China’s Data Privacy Regulations: A Tricky Trade-Off between ICT’s Productive Utilization and Cyber-Control

By: Nir Kshetri

Kshetri, Nir (2014). “China’s Data Privacy Regulations: A Tricky Trade-Off between ICT’s Productive Utilization and Cyber-Control”, *IEEE Security & Privacy*, 12(4), 38-45.

Made available courtesy of IEEE Computer Society:
http://dx.doi.org/10.1109/MSP.2013.105

Abstract:

China's data privacy laws and regulations reflect the tension it faces between using modern information and communications technologies (ICTs) to maintain unity and stability via cybercontrol and using them to stimulate economic growth and productivity. The evolution of China's data privacy regulations and policies and their impact on provisioning and use of cloud computing and other IT services are substantial. They deserve close examination by IT service providers and users as well as IT professionals in China and other countries.

Keywords: privacy | data privacy regulations | China | cyber-control | cloud computing | microblogging

Article:

China’s data privacy laws and regulations reflect the tension it faces between using modern information and communications technologies (ICTs) to maintain unity and stability via cybercontrol and using them to stimulate economic growth and productivity. The evolution of China’s data privacy regulations and policies and their impact on provisioning and use of cloud computing and other IT service are substantial. They deserve close examination by IT service providers and users as well as IT professionals in China and other countries.

In this article, I analyze the key features of China’s data privacy regulations, especially priorities placed on cybercontrol versus consumer data protection, the key drivers behind these regulations, their impact on various IT service providers and users, and the similarities to and differences from the EU and the US. These aspects distinguish this work from prior studies, which mainly provide journalistic and legal perspectives.[1–3]

Background

A 2012 *China Daily* piece titled "Personal Data Protection" provided a succinct and valuable update on China's data privacy breaches' increasing prevalence and consequences.[4] According to the editorial, illegal firms in the country specialize in collecting and selling personal information, acquiring information from subsidiaries of major telecommunication firms, and sending text messages for profit. Some bank and telecommunications company employees have been arrested for selling personal information to such firms. A China Internet Network Information Center report indicated that, in the first half of 2011, 121 million Chinese had their online account information stolen.[5]

The abuse of personal information is widespread. A sizable and rapidly growing black market of personal information has reportedly emerged. A malicious actor can sell a database containing a specific type of information, for instance, phone numbers, for more than US$1,500 on the black market. The illegal companies, in turn, charge their clients between $1,500 and $150,000 for services such as private investigation, illegal debt collection, asset investigation, and even kidnapping.[6] The *China Daily* editorial warned that "the booming trade in personal information and its illegal use will finally ruin online economic activities and disturb even the order of off-line business activities."[4]

The lack of a comprehensive data protection law in China has been a concern to those interested in China's online market development.[7] Chinese policymakers have responded to this issue but have given a high priority to cybercontrol measures—that is, administrative, legislative, and technical measures as well as procedures and resources to monitor, control, and regulate users' access to and activities in cyberspace. According to Reporters without Borders, "China was one of the first countries to realize it couldn't do without the Internet, and so it had to be brought under control."[8] Unsurprisingly, the Chinese government assigned concerns related personal information abuse a relatively low priority level. The upshot is that many foreign IT service providers have chosen not to operate in China. This, along with China's strict filtering system, has resulted in low-quality or unavailability of services from China's global IT service providers.

Cybercontrol as a Key Element

Table 1 lists key legislations governing data privacy and security in China. As the second column shows, the stringent ISP recordkeeping requirements and the requirement to provide technical support to government authorities and prosecutorial authorities' power to access private information under various regulations reflect a strong emphasis on cybercontrol measures. The National People's Congress (NPC) succinctly stated the rationale of the 2012 "Decision of the Standing Committee of the National People's Congress to Strengthen the Protection of Internet Data" (2012 Decision): "to protect network information security, protect the lawful interests of citizens, legal persons and other organizations, [and] safeguard national security and social order."[9]

From a cybercontrol point of view, the last point— safeguarding national security and social order—needs elaboration. Various cybercontrol measures' stated goals have been to control

information that's harmful to state security or social stability. Regarding the various cybercontrol measures, government-sponsored Xinhua News Agency noted that the 2012 Decision "will help, rather than harm, the country's netizens."[10]

Table 1. Key legislation governing data privacy and security in China.

