By effectively managing the IAPs and IXPs, the Chinese government can control information flowing into the country from abroad.[60]

The Chinese government has thus crafted the nation's Internet into two layers.[61] The lower layer is that part of the network where ISPs provide Internet access to consumers, while the upper layer is another set of connections where the lower layer can connect to the networks outside the country.[62] China has pioneered Internet filtering globally by building the national filtering system on the nation's backbone.[63] It has been reported that in the upper layer there are nine gateways connecting the nation's Internet to the global Internet network.[64] By controlling a number of key connection points in the upper layer, the government can control online information flowing from abroad.[65] Therefore, the filtering technologies are imple-

57. *Internet Filtering in China: 2006–2007*, OPENNET INITIATIVE, http://opennet.net/studies/china2007 (last visited Mar. 26, 2010); *see also* Deibert, *supra* note 5, at 147 ("Such funneled access provides the most important outer layer of control and the basis for 'firewall' technologies to be implemented that ostensibly block controversial or politically undesirable Web sites."); Faris & Villeneuve, *supra* note 8, at 14 ("[China's] blocking is done at the international gateway level affecting all users of the network regardless of ISP.").

58. OpenNet Initiative (ONI), *Country Summaries*, *in* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING, *supra* note 9, at 235, 264–65.

59. Ling, *supra* note 11, at 184.

60. *Id.*

61. Stevenson, *supra* note 5, at 540.

62. *Id.*

63. Deibert & Rohozinski, *supra* note 16, at 4.

64. Qiang, *supra* note 10, at 207.

65. *Id.* at 206.

mented on both layers of the Chinese Internet, which means that prohibited keywords and URLs are programmed into both the lower layer of ISPs and the upper layer of gateways controlled by the government.[66]

III. CODE-IS-LAW IN THE CONTEXT OF INTERNET FILTERING

This section applies the code-is-law theory to the Internet-filtering scenario in China. We will first introduce the theory and then explore its implications in the context of China's Internet filtering. We believe that China's Internet-filtering regime and its underlying policy implications exemplify the code-is-law theory quite well. By applying the theory to the subject matter, we can see from a policy perspective how code-based regulation is different from the law and how technological architecture regulates human behavior subtly.

A. CODE-IS-LAW THEORY

The code-is-law theory is most notably illustrated by Professor Lawrence Lessig, who has argued that code—software or hardware—can perform regulatory functions and can have the same effects as legal regulation.[67] The architecture of the Internet, including the languages and protocols underlying software and hardware, has determined how messages are moved from one place to another and how people perceive them.[68] Therefore, whether and how the Internet is regulated depends primarily on its architecture of code.[69] The code is law in the sense that it constrains what you may or may not do in cyberspace.[70] It enables certain activities while disabling others.[71] Lessig believes that the "code" which controls the Internet effectively creates the Internet's architecture and its "laws."[72] In a place like cyberspace, sometimes it is the code—not the law—that has the greatest impact on human behavior.[73] In Lessig's words, "A rule is defined, not through a statute, but through the code that governs the space."[74] According to him,

66. *See* Deibert & Rohozinski, *supra* note 16, at 4.
67. CODE VERSION 2.0, *supra* note 18, at 5.
68. *See id.*
69. *Id.* at 24.
70. *See id.* at 6.
71. *Id.* at 6.
72. *Id.* at 5–6.
73. *Id.* at 124.
74. *Id.* at 24.

> 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 . . . .[75]

Lessig has observed that "[w]e 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."[76] From a policy perspective, Lessig has reminded policymakers to try to identify the means by which states can best advance their goals.[77] Just as the code's functionality defines the digital universe where people act, it also defines the range of regulatory options for policymakers.[78] Although Lessig has explicitly acknowledged the fundamental differences between the law and code,[79] some commentators have criticized his theory as a disingenuous representation of the role of technologies in regulation.[80]

B. THEORY APPLICATION

It is possible that the Chinese government has built the most complicated Internet filtering architecture.[81] It is an architecture that has been crafted according to the preferences espoused in the state's nationalist ideology.[82] This is an example of how the government can use the Internet's architecture to enhance the ability to regulate the Internet. The Internet architecture of China has significantly deviated from that of the

---

75. *Id.* at 124–25.

76. *Id.* at 6 (emphasis omitted).

77. *Id.* at 129.

78. *Id.*

79. *Id.* at 5.

80. R. Polk Wagner, *On Software Regulation*, 78 S. CAL. L. REV. 457, 460–61 (2005).

81. *See, e.g.*, Rebecca MacKinnon, *Flatter World and Thicker Walls? Blogs, Censorship and Civil Discourse in China*, 134 PUB. CHOICE 31, 32 (2008); THE OPEN NET INITIATIVE, INTERNET FILTERING IN CHINA IN 2004–2005, 4 (Apr. 14, 2005), http://www.opennetinitiative.net/files/ONI_China_Country_Study.pdf ("China operates the most extensive, technologically sophisticated, and broad-reaching system of Internet filtering in the world."); *see also* Farrell, *supra* note 6, at 577 ("Compared to other states, China's censorship regime is pervasive, sophisticated, and effective.").

