Internet Development, Censorship, and Cyber Crimes in China

Bin Liang¹ and Hong Lu²

Abstract
Since its first Internet connection with the global computer network in 1994, China has witnessed explosive Internet development. By the end of 2008, China replaced the United States as the largest Internet user of the world. Although China enjoyed tremendous economic benefits from Internet development, the Chinese government has tried to maintain tight control over the telecommunications industry and the public Internet use, and fight increasing cyber crimes. In this article, we first review historical development of Internet use in China and then focus on China’s Internet censorship and its regulatory control. Next, we explore how the Internet is actively utilized by both the government and the public to serve political and civic functions. Finally, we discuss cyber crimes as an emergent form of crime in China and examine how the Chinese government reacts to these offenses. Lessons from Internet use and regulation in China are also discussed within the context of China’s economic, political, and legal conditions.

Keywords
Internet, Internet censorship, Internet regulation, cyber crime, China

Introduction
Internet use and development is one of the most important inventions in the second half of the 20th century. It has transformed people’s lives and its impact is beyond one’s imagination and is still to come in many aspects.

¹Oklahoma State University–Tulsa
²University of Nevada, Las Vegas

Corresponding Author:
Bin Liang, Associate Professor, Department of Sociology, Oklahoma State University–Tulsa, 700 North Greenwood Avenue, Main Hall, 2223, Tulsa, OK 74106
Email: bin.liang@okstate.edu
China’s Internet use and development did not begin until a decade later after its economic reforms. Its growth has outpaced other countries, and China by 2008 has the largest number of Internet users in the world. What accompanied China’s Internet development is the government’s tight control and regulation over Internet infrastructure, its commercial and social use, and its potential political ramifications. Despite being criticized by human rights groups and activists, China’s Internet censorship system seemingly functions well as the “Great Firewall of China.”

On the other hand, there is high hope that Internet use and development in China will eventually lead to democracy in the largest country, testing the hypothesized relationship between Internet use, free flow of information, and democracy. Indeed, the Internet has profoundly transformed the Chinese society in the last decade, even in China’s political-legal reforms. However, democracy is still as far-reaching as it once was and the role of the Internet in this reform has been constrained by the wider socio-political and economic context of China.

Like many other nations, China’s Internet use and development also witnessed surging cyber crimes, many in traditional forms but others as new phenomena. Unfortunately, this appears to be the least studied subject. Key questions such as the status of cyber crimes in China, the features of such crimes, and the government’s response to these crimes are rarely answered.

In this article, we briefly review the historical development of Internet use in China and its regulation. We also explore the issues of China’s democracy on Internet use, the political and civic functions of the Internet, and emergent forms of cyber crimes and the Chinese government’s response to them. These issues are all discussed within China’s wider social, economic, political, and legal conditions.

**Internet Development: Beyond the Great Wall, Joining the World**

China’s Internet development has come a long way in a very short time (Wu, 1996). Though China initiated the economic reform and “open-door” policy in the late 1970s and early 1980s, the use and development of Internet did not appear until almost a decade later. In the late 1980s, China’s academia, with the support of foreign partners, began to explore Internet use. In September 1987, a symbolic message “Beyond the Great Wall, Joining the World (yueguo changcheng, zouxiang shijie)” was sent from China via email (Qiu, 2003). In 1994, China connected its first international dedicated line to the Internet and became the 71st country to register onto the global computer network and received CN as the highest level domain name (Lu et al., 2002; Taubman, 1998).

Similar to other countries, China’s early efforts at creating Internet networks were focused on the scholarly exchange of information. Its first networks reflected these interests, including the China Academic Network (CANET), China Research Network (CRNET), and the Institute of High Energy Physics (IHEP) Network (Harwit & Clark, 2001). Soon after, China began to realize the significance of computer information
technology in its economic development and encouraged fast development of Internet in commercial use to embrace the new information era. As a result, China witnessed tremendous expansion of Internet use.

China’s total estimate of Internet users was only a few thousands by the mid-1990s but grew exponentially afterwards. Based on annual survey data by the Chinese Internet Network Information Center (CNNIC), Internet uses in China reached 2 million in 1998, surpassed 100 million in 2005, and rose to 298 million by the end of 2008. China also replaced the United States as the largest Internet user of the world. Despite its uneven distribution across geographical regions (e.g., rural areas carry fewer users than urban areas), China’s Internet coverage of its total population (23% by 2008) already passed the world average coverage (22%) (CNNIC survey reports at http://www.cnnic.cn/en/index/00/02/index.htm; Dowell, 2006; Srikantaiah & Dong, 1998; Tan, 1999; Tai, 2006; Wang, 2002).