Legislation	Explanation/main provisions
Chinese Constitution (1982)	Per article 40, organizations and individuals can't infringe on the right of citizens' privacy.[15]
The Measures for Security Protection Administration of International Networking of Computer Information Networks (1997)[24]	Per article 4, international networking can't be used to endanger state security, divulge state secrets, infringe on national, social, and collective interests and the legitimate rights and interests of citizens and engage in criminal activities.
The Telecommunication Regulations (2000)[25]	This piece of legislation provides the legal basis for telecommunications-related data protection, which supports users' freedom to use telecommunications and the privacy of communications.
The Regulation on Internet Information Service, promulgated by the State Council on 25 Sept. 2000[26]	Article 14 requires ISPs to keep records of each user including time spent online, account, IP address or domain name, phone number, and so forth, for 60 days and provide that information to the government authorities when required.
Measures for the Administration of Internet Email Services (2006)[27]	Article 3 guarantees citizens' privacy in using Internet and email services. However, public security and prosecutorial authorities can access private information for protecting state security or investigating crimes.
The Employment Services and Management Regulations, issued by the Labor and Social Security Ministry, now known as the Human Resources and Social Security Ministry, effective 1 January 2008[28]	An employer is required to keep certain data relating to employees confidential. The regulation also limits the usage of such data by the employer.
Criminal Law amended in 200915 (www.whitecase.com)	The Criminal Law's many amendments include definition of acts related to data collection and privacy that can be considered as criminal offenses.
Tort Liability Law, effective 1 July 2010[15]	Establishes data protection violations as a tort claim that recognizes that a party whose right to privacy is infringed can claim for the losses, profits arising from the breach, and damages associated with emotional distress.
Certain Regulations on Standardizing the Order of the Internet Information Service Market, issued 15 March 2012[1]	The regulations contain the first legal definition of personal information.
The Decision of the Standing Committee of the National People's Congress to Strengthen the Protection of Internet Data, 28 December 2012[9]	Article 7 prohibits sending commercial advertisements to telephones and email accounts without user consent.
	Per article 8, citizens may request ISPs to delete information that leaks individual identity, invades personal privacy, or infringes on other rights and interests.
	Per article 9, the victims of criminal acts related to personal data can file an accusation with government authorities or a lawsuit in a court.
	Article 10 requires ISPs to cooperate with the government and provide technical support upon inquiry from the authorized government authorities.
Information Technology Security—Guideline for Personal Information Protection Within Information Systems for Public and Commercial Services, issued 1 February 2013[6]	The guideline provides further details and establishes eight basic principles regarding the protection and handling of personal information.

A distinguishing feature of China's data privacy regulations and enforcement mechanisms is the sophisticated programs and systems that closely monitor cyberactivities of activists whose viewpoints challenge the Chinese Communist Party or its mainstream policies. China reportedly has the world's largest cyber–police force, with tens of thousands of government agents monitoring and controlling cyberspace activities.[11] Some reportedly pretend to be dissidents and participate in chat rooms, speaking out against the government. Thus, many Internet users are afraid to engage in online conversations on sensitive topics such as democracy, Japan, and religion.

The relatively selective enforcement of existing regulations and intensification of cybercontrol measures have led to the arrest of several democracy organizers, human rights activists, members of the spiritual organization Falun Gong, scholars, and other dissidents for alleged involvement in cybercrimes. On the other hand, the Chinese government has devoted relatively few resources to enforce data privacy measures.

Other Entities

Note that because of the government's various control measures, nongovernment entities, special interest groups, and the civil society are organized loosely. There's little room for these groups to influence national policymaking. Some nascent special interest groups, such as environmental and animal rights organizations and sports clubs, have placed new demands on the state and created competition for resources, attention, status, and legitimacy. Although such groups provide tremendous societal benefits, their potential for mobilizing people on a regional or even national scale has increased the government's nervousness. Although China's industrial leaders and state science and technology officials have repeatedly appealed to the government to take measures to increase the participation of trade, industry, and professional associations, the regime has responded with resistance to accept an increased role in the independent civil society.

The situation contrasts with India's. Trade associations, such as the National Association of Software and Services Companies (NASSCOM), have strengthened India's data privacy and security standards. For example, the Data Security Council of India—a self-regulatory member organization set up by NASSCOM—imposes a fine of up to $1 million for member companies that fail to secure data.