82. CODE VERSION 2.0, *supra* note 18, at 79–80.

Western world, which has been characterized by its openness and freedom.[83] Comparing the differences of these two types of Internet architecture, it is not difficult to understand Lessig's argument that "some architectures enable better control than others."[84] Chinese Internet filtering has provided an ideal example for Lessig's "code is law" theory. From the Chinese case, we can observe how code-based regulations function differently from law-based regulations. Although it is quite possible for policymakers to shape citizens' behavior and achieve state goals through technological design, the success of technology- or code-enabled government control depends on other factors. In the case of Internet filtering, China's exceptional censorship regime is attributable not only to the government's determined control of online information flows and the government's substantial investment in various technical measures, but also to the government's early intervention in the network design.

1. Law vs. Code as Regulation

The "code is law" theory raises interesting questions regarding the role of code or architecture as an alternative to the law. Policymakers that have regulatory options between code and law take into account costs, benefits, and the impact associated with each option.[85] In China, the government has employed several mechanisms to regulate online information available to its citizens. Such mechanisms include laws, forcing search engines to censor and remove inappropriate content, intensive cyber policing, and technologies that filter online content.[86]

---

83. Stevenson, *supra* note 5, at 533–34.

84. CODE VERSION 2.0, *supra* note 18, at 24.

85. *See, e.g.*, Jay P. Kesan & Rajiv C. Shah, *Shaping Code*, 18 HARV. J.L. & TECH. 319, 321–23 (2005).

86. CODE VERSION 2.0, *supra* note 18 at 80, 309; ONI CHINA, *supra* note 7, at 461; Shirk, *supra* note 40, at 14 (stating that "human monitors are paid to manually censor content proactively"); Cannici, *supra* note 21, at 130 (noting that there are 30,000 to 40,000 Internet police patrolling cyberspace in China); Lloyd, *supra* note 40, at 303; Scotton, *supra* note 10, at 29 (stating that an estimated 30,000 to 50,000 Internet monitors operate in China); Stevenson, *supra* note 5, at 532, 540–44; Qiang, *supra* note 10, at 207–08 ("[H]uman monitors are employed by both Web sites and the government to manually read and censor content."); *see* ZHAO, *supra* note 7, at 20. According to Professor Yuezhi Zhao, a great number of "cyber police squads . . . are patrolling Chinese cyberspace, deleting politically incorrect content in real time, blocking websites, monitoring networking activities of citizens, and tracking down and arresting offending individuals." ZHAO, *supra* note 7, at 20.

It is usually more difficult for citizens to realize that they are regulated by code than by the law. Therefore, as Lessig points out, the uniqueness of code-based regulations is "how they are experienced."[87] When citizens are regulated by code, rather than the law, they will "experience these controls as nature."[88] In circumstances where a Chinese end user never opens a forbidden website, the screen will not show "Blocked by the Chinese Government": it will only show the signal of "site not found."[89] Some countries, such as Tunisia, Iran, the United Arab Emirates, and Saudi Arabia, use SmartFilter software, developed by the United States company Secure Computing, as a proxy filter. [90] The software provides "a blockpage that looks like the. . .browser's default error page . . . ."[91] Likewise, Uzbekistan's Internet filtering hides the government's blocking efforts by redirecting users to Microsoft search engine www.live.com.[92] The software used by China is similar to SmartFilter, but has been developed "in-country."[93] All of this software has helped China conceal the fact that blocking is taking place. An Internet user who is unable to open a webpage may not know at all whether this problem is because of government intervention or a purely technical problem.[94] And in this way, code shapes and regulates human behavior more surely and subtly than the law.

The invisibility of Internet filtering in China proves that Lessig's concern over code-based regulation is not overstated.

---

87. Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 509 (1999).

88. CODE VERSION 2.0, *supra* note 18, at 138.

89. GOLDSMITH & WU, *supra* note 36, at 94; *see also* Bambauer, *supra* note 15, at 391 (noting that Internet users in China are not informed when they are prevented from reaching desired material, and instead, their Internet connections are reset).

90. Faris & Villeneuve, *supra* note 8, at 15; Stevenson, *supra* note 5, at 542.

91. Faris & Villeneuve, *supra* note 8, at 15.

92. *Id.* at 16.