Along with the growth of Internet users, other indexes of Internet development are impressive as well. Since the official establishment of the CNNIC in 1997, the number of registered domain names increased from a little more than 4,000 in 1997 to 1.8 million in 2004 and reached nearly 17 million by 2008; the number of registered Web sites increased from less than 4,000 in 1997 to almost 3 million by 2008.

China’s Internet development has been bound to its overall economic development in general and the growth of its telecommunication industry in particular over the years. For example, in 1997, the numbers of fixed-line telephones and mobile phones were about 70 million and 13 million, respectively (annual data reported by the National Bureau of Statistics of China). By 2001, China surpassed the United States to become the world’s largest mobile telecom market and its total number of mobile phone users reached nearly 373 million by 2005 while the number of fixed-line telephone reached 342 million (Tai, 2006, p. 119). CNNIC (2008) estimated that more than 117 million Internet users accessed Internet via their mobile phones by 2008 and more than 90% of Internet users (270 million) had broadband Internet access.

In comparison to other nations (e.g., Abbott, 2001; Fan, 2005; Srikantaiah & Dong, 1998; Xue, 2005), the intervention and domination by the Chinese government has been the major distinctive feature of China’s Internet development. The Internet boom was made possible largely because of a “state-centric strategy for comprehensive informationization” (Hartford, 2000). This state-precipitated development of the Internet also ensured the state ownership and control of main Internet infrastructure and the use of Internet.

**Internet Censorship and Regulation: The Great Firewall, Self-Censorship, and Multidimensional Regulations**

Given China’s single-party political system and its heavy intervention in Internet development, its Internet censorship and regulation has evolved into a comprehensive, multidimensional system that governs Internet infrastructure, commercial and social use as well as legal domains.
The great firewall. The predominant method of control at the infrastructure level is restriction of access to Internet information (e.g., regulating access and content, monitoring Internet use). At the national level, only government-approved agencies and businesses are permitted to establish an Internet Interconnecting Network (also called “backbone network” or  gugan wangluo in Chinese) and to license the operation of Internet service providers at the next tier. These networks are required to go through international gateways located in Beijing, Shanghai, and Guangzhou and are subject to governmental control and regulation (see, for example, Cheung, 2006; Fan, 2005; Perritt & Clarke, 1998; Tan, 1999). At the next tier, all private Internet service providers are licensed through one of these Internet Interconnecting Networks and are required to install filters to block away undesirable content. The bottom tier involves Internet users who are required to register with Internet service providers to gain Internet access.

The Chinese government has also been constantly updating its surveillance and control system. Take the “Golden Shield” project for example. As one of the “Three Golden Projects,” it was first proposed in 1993 and approved in 1998. This project, still going on, is part of the Great Firewall of China. Its main function is to censor and control Internet information both domestically and globally (Dowell, 2006). In addition, China has established a special Internet police force to assist its Internet surveillance. In August 2000, Anhui became the first province to set up Internet police force and 20 others followed suit later; more than 300,000 personnel were reportedly hired nationwide by the end of 2000 (Endeshaw, 2004; Harwit & Clark, 2001; Keith & Lin, 2006; Tai, 2006).

Prohibited activities/materials/information related with the Internet are placed in nine broad categories by the Chinese government. These include information that (a) is contrary to the basic principles that are laid down in the Constitution, laws, or administration regulations; (b) is seditious to the ruling regime of the state or the system of socialism; (c) subverts state power or sabotages the unity of the state; (d) incites ethnic hostility or racial discrimination, or disrupts racial unity; (e) spreads rumors or disrupts social order; (f) propagates feudal superstitions; disseminates obscenity, pornography, or gambling; incites violence, murder, or terror; instigates others to commit offences; (g) publicly insults or defames others; (h) harms the reputation or interests of the state; or (i) has content prohibited by laws or administrative regulations (pp. 13-14; Cheung, 2006; Dai, 2000; Human Rights Watch, 2006, pp. 18-19).

Despite its great effort, the effectiveness of China’s Internet censorship is unclear. Although some argued that it is very questionable (e.g., Deibert, 2002; Lacharite, 2002), others viewed it as effective (e.g., Kalathil & Boas, 2001) and even as “the most sophisticated effort of its kind in the world” (Open Net Initiative, 2005).

Though there are many ways to circumvent the government’s Internet filtering, such as use of proxy servers, private emails, and manipulating one’s search (Abbott, 2001; Dai, 2000; Deibert, 2002; Lacharite, 2002; Zittrain, 2004), there still lacks knowledge of how many Chinese Web surfers adopt such approaches (Human Rights
Watch, 2006). One common finding is the inconsistent enforcement of China’s Internet filtering. Studies show that Internet blocks have come and gone, and the content of blocks also varies from time to time, most likely because of the fact that there is no coherent and consistent decision-making process (Hartford, 2000; Sohmen, 2001). Another finding is the extensive scope of China’s censoring, covering not only political issues but also issues such as crimes and economics (Hartford, 2000; Open Net Initiative, 2005). Empirical testing of the Chinese filtering system also found that the filtering system is rather dynamic and has been self-changing and refining over time (Open Net Initiative, 2005). In sum, China’s Internet control represents an “imperfect control,” aiming at keeping the vast majority from sensitive materials and preventing the nonconforming small minority from mounting a real challenge (Hartford, 2000).