The Internet Society of China (ISC) can be considered an entity analogous to NASSCOM. However, it's been described as a quasi-governmental organization and hence mostly acts under the government's guidance.[12] Under China's current institutional structures, trade associations and special interest groups are less prevalent than in India or the West, and those that exist aren't in a position to function like they do in the West or in India.

Indeed, the best way for trade associations such as the ISC to promote their interests has been to contribute to the government's cybercontrol goals. Unsurprisingly, the ISC has developed and implemented sophisticated cybercontrol strategies rather than help protect Internet users' security and privacy. In 2001, the ISC asked Internet companies to sign a voluntary pledge that required them to not disseminate information that could threaten state security or social stability. In 2009, the ISC awarded China's largest search engine company, Baidu, and 19 other companies the

China Internet Self- Discipline Award for fostering and supporting "harmonious and healthy Internet development."[8]

A strong state and a weak civil society means that there's little pressure to improve security and performance and develop appropriate industry standards in major industries, such as cloud computing and healthcare. Western initiatives illustrate this point. The American Institute of Certified Public Accountants (AICPA) is trying to accelerate cloud adoption among its members. It endorsed Paychex for payroll solutions, bill.com for invoice management and payment, Intacct for financial management and accounting, and Copanion for tax automation. AICPA's endorsements are based on an extensive due diligence on the vendors' security practices. Cloud vendors have also started pressuring policymakers for sensible regulations. IT companies such as Oracle, Cisco, SAP, Apple, Google, and Microsoft lobbied to streamline the EU's fragmented national data protection laws. Because of China's unique institutional arrangements, such initiatives and pressures are conspicuously absent in the country.

China's Regulations and Their Key Drivers

One complaint about China's data privacy regulation is its piecemeal approach that doesn't adequately provide systematic and comprehensive personal data protection.[13] As I indicated earlier, data privacy issues in China have been governed by many regulations, legislation, and guidelines as well as industry-specific regulations. At a press conference, the NPC Standing Committee's spokesperson stated that the State Council had previously issued nine regulations in this area. In addition, various ministries and departments have issued more than 10 administrative rules regulating the Internet. The critics also complained that the data privacy provisions are often ambiguous and vague, making interpretation and enforcement difficult. In this regard, an NPC Standing Committee's spokesperson stated that the regulations would be reviewed and amended in accordance with the 2012 Decision.

A key driver of data privacy regulations is the public's increased awareness of their right to privacy. The new regulations have thus emphasized the protection of personal data. The Employment Services and Management Regulations require employers to keep certain employee data confidential. Similarly, "Certain Regulations on Standardizing the Order of the Internet Information Service Market" (2012 Regulations) provided a legal definition of personal information (see Table 1).[1] Likewise, the 2012 Online Data Protection Regulation bans the sale and distribution of personal information without the owner's consent.[14] It also requires ISPs to ensure the security of personal data and prevent misuse as well as provides consumers the right to seek deletion of personal data posted without consent and to sue for violations.

China has also started enforcing data privacy laws. In 2010, in the first criminal sentence for illegal acquisition of personal information under the amended Criminal Law,[15] a Zhuhai court gave the alleged criminals monetary fines and jail sentences. The case involved illegal acquisition and sale of information related to 14 high-ranking government officials' telephone calls, which was used in extortion schemes.

The adoption of international data privacy standards would likely facilitate and promote domestic economic development as well as international trades and investments. As in other

economies, the cloud's evolution appears to be among the influential forces to shape China's data privacy regulations. The cloud's transformative nature has fundamentally changed the tradeoff between economically productive utilization of the technology and the government's preference for cybercontrol.

In 2011, the Chinese government announced an investment of $154 million to develop a cloud center for high-tech and start-up firms in Chongqing, which would be free of censorship. In general, China has implemented major policy improvements in areas such as cybercontrol, international economic relations, and data privacy to create a cloud-based economy. At the same time, policies that lack specificity regarding the agencies enforcing the laws and penalties, the government's engagement in cybercontrol, and the restriction of foreign firms' participation have hindered this sector's growth.

Although China has initiated new regulatory efforts to address emerging data privacy problems, a closer look reveals Chinese policymakers' preference for vagueness and ambiguity. Despite some enforcement activities, there's an enormous gap between laws on the books and the government's capability and willingness to enforce these laws.