93. HUMAN RIGHTS WATCH, *supra* note 25, at 10; *see also* Wacker, *supra* note 17, at 69 (stating that Chinese companies have begun to supply the government with filtering software). *See generally* OPENNET INITIATIVE, INTERNET FILTERING IN TUNISIA IN 2005: A COUNTRY STUDY (2005), *available at* http://opennet.net/sites/opennet.net/files/ONI_Tunisia_Country_Study.pdf (describing how SmartFilter works).

94. GOLDSMITH & WU, *supra* note 35, at 94; Bambauer, *supra* note 15, at 391; Deibert & Rohozinski, *supra* note 16, at 4.

Lessig has warned that since regulation by code is not as transparent as regulation by the law, the former may weaken a society's democratic value.[95] Code-based regulation is different from law-based regulation because it enables the government to regulate human behavior in a secret way and hides its choices or values behind the code.[96] This is what is now happening in China. When accustomed to the inaccessibility of many websites, citizens will be more likely to take such intervention and control (or technical problems, if that is the diagnosis) for granted. It is considerably more difficult to evaluate the justifications for and the true merits of Internet filtering than to apply those same types of evaluations to law-based regulation. Additionally, there is a relatively pronounced difficulty accompanying efforts to evaluate whether or not the original policy goals are realizable and remedies are available.

The Chinese government has never disclosed its filters' targets or its filtering systems' criteria, and this practice has garnered significant controversy.[97] According to the Chinese government, the purpose of filtering online information is to block "spiritual pollution" from foreign countries.[98] Nevertheless, most commentators believe that the goal of the Chinese government's Internet filtering and censorship is to minimize the discussions on sensitive political issues and to avoid the potential organization of online anti-government voices.[99] The accountability issue associated with Internet filtering can be illustrated in the controversy between the Chinese government and several human rights organizations on the strength and scope of China's Internet filtering. Although the Chinese government asserts that it filters only websites disseminating inappropriate material (e.g., content promoting terrorism or other types of violence), the aforementioned organizations believe that the coverage of the online content being filtered is much wider than what the government claims.[100]

Of course, governments implementing a filtering system can choose not to disguise the fact that they are blocking websites. They may decide to declare what material they block in

95. CODE VERSION 2.0, *supra* note 18, at 138; Lessig, *supra* note 87, at 535, 541.

96. Lessig, *supra* note 87, at 541–42.

97. Bambauer, *supra* note 15, at 394; Shyu, *supra* note 32, at 227.

98. Deibert, *supra* note 5, at 147.

99. *Id.*

100. Tsai, *supra* note 53, at 406.

laws or public announcements.[101] For example, Saudi Arabia has a government website explicitly disclosing the reasons for the state's Internet filtering.[102] Saudi Arabia using SmartFilter has decided to provide a blockpage notifying users that the requested content has been blocked.[103] The blockpage also informs users how they can lift the block.[104] However, Saudi Arabia is one of the few countries willing to disclose blocking information and to provide a way around the block.[105] The case of Saudi Arabia demonstrates that, when regulating by code, governments certainly have the option of whether to disclose their intent to censor information and to constrain behavior.

Costs associated with different types of regulation can constitute a crucial consideration for policymakers contemplating various regulatory options.[106] Use of the law and use of code differ from each other regarding the monetary costs of implementing and executing the given strategy.[107] Law regulates behavior through an ex post approach.[108] Law is not enforced until a violation takes place.[109] Although the threat of law enforcement applies to potential future violations, it may also incur significant costs for the regulator. From the perspective of the Chinese government, sending law-breakers—that is, people who have used the Internet to disseminate prohibited content—to jail or imposing other punishments on them may draw considerable negative attention internationally. The associated costs are extraordinarily high given China's increasing importance and visibility in the global community.[110] In contrast, regulating by code is an ex ante approach with much fewer political costs.[111] Although adopting the Internet-filtering techniques may lead to certain criticisms regarding citizens' right to information, the techniques' costs are lower for the government than would be law-based regulation. Moreover, the Chi-

101. Bambauer, *supra* note 15, at 394–95.
102. *Id.* at 390–91.
103. Faris & Villeneuve, *supra* note 8, at 15.
104. *Id.*
105. *Id.* at 16; Stevenson, *supra* note 5, at 536.
106. *See* CODE VERSION 2.0, *supra* note 18, at 310.
107. *Id.*
108. *Id.* at 124.
109. *Id.*
110. Lessig, *supra* note 87, at 541.
111. *Id.*

nese government could try to justify the practice by noting that many countries filter online content.[112]

Sometimes code-based regulation needs to be implemented via laws and policies. For example, Singapore's filtering system is implemented by law, which specifies the content filtered.[113] Nevertheless, when such laws and policies are announced, policymakers may experience considerable costs because this is an ex post approach, rather than a purely code-based regulatory approach. In May 2009, the Ministry of Information Technology initiated a project requiring that all computers made and sold in China be preinstalled with the filtering software Green Dam Youth Escort.[114] However, this project was cancelled because of strong public protest.[115] The filtering software was eventually required only for computers in schools and Internet cafes.[116] The Green Dam Escort initiative was actually an ex post measure that made citizens aware of the subject regulation, and thus, forewarned citizens could and did oppose the initiative before it went into effect. The government could not secretly install the filtering software on every computer without first somehow acquiring every private entity's cooperation. In other words, to some extent the government needed to use the law for this mandate. In sum, Internet filtering at the gateway level or in the upper layer incurs much lower costs and is obviously more effective than the aborted Green Dam Escort initiative.