Self-censorship. In addition to setting up technological restrictions to Internet information at the infrastructure level, the Chinese government also put high pressure on businesses and individuals to conform to its censorship in Internet commercial and social use. For instance, governmental regulations after 2000 set a priority instituting self-regulation and increasingly delegated policing power to nonstate sectors (Cheung, 2006; Endeshaw, 2004). Given their limited choices, high governmental pressure, and potential stiff penalties, adopting “self-regulation” and complying with state censorship seems to be the only viable option to business owners. In March 2002, for example, the Internet Society of China (ISC) issued a “Public Pledge on Self-Discipline for the China Internet Industry” (zhongguo hulianwang hangye zilü gongyue) in Beijing, establishing the foundation of domestic self-discipline mechanism (Endeshaw, 2004, CNNIC Web site). Given the broad and vague nature of government regulations, many businesses decided to play safe and end up with even more sweeping censor mechanisms (e.g., Human Rights Watch, 2006; Sohmen, 2001).

China’s surveillance system also target foreign business investors in China. The Chinese government gained technical support from foreign companies (e.g., Cisco, Sun Microsystems) in building its Internet infrastructure (e.g., Qiu, 2003), yet required Internet corporations such as Google, Inc., Yahoo!, Inc., Microsoft Corp., and Skype to comply with Chinese laws and regulations and to modify their Chinese version of search engines to filter sensitive information (Battelle, 2005; Fry, 2006; Hinman, 2005; Human Rights Watch, 2006). In 2002, Yahoo! also voluntarily signed the “Public Pledge on Self-Discipline for the China Internet Industry” (Dowell, 2006; Human Rights Watch, 2006). Despite strong criticism from human rights activists, these corporations have justified their censoring as necessary compliance with local laws to run business (and the Chinese market is simply too large to ignore). Moreover, foreign investors are specifically prohibited from owning, operating, or managing telecommunications services in China. Even after its entry into the World Trade Organization (WTO) in 2001, the Chinese government carefully controlled its telecommunication industry: foreign ownership is capped at 50% for value-added services and 49% for mobile telephone and domestic and international services (Pangestu & Mrongowius, 2002). Despite great hope by many (e.g., Dai, 2000; Deibert, 2002;
Harwit & Clark, 2001), the impact of WTO on China’s democracy in general and Internet censorship and control in particular remains unclear.

**Multidimensional regulations.** China’s legislation over Internet use and development has definitely grown and become more comprehensive over time. The increasing legislation also accompanied a series of changes in regulating agencies. As Tan (1999) delineated, the pre-1994 era represented an experimental era characterized as a fragmented structure without a single authority; from 1994 to 1998, China witnessed a transitional period, during which a single regulatory coordinator, the State Council’s Steering Committee of National Information Infrastructure, was established to negotiate and cooperate with other governmental agencies; in 1998, the Chinese government merged the existing Ministry of Post and Telecommunications with the Ministry of Electronics Industry to form one major single regulator, the Ministry of Information Industry (MII). Since then, the MII has become the dominant regulator of China’s telecommunications industry.

Given the complex and comprehensive scope of China’s Internet regulations, however, many other agencies (e.g., State Council, Ministry of Public Security (MPS), Ministry of Culture, and State Secrets Bureau) still have regulatory authorities in Internet use and development and remain actively involved (Open Net Initiative, 2005; Zheng, 2008). While making comprehensive Internet control possible, the involvement of multiple agencies and players also creates inefficiency, redundancy, uncertainty, and confusion (Endeshaw, 2004; Qiu, 2003). In addition, the lack of separation between state-owned operation and regulation (e.g., the MII is closely involved with China Telecom which owns CHINANET) may enable agencies with regulatory power to directly obtain financial gains (Sohmen, 2001).