An observation made by W.H. Myers more than 15 years ago is still true today: "the law [in China] is marginalized and the legal system relegated to a lowly position in a spectrum of meditative mechanisms, while at the same time available for manipulation by powerful sectors within the state and the society at large."[16] An international comparison would be informative and might help clarify China's ambiguous data privacy regulations and weak enforcement. In the 2012 Data Centre Risk Index issued by International consultancies Cushman & Wakefield and HurleyPalmerFlatt, China ranked near the bottom of the list: 26th out of 30 nations. The lack of an effective regulatory framework to address data theft and cybercrimes as well as tight government control over data contributed to China's low rank.

Effects on Foreign IT Services Providers

China's uncertain legal environment and vague regulations have presented a big dilemma for foreign IT service providers because compliance with the Chinese government's requirements might infuriate stakeholders in home countries. Yahoo and Google faced criticism in the US for complying with Chinese regulations and government demands. Yahoo and its Chinese subsidiary also faced lawsuits in the US for their actions in China. Likewise, Amnesty International accused US-based Internet companies such as Google, Microsoft, and Yahoo of violating the Universal Declaration of Human Rights in their agreement with Chinese government to censor Internet use in China. In August 2013, Yahoo closed its email service in China.[17]

Some cloud providers located their servers in neighboring economies, such as Singapore and Hong Kong, to serve the Chinese market. For instance, following its withdrawal from China, Google's search site for China was hosted on servers in Hong Kong, and Chinese users were redirected to the Hong Kong site google.com.hk. In light Edward Snowden's fleeing to Hong Kong due to its strong protections for free speech, it's worth noting that as a Special Administrative Region of the People's Republic of China, Hong Kong, has a high degree of autonomy, except in defense and foreign policy. In particular, Hong Kong's mini-constitution

guarantees its own political system, a high degree of autonomy, and Western-style civil liberties such as freedom of speech until 2047.

Although the Hong Kong government doesn't censor google.com.hk, the Chinese government filters search results for users accessing the site from mainland China. As in the cases of other US-based datacenter and cloud providers, Google has avoided mainland China for datacenter location due to the country's strict filtering policies. In 2011, Google purchased land in Changhua County in Taiwan, the Kowloon region of Hong Kong, and the Jurong West section of Singapore to develop datacenters. Likewise, Digital Realty Trust, Equinix, and Yahoo have built major datacenters in Singapore and other Asian locations to serve consumers from China and other Asian economies.

Chinese Internet Users and IT Services Providers

Putting foreign cloud providers' servers in neighboring countries—thus requiring foreign-originated traffic to pass through China's firewall—leads to long loading times for Chinese consumers. A study of content delivery network provider CDNetworks indicated that China's firewall leads to an increase in load time by 450 milliseconds or more for an object hosted on a server outside China. For a typical website hosted in Asian cities such as Hong Kong, Singapore, or Tokyo, the firewall adds 10 to 15 seconds. The average time to load an object from a Hong Kong datacenter is 50 percent longer than in China. Websites hosted in the US take 20 to 40 seconds to load.[18] Thus, accessing cloud services provided by foreign vendors, such as Google Docs and Dropbox, is difficult or impossible. Moreover, if a cloud provider's contents are on a server that also hosts content objectionable to the Chinese government, they might be blocked.[12]

Cybercontrol has been challenging for the Chinese government. Consequently, many enforcement mechanisms related to censorship are delegated to trade associations such as the ISC or individual service providers. Chinese consumers and service providers have exhibited a tendency toward noncompliance with government regulations.[19] For example, a 2011 regulation required microbloggers to register using their real names. Sina, a Nasdaq-listed Chinese online media company warned that the requirement would negatively affect user activity and threaten its popular microblogging service, Sina Weibo. Even after the 16 March 2012 deadline, Sina Weibo continued let users who hadn't registered their real names use its services.

Comparing China's and Other Major Economies' Regulations

Two major approaches have been used to characterize data privacy regulations: the EU model and the US model. The EU set a baseline common level of privacy to protect its citizens' rights, irrespective of data location. The US, on the other hand, prefers to rely more on voluntary self-regulation in an attempt to encourage firms' marketing and innovation. However, it has sector-specific strict regulations for sensitive data. To comply with the Sarbanes-Oxley Act (www.soxlaw.com), public companies must have IT controls designed to ensure that data is accurate and protected from unauthorized changes. Likewise, the Health and Human Services Health Insurance Portability and Accountability Act requires healthcare providers to have measures in place to protect patient data privacy, integrity, and availability. Those not complying with the act might face up to $1.5 million in fines and 10 years in prison.