2. Fulfilling Policy Goals via Architecture Design

As a number of commentators have illustrated, the history of the Internet stands for freedom and openness.[117] The original Internet architecture was designed as a distributed network without central control, and by its very design, the Internet is indeed quite difficult to control.[118] The values underlying the original Internet design include at least interconnectivity, openness, flexibility, and the lack of a pervasive centralized authority.[119] Nonetheless, such attributes do not perfectly exist in

112. Faris & Villeneuve, *supra* note 8, at 6, 13.
113. Bambauer, *supra* note 15, at 405.
114. ONI CHINA, *supra* note 7, at 472; Qiang, *supra* note 10, at 209.
115. Ling, *supra* note 11, at 184–85.
116. *Id.* at 185.
117. CODE VERSION 2.0, *supra* note 18, at 146.
118. *See* Shyu, *supra* note 32, at 215.
119. *See, e.g.*, JOHN NAUGHTON, A BRIEF HISTORY OF THE FUTURE: FROM RADIO DAYS TO INTERNET YEARS IN A LIFETIME 275–77 (2000); Shyu, *supra*

the Chinese Internet architecture, as the Chinese government has been weaving nationalist ideology into the Internet itself. Similar to the practice of contemporary Chinese law, where the Chinese government monopolizes law enforcement virtually in all areas, the Chinese government has dominated the design and the construction of China's Internet architecture since the inception of the Internet.[120] Therefore, the Chinese government could rather successfully "architecture" its preferences into the Internet, making it significantly different from manifestations of the Internet in the Western world.[121] In the case of Internet filtering, the Chinese government has understood that code, once it has evolved into law, becomes "a crucial focus of political contest."[122]

Another witnessing its establishment of a successful Internet filtering system, Saudi Arabia created its own unique network where Internet traffic flows through three "choke points" overseen by the Communications and Internet Technology Commission.[123] Both China and Saudi Arabia designed centralized control points in the international gateways to their respective Internet architectures when they were built in the mid-1990s. Therefore, the filtering systems have been implemented at the international-gateway level regardless of the cooperation or non-cooperation from ISPs.[124] Such centralized control points have enabled the Chinese and Saudi Arabian governments to exercise control over information not only viably but also effectively. Jonathan Zittrain explains the code-is-law theory: "If regulators can induce certain alterations in the nature of Internet technologies that others could not undo or widely circumvent, then many of the regulatory limitations oc-

---

note 32, at 215–16.

120. Nawyn, *supra* note 28, at 509, 513; Stevenson, *supra* note 5, at 540.

121. *See* YANG, *supra* note 14, at 44 ("[I]t is ultimately the government that has the power to decide what architecture to build and how regulatable the Internet remains.").

122. DAVID G. POST, IN SEARCH OF JEFFERSON'S MOOSE: NOTES ON THE STATE OF CYBERSPACE 133 (2009) (quoting CODE VERSION 2.0, *supra* note 20.)

123. *See Content Filtering in Saudi Arabia*, *General Information on Filtering Service*, COMMUNICATIONS AND INFORMATION TECHNOLOGY COMMISSION OF SAUDI ARABIA, http://www.Internet.gov.sa/learn-the-web/guides/content-filtering-in-saudi-arabia (last visited Apr. 1, 2010).

124. Faris & Villeneuve, *supra* note 8, at 14; *see also* Scotton, *supra* note 10, at 31 (stating that the effectiveness of Internet filtering in China depends on "a small number of state controlled backbone networks.").

casioned by the Internet would evaporate."[125]