One direct result of such a multidimensional regulatory system is the comprehensive scope of agency regulations. Laws and regulations enacted over time cover a broad range of issues from infrastructure construction to Internet network security, Internet domain names registration, computer encryption, management of online business operation, Internet news reporting and publication, and copyright protection. For example, regulations in April 1996 stipulated that all domestic computer systems could only be connected to Internet Interconnecting Networks via the gateways established and managed by the Ministry of Post and Telecommunications (which was later merged into the MII). The *Administration of the Maintenance of Secrets in the International Networking of Computer Information Systems Provisions* in 2000 prohibited Internet users from sending state secrets via email or discussing state secrets in Internet chat rooms or on bulletin boards. The *Administration of Engagement by Internet Sites in the Business of News Publication Tentative Provisions* in 2000 and *Interim Regulations for the Administration of the Internet Publications* in 2002 tightened control over Internet news reporting and publication. Based on both, the only bona fide news is official news from government sources such as the Xinhua News Agency and the *People’s Daily* (renmin ribao); Internet organizations cannot cite foreign news without official approval; all online publications must be inspected and approved as well. The *Regulations on the Administration of Business Sites of Internet Access*
Services in 2002 (replacing the old one in 2001) requires that Internet business owners (e.g., Internet cafés) keep records of users’ information for 60 days for government inspection purpose.

Besides its broad scope, there are a number of other features about China’s legislation over time. First, China’s legislation is often vague and uncertain in nature. For example, the key term “state secret” was ill-defined in the 2000 regulation cited above (Tai, 2006). Some scholars (Cheung, 2006; Endeshaw, 2004; Keith & Lin, 2006; Weber, 2002) pointed out that the Chinese government did this on purpose to ensure ample room for its interpretation and manipulation. In addition, the uncertain and unspecified broadness holds Internet business owners and users in constant fear and therefore strengthens their self-censorship (Cheung, 2006). Second, many regulatory measures are often post hoc reactions to unpredictable conditions (Endeshaw, 2004; Qiu, 2003). As a result, many key regulations have been revised and refined over the years to “bring social and economic life in line with a priori principles and expectations” (Endeshaw, 2004, p. 46). Third, many laws and regulations overlap and create redundancy and confusion sometimes (e.g., due to different expectations and requirements between the Communist Party and the central administration), and such confusion is reflected in the lack of coherent and consistent decision-making processes and inconsistent enforcement (Endeshaw, 2004; Sohmen, 2001; Qiu, 1999/2000).

Internet Development and Democracy, E-Government, and Civic Engagement

Internet & democracy. Given China’s Internet censorship and authoritarian polity, a question, often asked, is the relationship between Internet development and democratization in China. There is a strong belief that Internet development, free flow of information, and formation of civil cyber groups pose potential threat to authoritarian regimes and China is no exception (Kluver, 2005; Tai, 2006; Taubman, 1998; Yang, 2003). However, Internet use and development in China has so far failed such an expectation (Kalathil & Boas, 2001) and some even argue that the Internet has become a new tool for governmental control (Tsui, 2003).

One possible answer could be found in the profile of Chinese Internet users. Besides demographic changes over the years (e.g., greater Internet penetration rate, lesser gender and geographic disparity), one consistent finding is the majority Chinese Internet users’ apathy for political communications (Hong & Huang, 2005). Instead, the majority of Chinese citizens use the Internet for gaming, entertainment, sports news, celebrities, and study and career opportunities (Kluver, 2005). Furthermore, China’s culture may have a role to play as well (Weber, 2002). Zhang, Chen, & Wen’s comparative study (2002), for example, found that compared to Americans, Chinese Internet users are more supportive of a greater extent of government involvement in Internet regulation, consistent with Chinese citizens’ general attitude toward a greater role of the government in governing the society. It is not clear, however, why the
majority of Chinese Internet users show little interest in political issues. More empirical studies need to address how Chinese Internet users feel about Internet use and development, despite the heavy top-down approach adopted by the Chinese government.

**E-government project.** The Government Online Project (*zhengfu shangwang gongcheng*) was kicked off in 1999. As part of this project, all government departments are required to build their own Web sites and provide online management and service functions (Lu et al., 2002; Wang, 2002). Registered government domain names (gov.cn) increased from 323 in 1997 to 13,963 by July 2004 (3.7% of the total registered domain names), and the number of Chinese government Web sites also amounted to 12,332 by 2004 (2.0% of the total Web sites) (Lagerkvist, 2005; Zheng, 2008, p. 38).

Through its E-government project, the Chinese government aims at reaching a number of goals such as increasing government transparency and organizational efficiency, strengthening propaganda (e.g., the opening of Tibet human rights Web site recently, www.tibet328.cn), reestablishing legitimacy of the Communist Party, containing or eradicating more pressing political problems (e.g., corruption), and gaining better control over lower-level and/or local cadres (Kalathil & Boas, 2001; Kluver, 2005; Lagerkvist, 2005). In this process, governments at all levels are encouraged to take advantage of the new computer information technology, and the central government is eager to show its lead. On June 20, 2008, for example, President Hu Jintao hosted his very first online communication with Web surfers, and Premier Wen Jiabao followed suit on February 28, 2009. Such Internet communication between users and top national leaders was hailed as a significant step toward “Internet politics” in which Internet users’ political rights of information, participation, and supervision were honored.