Australia provides a good comparison with China and Saudi Arabia. The Australian government has attempted to build a filtering system into its existing Internet architecture.[126] However, because the country's Internet is as decentralized as its counterparts in other Western countries,[127] the government has been unable to find a control point for deploying an effective filtering system.[128] The case of Australia reveals that the cost and the difficulty of implementing an Internet-filtering system are quite high if the government in question fails to take such a system into consideration when structuring the country's Internet architecture from the outset. Other countries that, like Iran, operate decentralized filtering regimes have found it difficult to maintain consistent results because filtering techniques differ from various ISPs.[129] The difference between the Australian and the Chinese Internet-filtering systems illustrates how a government can determine the regulablility of the subject architecture and how open architecture can constrain a government's power. As Lessig has pointed out: "[w]hether [the Net] can be regulated depends on its architecture. Some architectures would be regulable, others would not. I have then argued that government could take a role in deciding whether an architecture would be regulable or not."[130] Therefore, if the Internet architecture has been crafted as an open and decentralized one since its inception, a government's power to regulate the network would be reduced. In other words, an open architecture represents a constraint on government power. This point echoes Lessig's suggestion that the Internet's architecture checks government control over both the Internet and the ideas it helps disseminate (or the values embedded in it).[131]

Although a controlled and centralized Internet facilitates effective government regulation, it may erect hurdles to a lot of online innovations and business ventures. Therefore, tensions do exist between the two policy goals of effectively controlled

---

125. JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 105 (2008).

126. *Filtering in Oz*, *supra* note 47, at 508.

127. *See, e.g.,* POST, *supra* note 122, at 86–87 (describing the decentralized nature of the Internet).

128. *Filtering in Oz*, *supra* note 47, at 509.

129. Faris & Villeneuve, *supra* note 8, at 16.

130. CODE VERSION 2.0, *supra* note 18, at 151–52.

131. *Id*. at 7.

Internet-based flows of information and a flourishing economy. The Chinese government has attempted to create an Internet with positive externalities in business and economic development, education, and information exchange.[132] This attempt, ideally resting on the open nature of the Internet, conflicts with the state's use of Internet-filtering and other regulatory Internet-targeting controls.[133] Consequently, achieving the two potentially incompatible policy goals has become perhaps the most critical challenge faced by Chinese Internet policymakers. It seems that, so far, the Chinese government's Internet policy has carefully maintained a tenable balance between openness and control. One commentator cited a 2005 *People's Daily* editorial to illustrate this viewpoint:

> 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, then we can turn it around on them . . . . [W]e won't be defeated in this huge Internet war by the various intranational and international reactionary ideological trends in the various areas. [134]

In sum, the Chinese government praises efforts to benefit from digital technology's advantages, but declares that use of digital technology must not undermine state control.[135] Main-

132. Deibert, *supra* note 5, at 147; MacKinnon, *supra* note 81, at 31.

133. *See, e.g.*, Deibert, *supra* note 5, at 151 ("[There is a] long-term incompatibility of China's restrictive Internet policies and its strong interest in promoting information and communication technologies through trade, foreign direct investment, and industrial policy."); Qiang, *supra* note 10, at 204 ("Since the introduction of the Internet in China, the Chinese Communist Party (CCP) and Chinese government have shown ambivalence toward its effects as a new force in Chinese society.").

134. MacKinnon, *supra* note 86, at 33 (citing G. Wu, *The Popularization of the Internet in China and the Bankruptcy of the Prediction in the New York Times*, PEOPLE'S DAILY, Nov. 30, 2005 http://www.zonaeuropa.com /20051130_1.htm).

135. *See, e.g.,* Shubo Li, *The Online Public Space and Popular Ethos in China*, 32 MEDIA, CULTURE & SOC'Y 63, 71 (2010) ("Since 2003, the Hu Jin-tao administration has successfully dismantled the online political discussion space, while at the same time maintaining the stability of the online public mood."); Shirk, *supra* note 40, at 13 (noting that the Chinese government embraces the Internet and invests more in controlling online content at the same time); Lokman Tsui, *An Inadequate Metaphor: The Great Firewall and Chinese Censorship*, 9 GLOBAL DIALOGUE 60, 62 (2007) *available at* http://www.worlddialogue.org /print.php?id=400 (describing Beijing's desire to simultaneously secure the Internet's economic advantages and limit the Internet's political disadvantages); Wang & Hong, *supra* note 49, at 73 ("The Chinese government has found a compromise between its desire to control the Internet and the need to become more competitive in the industry. . . . China's

taining this balance is a core goal of China's Internet policy, and goes far in explaining why, according to empirical evidence, the Internet promotes both freedom and control in China.[136]

3. Architecture's Impact on Human Behavior

Governments have various options in shaping citizens' behavior. A case in point: it has been reported that a great number of Internet police in China have been trying to shape public opinion by providing speeches favorable to the government.[137] Among other strategies, Internet filtering plays a crucial role in Chinese netizens' behavior and can have an impact that is much greater than that of China's Internet police.[138] Some researchers have argued that the goal of Internet filtering is "to shape citizens' information environments and thereby alter behavior."[139] Judging from the direct and indirect evidence presented below, Internet filtering has affected Chinese netizens' behavior in some intended and unintended ways.

Most users trying to open a webpage that does not display would try to visit a substitute webpage rather than wait for the originally targeted webpage to show up on their screens.[140] Users who are aware of the government filtering and censorship may still feel frustrated or angry when continuously being blocked from the content they wish to browse.[141] Although sophisticated users can always circumvent the Internet-filtering technologies and reach the blocked foreign sites,[142] there should be little doubt that the filtering system has effectively prevented most Chinese end users from accessing foreign websites deemed inappropriate by authorities.[143] This is just one aspect of how architecture regulates behavior. However, one of the most profound consequences of this architecture is not that it immediately limits citizens' access to sensitive foreign content,

---

model [is] a blend of economic openness and strict control over politics and dissent. . . .").

136. Lijun Tang & Peidong Yang, *Symbolic Power and the Internet: The Power of a "Horse,"* 33 MEDIA, CULTURE & SOC'Y at 675, 679 (2011); *see also* Tang & Yang, *supra* note 7, at 675, 679.

137. Cannici, *supra* note 21, at 130.

138. *Id.* at 131.

139. Bambauer, *supra* note 15, at 383.

140. *See* ZITTRAIN, *supra* note 125, at 105.

141. ONI CHINA, *supra* note 7, at 461; Bambauer, *supra* note 15, at 392.

142. Nawyn, *supra* note 28, at 514.

143. *But see* Zittrain, *supra* note 125, at 106 (optimistically and theoretically arguing that less savvy users could easily learn how to get around blocks).

but that it is gradually shaping human behavior in cyberspace.

These censorship policies, together with other regulations and monitoring techniques imposed by the government, have created a situation where some end users in China are inevitably using the Internet in ways consistent with the Chinese government's planned agenda. According to a 2005 study conducted by the Chinese Academy of Social Science, most Chinese Internet users look for entertainment, rather than political discussions, on the Internet.[144] Several recent research projects have reached similar conclusions: regarding their Internet habits, most Chinese netizens are more interested in online entertainment than acquiring political information.[145] Even most university students who are aware of technologies such as proxy servers that enable circumvention of Internet filtering are not interested in taking advantage of these technologies to reach blocked foreign websites.[146] For those Chinese youths who are technologically savvy enough to access blocked websites, such circumventions of censorship are frequently just a game in which political interest plays a peripheral role.[147] The above phenomenon echoes one of Lessig's arguments: we cannot reasonably conclude that effective control of code is impossible only because complete control or perfect control does not exist.[148] Although Internet filtering does not enable perfect con-

144. MacKinnon, *supra* note 81, at 33; *see* YANG, *supra* note 14, at, 28-31; *see also* Ian Weber & Lu Jia, *Internet and Self-regulation in China: The Cultural Logic of Controlled Commodification*, 29 MEDIA, CULTURE & SOC'Y 772, 776 (2007) ("[E]ntertainment is one of the main drivers of China's Internet development"). Chinese Internet users also use the Internet for a new form of online activism rising in China.

145. *See, e.g.,* Li, *supra* note 135, at 75 (stating that "the folk society . . . [of] the Chinese web, once demonstrated the aspiration for civic virtue as well as the capacity to organize democratic practices and to generate deliberative discussions, now is preoccupied with a crave for mind-paralyzing fun time."); Scotton, *supra* note 10, at 32 (introducing the China Internet Network Information Center's research finding that young Chinese Internet users have little interest in political information discussion or information in online environments); Wang & Hong, *supra* note 46, at 75–77 (finding that political interest is absent in the Chinese blogosphere); s*ee also* Scotton, *supra* note 10, at 26 (attributing the Chinese blogosphere's declining interest in political issues to strict government control).

146. MacKinnon, *supra* note 81, at 33; *see also* Scotton, *supra* note 10, at 31 (introducing Benjamin Bates' research on the ease of circumventing Internet filtering in China via proxy servers).

147. Wacker, *supra* note 17, at 72.

148. *See generally*, CODE VERSION 2.0, *supra* note 18, at 59–60 (noting that

trol over online information flows, it is an essential and effective policy tool for the Chinese government. By shaping citizens' online behavior via Internet architecture, the Chinese government has slowed down the Internet's role as a tool for political change[149] and, thus, has reinforced the Chinese government's political authority.[150]

Nonetheless, it would be naïve to jump to the conclusion that Internet filtering and other government measures completely eliminate subversive online content. Although some researchers believe that the Internet filtering together with strict laws has created powerful psychological pressure on Chinese netizens,[151] many netizens have worked out some ways to avoid censorship tools that would otherwise filter out personal politicized online expressions. For instance, it has become quite popular for Chinese netizens to use homophonies in their online expression to circumvent filtering technologies. Here we provide some representative examples. The pronunciation of *river crab* in Chinese is *he xie*, which is similar to that of *harmony*. Therefore, Chinese netizens use *river crab* in place of *harmony* when they are mocking the government's use of Internet filtering to create a harmonious society.[152] Another popular term used by Chinese netizens is "grass-mud horse," the pronunciation of which is *cao ni ma*, a near homophone of "fuck your mother" in Chinese.[153] It has been reported that the Chinese for

---

the "unregulability of the Internet was a product of design: that the failure of that network to identify who someone is, what they're doing, and where they're from . . . would be particularly difficult to enforce . . . . Not impossible, but difficult . . . .").