These e-projects also have an impact on the legal system. Take judicial reforms for example. In 2009 the Supreme People’s Court (SPC) published its *Outline of the 3rd Five-Year Reform of the People’s Courts* (2009-2013). To improve adjudication and execution of judicial verdicts, the SPC proposes displaying judicial judgments online whenever feasible. Several courts such as courts in Beijing, Henan, and Hebei have already started such a practice as early as in 2003. By April 10, 2009, more than 160 basic courts and 50 intermediate level (appellate) courts have reportedly adopted such a practice, and a total of 59,744 judicial judgments have been posted online at various courts’ Web sites (News reported on April 10, 2009 at http://www.chinacourt.org/html/article/200904/10/352466.shtml, last retrieved on April 29, 2009; the *Legal Daily*, December 17, 2008; the *People’s Daily*, March 17, 2009). Most recently on April 14, 2009, the official Web site of China’s courts (www.chinacourt.org) also announced establishment of free email boxes at all courts to facilitate communication between the courts and the public (News posted on April 14, 2009 at http://www.chinacourt.org/html/article/200904/14/352922.shtml, last retrieved on April 29, 2009). Such a practice echoed similar moves by many administrative organizations and leaders, which seemingly gained much support (Hartford, 2005). To go one step further, some courts even started televising live trials online.
Civil engagement. It is not accurate that all Chinese Internet users shun away from political issues in China. Rather, their participation shows in a unique form (often event driven) at critical moments (sometimes unexpected). Given the growing mass of Internet users, their online response, reaction, and participation have already created an unexpected amplification of public engagement in some key events (Dowell, 2006; Zheng, 2008). Take the 2009 “hiding from the cat” event for example. In January, 2009, Li Qiaoming was arrested for cutting down and stealing trees and put into jail in Jinning county, Yunan province. On February 8th, Li was mysteriously injured and died in a local hospital on the 12th. After a perfunctory investigation, local police and procuratorate announced that Li got injured when he was playing a game called “hiding from the cat” (duo maomao) with his jail mates. What was unexpected after the official announcement this time was the strong criticism and questioning by Internet users, and suddenly “hiding from the cat” became a new online bomb. Under the pressure to discover and disclose the “truth”, the Chinese Communist Party Propaganda Department in Yunan (CCPPDY) recruited five Internet users to form a special investigation committee (and two Internet users even chaired the committee). On the 20th, the committee went to Jinning county and conducted its investigation. Due to lack of access to key evidence (e.g., the coroner report, surveillance tape of the jail, and interviewing jail mates), the committee could not reach a conclusion and simply posted its investigation process online on the 21st. On the 27th, the Public Security and Procuratorate officials of the Yunan province announced the result of its official investigation. According to the report, Li was bullied numerous times by his jail mates in jail and suffered injuries. On the 8th, his jail mates blindfolded Li and beat him up. Li’s head was hit and bumped into the wall, which eventually caused his death. Li’s jail mates made up the story of playing a game to cover the truth. The report also disclosed various violations of prison management rules and regulations by both prison guards and bully inmates and called for further action. As a result, one director of the procuratorate in Jinning county was deposed, and three jailmates were charged with assaults and sentenced in August along with two prison guards who were found negligent (information summarized from various Internet sources).

The “hiding from the cat” event finally came to a conclusion but the term becomes a new symbol among Chinese Internet users. It is true that public engagement in major events such as the “hiding from the cat” is nonsystematic, spontaneous, and unpredictable. These events, however, do carry a great potential to shake political-legal reforms in China to some extent.

Cyber Crimes: Control and Evolution

In comparison to Internet censorship and regulation, studies on China’s cyber crimes (wangluo fanzui) are scarce. Similar to Western nations, cyber crimes are broadly defined in China to cover crimes that are committed with the involvement of computer information technology; cyber crimes are further classified into two large categories: one on crimes directly targeting computer systems and information networks, and the
other on crimes committed through the use of computers and their related networks (Chen, 2004; Keith & Lin, 2006, p. 119).

Based on statistics from the MPS, Yu (2007) reported that the total number of investigated cyber crimes in China was a little more than 400 in 1999; it jumped to 2,700 in 2000, 4,500 in 2001, and reached 6,633 in 2006. These numbers are no doubt only the tip of the iceberg, as the Chinese official admitted that the authority could have only managed to investigate 20% of estimate cyber crimes (News reported by the Xinhua.net.com in Tianjin on November 17, 2005, available at http://www.tj.xinhua.org/misc/2005-11/17/content_5613021.htm, last retrieved on April 30, 2009). A report from singtaonet.com in 2007 even listed China as the second largest cyber crime nation in the world, only behind the United States (News reported at http://www.singtaonet.com/society_focus/200708/t20070810_595551.html, last retrieved on April 30, 2009).