149. *See* MacKinnon, *supra* note 81, at 34.

150. In making this argument, we do not mean that Chinese citizens in the People's Republic of China are not interested in engaging in online political discussions. We only wish to point out that many of them might be losing interest in finding sensitive political information online.

151. Shyu, *supra* note 32, at 227; *see also* Lloyd, *supra* note 40, at 305 ("[T]he [Chinese] government also relies heavily on self-censorship resulting from the public's fear of possible punishment").

152. *See, e.g.*, HONGMEI LI, PARODY AND RESISTANCE ON THE CHINESE INTERNET, IN ONLINE SOCIETY IN CHINA: CREATING, CELEBRATING, AND INSTRUMENTALISING THE ONLINE CARNIVAL 71, 78–79 (David Kurt Herold & Peter Marolt eds., 2011); Dong Han, *"Use" Is an Anagram of "Sue": Cultural Control, Resistance, and the Role of Copyright in Chinese Cyberspace*, 7 GLOBAL MEDIA & COMM. 97, 108 (2011); Qiang, *supra* note 10, at 210; Tang & Yang, *supra* note 136, at 680; Michael Wines, A Mythical Beast (A Dirty Pun) Tweaks China's Web Censors, N.Y. TIMES, Mar. 11, 2009, at A1.

153. *See* Scotton, *supra* note 10, at 41; Tang & Yang, *supra* note 7, at 679–80.

grass-mud horse is now filtered in China because "the issue has been elevated to a political level."[154] Other popular homophones in China include *du cai* (meaning "poisonous jackal," a homophone of "dictator" or "dictatorship") and *min zhu* (meaning "talking pig," a homophone of "democracy").[155] In most cases, homophony will not cause comprehension problems, but it is very difficult for the government to ban all the homophonic keywords because the Chinese language is abundant in homophones.

Obviously, in the short run, the Internet's role in enabling a public discourse around political and policy debates in China has been limited because of governmental control. The filtering technologies have prevented rich online information from flowing into the country. Nevertheless, the Internet has become an essential part of many peoples' lives and has dramatically changed the way they communicate. Therefore, it is quite difficult to assess whether Internet filtering in the long run can really shape citizens' behavior according to the government's preference.

4. Regulating the Intermediaries

As mentioned above, the Chinese government implemented its Internet-filtering strategy primarily in the international gateway at the level of IAPs, IXPs, and ISPs. This practice provides a good example of how government can regulate a decentralized Internet architecture. Because of the open and decentralized nature of the Internet, it is extremely difficult and costly to directly regulate each Internet user's behavior. Professor Lessig has argued that it is more difficult to regulate scattered individuals than to regulate a few large firms in cyberspace.[156] As a result, it is no surprise that government censors' targeting of intermediaries has become a quite common and effective alternative for government control in the digital environment.

In the case of online content control in China, it would be more effective for the government to indirectly regulate those

154. Scotton, *supra* note 10, at 41.

155. KIRK ST. AMANT & SIGRID KELSEY, COMPUTER-MEDIATED COMMUNICATION ACROSS CULTURES 165 (2011).

156. *See* CODE VERSION 2.0, *supra* note 18, at 149–52; Lawrence Lessig, *The Limits in Open Code: Regulatory Standards and the Future of the Net*, 14 BERKELEY TECH. L.J. 759, 764 (2001).

users by directly regulating intermediaries like IAPs or IXPs. A possible explanation for such indirect regulation is that intermediaries such as IAPs and IXPs are far more susceptible to pressures from the government than are individual Internet users. Those providers have little choice but to comply with filtering-related regulations and directives imposed by central and local governments.[157] In summary, it would be much less effective for the government to control individual Internet users' access to unwanted website than to directly mandate Internet filtering implemented by IAPs or IXPs.