Laws and regulations. Cyber crimes are not regulated by one single special law in China. Rather, they are covered by a scope of laws and regulations with a comprehensive nature as discussed above (Zhou, 2009). The first effort, the Ordinance for Security Protection of Computer Information System issued by the State Council in February 1994, gave the MPS the overall responsibility to supervise, inspect, and guide the security protection of computer information systems and “to investigate criminal activities” that undermine computer networks, though the ordinance failed to specify the forbidden content (Tai, 2006).

The revised Criminal Law in 1997 (CL97) tried to formalize legislation on such crimes in articles 285-287. Article 285 covered unauthorized criminal access to computer-housed information concerning state affairs, national defense establishment facilities, and sophisticated science and technology; article 286 stipulated crimes of deleting from, altering, adding to, and interfering with computer information system, causing abnormal operations and grave consequences, and addressed the creation and spread of viruses; article 287 covered crimes concerning the use of a computer to carry out financial fraud, stealing, embezzlement, the appropriation of public funds, the stealing of state secrets, and other like criminal activities (Keith & Lin, 2006, p. 123).

To keep up with the new development of Internet use, the Standing Committee of the National People’s Congress further issued a Decision Regarding the Maintenance of Internet Security in 2000. The 2000 Decision places cyber crimes within six categories: (a) crimes disrupting the safe operation of computer networks; (b) crimes of using the internet to fabricate and disseminate information harmful to national security and social stability; (c) crimes of using the internet to disrupt the socialist market economic order and the management of social order; (d) crimes of using the internet to violate personal, property, and other legal rights of individuals, legal entities, and other organizations; (e) illegal acts, using the internet, that are not serious enough to warrant CL97 punishment, but could not be alternatively punished under the 1986 Provisions on Administrative Punishment concerning the Management of Public Security; and (f) civil infringement and liability committed while using the internet that are not serious enough to be punished according to either the CL97 or the 1986
Provisions (Keith & Lin, 2006, p. 128). Besides these two major laws (CL97 and 2000 Decision), many administrative rules and regulations are also adopted to cover various instances of cyber crimes.

**Pornography and online gambling.** Due to this comprehensive nature of China’s regulation, an array of crimes are targeted by the Chinese authority such as online fraud, selling illegal goods, libel, invasion of personal privacy, manufacturing and disseminating computer virus, online gambling, and pornography (Chen, 2004). Though online fraud constitutes the largest group of cyber crimes, the Chinese official has paid more attention to online pornography and gambling, because these types of moral crimes are often viewed as serious challenges to socialist social order.

In 1996, the Chinese authority took its first action against pornography on the Internet by adopting the *Interim Regulations on the Management of International Networking of Computer Information*. Article 13 of the regulation stipulated that “Organizations and individuals who get involved in Internet business shall abide by national laws, administrative regulations . . . shall not browse, copy and disseminate harmful information to public security, and pornographic materials and information.” Online pornography was once again prohibited under Article 5 of the *Computer Information Network and Internet Security, Protection and Management Regulations* (December 1997). Section (6) of the Article 5 prohibits any organization or individual from manufacturing, copying, browsing, and disseminating information that “propagates feudal superstitions; disseminates obscenity, pornography or gambling; incites violence, murder, or terror; instigates others to commit offences.” As usual, such regulations on pornography could also be found among many other regulations (Gomez, 2004).

One frequent target of the antipornography campaigns is Internet cafés (wangba). Since their first debut in 1996, Internet cafés have gained tremendous growth. The proportion of Internet café users as China’s total internet population soared from 3% in 1999 to 21% in 2001; the total number of registered cafés reached 64,000 in 2002 and the number of users rose to 16 million in 2004, though the percentage remained relatively stable between 15%-20% from 2002 to 2004 (Hong & Huang, 2005, p. 379; Qiu & Zhou, 2005, pp. 266-267). Besides registered Internet cafés, unregistered ones in China are virtually uncountable. Though they are heavy targets in crackdowns, unregistered cafés (heiba, literally “black bar”) remain popular and sometimes outnumber the registered one in some cities, and a total of 110,000 were estimated by the end of 2003 (Hong & Huang, 2005). Many features of Internet cafés make them popular among Chinese young Internet users, such as the private-business nature, relaxed regulation, low cost, convenience, and updated equipments and services. Gaming and group chat are very popular among Internet café goers and some even search for censored information and express their political opinions with the assumption that it is easier to hide their identities there (Hong & Huang, 2005). Nevertheless, online pornography and violent games are the primary concerns for parents and the government. China’s definition on pornography and violence are much broader and the government tries to stop both in the real and the virtual worlds.
Despite existence of various regulations (e.g., user registration, record keeping, prohibition of smoking, filtering of gambling, and pornographic content, no entry for those under 18, no Internet café in the vicinity of 200 meters of elementary and middle schools), enforcement by café owners is very relaxed in practice (Qiu, 2003). The government therefore has resorted to frequent crackdowns to clean up Internet cafés since 2001. In 2002, for example, followed a deadly fire at an Internet café in Beijing that killed 24, the government closed 3,300 cafés indefinitely and 12,000 others until they improved their safety measures (Endeshaw, 2004); in 2003, another 27,000 unregistered cafés were shut down (Hong & Huang, 2005). Since 2003, the government has also tried to push forward a chain-store model and hoped to tighten its control through chain-store standard management (Hong & Huang, 2005; Qiu & Zhou, 2005). The effect of such standardization, however, remains to be seen and it is unlikely that the chain stores will take up the whole market, especially given the existence of many unregistered cafés. In February 2007, 14 ministries and commissions further issued the Circular Concerning Further Strengthening the Management of Internet Cafés and Online Games, which regulates for the first time the virtual currency transaction in online games.

In addition to physical control over Internet cafés, the Chinese government keeps constant surveillance online via its infrastructural and technological equipments and skills (e.g., blocking and filtering pornographic Web sites; Zittrain & Edelman, 2003), and there are signs that the authority has stepped up such surveillance in recent years. For example, the MPS in 2007 announced 10 major cyber crime cases that the authority cracked in 2006 and 2007. Seven of the 10 were online obscenity, pornography, and prostitution-related cases (News posted by Xinhua.net on April 13, 2007 at http://news.qq.com/a/20070413/001256.htm, last retrieved on April 30, 2009). The CNNIC also stepped up its role and has been exposing and cleaning up Web sites where pornographic, vulgar, and degrading contents were found. Twenty such Web sites were exposed in the CNNIC’s ninth and tenth public postings this year, and even foreign investors such as Google were targeted (see the People’s Daily, February 24, 2009; http://news.sina.com.cn/c/2009-04-10/135817584966.shtml, last retrieved on April 30, 2009; the Straits Times, January 6, 2009).

Compared to pornography, online gambling is seemingly less prevalent in China (especially given the increasing popularity of traditional gambling), but the scale and impact of such crimes is still staggering. Citing data from the China Center for Lottery Studies at Beijing University, Wang (2009) reported that more than 300 billion Yuan (RMB) were transferred out of China and were invested in online gambling abroad in 2008 alone, and so did more than 600 billion Yuan in 2006. Systematic data and research on online gambling are extremely lacking and the public only gains a glimpse of the scale of such crimes through occasional news reports. On February 15, 2009, for instance, the largest-ever Shanghai online gambling case was tried in Shanghai and more than 20 defendants were sentenced to various terms of imprisonment. These offenders reportedly managed to build a rather sophisticated online gambling scheme and amassed more than 6.6 billion Yuan in 2006 and 2007 (Wang, 2009).
above, much of online gambling action and funds was shoved abroad to avoid tight control and severe punishment domestically, making governmental investigation more difficult.

**New crimes and regulations.** In addition to traditional cyber crimes, China also struggles with many new issues of Internet use. Take the “human flesh search” (*renrou sousuo* in Chinese), for example, in the last few years. Though targeted online people search started as early as 2001, the term did not draw enough attention until 2006. In 2006, a video clip was posted online in which a woman stomped a cat to death with her high-heeled shoes. Once the clip was posted, angered Internet users initiated the first mass search of the perpetrator. Soon she was found to be a nurse in Heilongjiang province. Under the pressure, her hospital fired her and she had to make an open apology for her misbehavior (information gathered and summarized from various internet sources).

As the “kitten killer” fell as the first “victim”, “human flesh search” has quickly become a powerful new tool by Web surfers to expose and hunt for immoral and unethical individuals who are labeled “human flesh”. Although such a practice gained more popularity and strength, concerns on potential abuse and invasion of people’s privacy started looming. In December 2007, a white-collar worker, Jiang Yang, committed suicide by jumping off the 24th floor balcony of her apartment in Beijing. In her blog (written before her death), she blamed her suffering to her unfaithful husband Wang Fei and posted a picture of Wang and his new lover. After her death, angry Internet users, led by a college classmate of Jiang, turned to “human flesh search”, posted all detailed information of Wang and his family online in a short time, and even sent Wang death threat emails and painted curses at his place. Wang lost his job as a result and suffered tremendous distress. In March 2008, Wang sued three Web sites where his information was posted for cyber violence and privacy violation. In February 2009, the people’s court in the Chaoyang district in Beijing ruled in Wang’s favor and awarded him 8,000 Yuan. This trial is quickly labeled as the first case of “human flesh search” and the first case of cyber violence, though public debates continue to support or question the use of “human flesh search” (information from various internet sources; Magnier, 2008; Wu, 2009). More recently in October 2008, Lin Ming, from Anhui province, tracked down his ex-girlfriend Zhou Chunmei, whom he got to know online, via “human flesh search,” and stabbed her to death in Xinxiang, Henan province. In April, 2009, Lin was convicted of murder and sentenced to death by the Xinxiang Intermediate People’s Court (information from various internet sources).