By the same token, ISPs are also the primary target in the Chinese government's efforts to control content over short message services (SMSs).[158] Because those ISPs cannot afford to disregard the state's control regime, they have consistently abided by their contracts with state-owned telecommunications operators and the government's political imperative.[159] The Chinese government applies the model of regulating intermediaries to instant-message transmission, as well. China's most popular instant messenger provider QQ received a mandate from the government to install keyword-blocking software whose basic function is to monitor users' online activities.[160] The Chinese government's placement of strict controls on search engines is another example of the government's regulation of intermediaries.[161] Because search engines have become the major tool for Internet users' information exploration, regulating search engines directly would be much more efficient and effective than regulating the behavior of individual users. In addition to regulating code, the Chinese government uses the law to control human behavior.[162] Among these regulations, the major laws to regulate online content impose significant obligations on ISPs as well.[163] These regulations prohibit ISPs from

157. Qiang, *supra* note 10, at 206–07.

158. ZHAO, *supra* note 7, at 33–34.

159. *Id.*

160. ONI CHINA, *supra* note 7, at 465.

161. *See, e.g.,* CODE VERSION 2.0, *supra* note 18, at 80, 309; JEFF JARVIS, WHAT WOULD GOOGLE DO? 176-77 (2009); ONI CHINA, *supra* note 7, at 461; Stevenson, *supra* note 5, at 532, 543–44.

162. *See* text accompanying note 60.

163. These laws include the "Provisions for the Implementation of the Interim Provisions Governing Management of Computer Information Networks in the People's Republic of China." Stevenson, *supra* note 5, at 557 (citing Measures on Internet Information Services, State Council Order No. 292, Sept. 25, 2000); *see* Standing Committee of Network Security; INTERNET

displaying any online content not approved by the government.[164] As Jack Goldsmith and Tim Wu argue, "when government practices control through code, it is practicing a commonplace form of intermediary control."[165]

Regulating content via intermediaries is not uncommon in other countries, which may have different ways of filtering online content. For example, in Australia, the Australian Communications and Media Authority (ACMA) has the power to issue a take-down notice to ISPs once the ACMA identifies prohibited or potentially prohibited content.[166] If such content is hosted abroad, the ACMA will filter it out by adding it to the blacklist via another intermediary.[167] Certainly, regulating intermediaries is not new in Internet law. Because ISPs are essential points of control in the flow of online information, they have become obvious and appropriate targets for government regulation.[168]

Professor Seth F. Kreimer wrote that the Internet "is a target-rich environment [for governments because it] . . . involves a series of electronic links; at each link, from user to originating computer to server to ISP to Internet backbone and back down the chain to the end user . . . ."[169] Because each country has its own ISPs that provide Internet access to individual users, governments naturally target ISPs for law-enforcement purposes. As a result, policymakers in different countries may impose different obligations on their local ISPs according to each country's unique set of general values and policy goals. These differences in obligations mean that the global Internet will be increasingly fragmented. In this sense, the Internet is local rather than global, especially when filtering or censorship is concerned.

FILTERING IN CHINA IN 2004–2005, *supra* note 81.

164. *See* Decision on Preserving Computer Network Security (promulgated by the Standing Comm. Nat. People's Cong. Dec. 28, 2000) (China) *available at* http://english.gov.cn/laws/2005-09/22/content_68771.htm.

165. GOLDSMITH & WU, *supra* note 36, at 72.

166. *Filtering in Oz*, *supra* note 47, at 503; Stevenson, *supra* note 5, at 535.

167. *Filtering in Oz*, *supra* note 47, at 499, 505; Stevenson, *supra* note 5, at 535.

168. Seth F. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 18–27 (2006).

169. *Id.* at 16.

IV. CONCLUSION

The Internet may have the power to eliminate sovereign boundaries in certain scenarios, but this openness does not mean that the Internet exists in a social and political vacuum. Conventional wisdom would have us believe that the Internet provides anyone with perfect access to information. However, this assumption turns out to be patently false in many countries that implement Internet-filtering systems. Like many other countries around the world, China filters Internet content that the government deems too sensitive for ordinary citizens. And it has done so with precision and effectiveness.

As China has stripped away much of the openness attributable to the Internet on Chinese soil, commentators' claim that the Internet will democratize the country has become obsolete. In fact, the Internet in China has endowed certain types of government control with political significance. In this Article, it is found that the development of Internet filtering in China verifies Lawrence Lessig's code-is-law theory. A code-based regulation, like Internet filtering, is not as transparent as the law. Moreover, from the government's perspective, regulating by code may occasionally incur costs that are much lower than those involved in regulating by law. This is notably true in the Chinese context of regulating the flow of online information. The unusual history of the Chinese Internet has made it unique and effective in filtering online information. Like Saudi Arabia, China designed its Internet architecture early on in the public's use of the Internet, the aim being to control and block information flows from abroad. As a result, China has been able to filter or block information much more effectively and efficiently than those countries with traditional open and decentralized networks. Together with other surveillance mechanisms, Internet filtering has, to a certain degree, shaped Chinese citizens' online behavior according to the government's preferences. Nonetheless, because of the dynamic nature of the Internet and of information in general, it is difficult to assess at this moment whether Internet filtering can always be an effective tool for government control over the online information.