Facing rampant use of the “human flesh search,” many people including scholars called for new regulation. While the central government is moving slow, local governments took the first action. In January 2009, Xuzhou city in Jiangsu province adopted a new ordinance, the *Computer Information System Security Protection Ordinance in Xuzhou City*. The new regulation specifically prohibits misuse of the “human flesh search” and stipulates that violators could be subjected to a fine up to 5,000 Yuan and banned from accessing Internet services. Internet users who favor the “human flesh search” quickly question Xuzhou’s new regulation and believe that it will carry a
negative effect on Internet use and development in China (reports at http://tech.163.com/09/0119/04/500BCRE0000915BF.html, last retrieved on May 1, 2009; the Guangzhou Daily, January 20, 2009; Ye, 2009). Amid continuing debate, “human flesh search” represents an example of Internet evolution in China and the government will definitely face more such challenges in future.

Conclusion

Since China’s first global Internet connection in 1994, a mere 15 years has passed. However, China’s Internet development in such a short time has been eye-catching and China has already had the largest Internet users of the world by 2008. The impact of Internet use and development has been enormous and it is evident in almost every aspect of people’s lives in China. Such dramatic changes have left ample room for scholars’ research, potentially covering a broad scope of issues and subjects.

Nevertheless, social studies on Internet use and development have been primarily concentrated on the implications of the Internet for China’s democratization, and the main concern is therefore state censorship, control, and regulation (Tsui, 2005). As we reviewed in this article, the Chinese government has, from the very beginning, adopted a “top-down, hands-on” approach in its plans and investments of telecommunications industry and tried to facilitate the national economic growth and maintain its political control at the same time. Tight control and regulation are implemented through a multidimensional approach involving multiple agencies and players and cover both Internet infrastructure and commercial and social use. All these requirements and measures eventually are backed up by various laws and regulations, aiming at a comprehensive control of Internet use and development.

Though there is strong hope internationally for China’s democracy potentially led by Internet development, free flow of information, and formation of civil groups, an increasing number of scholars are realizing that the Internet is a double-edged sword. As a technology tool, the Internet cannot be isolated from social context in which its use and development is inevitably intertwined with habits, beliefs, and values in a specific culture (Tsui, 2005). The borderless nature of Internet information is also subject to control of local laws and regulations within boundaries (Goldsmith & Wu, 2006). China’s testing case seems to prove just that. This is not, however, to deny the great impact that the Internet has brought to the Chinese society. We have seen ample evidence, especially in recent years, that the Internet empowers both the government and the general public to move forward political-legal reforms. Indeed, the Internet provides another tool for the public to better participate in such processes. To what extent that this type of government–public e-interaction will lead to democratization, however, still remains to be seen.

Although Internet use and development prompted economic development in China, it also led to rising cyber crimes, a topic largely understudied. Similar to its approach toward Internet regulation in general, the Chinese government combined its criminal laws with many other administrative rules and regulations to cover cyber crimes comprehensively (online pornography and gambling are such examples). Besides
conventional cyber crimes, the Chinese government struggles with new phenomena such as the “human flesh search” and ponders the costs and benefits of new legislation and regulation. It is clear that China will face more challenges, both legally and politically, in its further transition in the new century, and the role of the Internet is still to be unfolded.

**Declaration of Conflicting Interests**

The authors declared that they had no conflicts of interests with respect to their authorship or the publication of this article.

**Funding**

The authors declared that they received no financial support for their research and/or authorship of this article.

**Reference**


Human Rights Watch. (2006, August). Race to the bottom: Corporate complicity in Chinese Internet censorship.* 18(8[c]).


**Bios**

**Bin Liang** is an associate professor in the Department of Sociology at Oklahoma State University–Tulsa. He has published numerous articles on crime and the legal system in China. He is also the author of two books, titled *The Changing Chinese Legal System, 1978—Present: Centralization of Power and Rationalization of the Legal System* with Routledge (2008) and *China’s Drug Practices and Policies: Regulating Controlled Substances in a Global Context*.
with Ashgate (2009). His current research interests include globalization and its impact on the Chinese legal system, crime and deviance in China, and the drug court in Tulsa County, Oklahoma.

Hong Lu is associate professor in the Department of Criminal Justice at University of Nevada, Las Vegas. She has published extensively in the fields of sociology of law and comparative criminology.