Table 2. Comparison of China, EU and US data privacy regulations.

Dimension	China	EU	US
Salient feature	China encourages purely economic use of information and communications technologies and strict cybercontrol measures.	EU policies indicate strict enforcement of privacy rights through legislation.	The US shows a preference to rely mostly on voluntary self-regulation but with sector-specific regulations for sensitive data.
Key driving factors	China aims to balance economic modernization and maintenance of unity and stability through political control	Primarily due to World War II–era fascists' and post-War communists' use of secret files as the basis for nefarious activities, Europeans are more fearful of the prospect of personal information abuse	The US encourages marketing and innovations
Effects on IT providers	Chinese policies lack the specificity required for accurate understanding and compliance. The 2012 Online Data Protection Regulation is broad and vague and favors guiding principles over law. Many provisions, such as department or agency to supervise and enforce, are unclear. No specific details are provided about the nature and amount of penalties.14 Lack of enforcement means that there's little legal recourse for data theft by employees or equipment loss during police inspections.	Requirement for compliance with strict regulations and the lack of economies of scale due to market fragmentation have imposed inefficiencies and acted as a barrier to incentive for the development and diffusion of cloud and other technologies. The EU Directive, which is stricter than US regulations, is likely to have more wide-ranging impact on all business types. It would require more than 42,000 firms in banking, transport, energy, and healthcare sectors and Internet and public administrations to inform their respective national network and information security authorities if their networks are attacked.	There is a fear among some EU-based consumers and activists that US cloud service providers are required to disclose data stored in clouds to their government without the data owner's consent or knowledge. Although US officials and vendors have emphasized that such concerns are exaggerated and overstated, convincing EU-based customers and activists that the Patriot Act doesn't present a risk has been a challenge for US providers.
Effects on IT users	Unavailability of some services has been a concern. Some foreign firms have located their servers in neighboring countries, which has caused a severe negative impact on service quality.	Users enjoy a high level of privacy but due primarily to the lack of choice and quality of cloud services, consumers are slower to adopt the cloud. According to Gartner, from 2012 to 2016, North America (led by the US) is expected to account for 58 percent of public cloud spending ($779 billion), compared to Western Europe's 22 percent share.	There have been some concerns related to the government's monitoring and companies' misuse of citizens' information.

Along with Singapore and Thailand, China has broadly followed the US model, which lacks comprehensive, mandatory regulations.[20] This approach differs from those in other Asian economies such as India, Japan, Malaysia, South Korea, and Taiwan, which have followed the EU directive model and adopted some forms of comprehensive data privacy laws that apply to all types of personal data.

Table 2 compares data privacy regulations in China, the EU, and the US in terms of salient features, drivers, and effects on IT providers and users. China has stricter data privacy regulations for sensitive personal information compared to other economic sectors. In 2011, the

People's Bank of China issued a "Notice to Urge Banking Financial Institutions to Protect Personal Financial Information." Effective since 1 May 2011, the notice prohibits banks, including foreign invested commercial banks, to store or process personal financial information obtained in China outside the country. Likewise, according the Criminal Law, it's a crime for employees of government institutions and organizations in financial, telecommunications, transportation, education, and medical sectors to unlawfully provide personal information to third parties.[15]

Another important difference between China and the US is that China lacks the self-regulatory component in data privacy laws—a result of its strong state and weak civil society. China's regulations on data transfer to foreign countries also differ from the US's, which has no general prohibition against transferring data outside its borders. As I noted earlier, in the US, sensitive data, such as healthcare and financial information, is regulated, and companies dealing with such data are expected to protect personal information irrespective of location.

Some similarities can be found in Chinese and US data privacy and security approaches, including sensitive national security–related information, despite significant differences in the two economies' approaches regarding this issue. It's worth noting that some European policymakers and privacy activists have drawn attention to the fact that the US Patriot Act and the Foreign Intelligence Surveillance Amendment Act allow US surveillance and spying agencies to access to EU citizens' data stored in US companies' clouds.[21] Following the revelation of the June 2013 US PRISM surveillance program, Europe's top policymakers, including European Commission vice president Neelie Kroes[22] and Germany's Interior Minister Hans-Peter Friedrich[23] indicated the possibility of further deterioration of trust in US-based cloud providers. However, important differences need to be noted regarding the two countries' data privacy laws and regulations' clarity and enforcement. Whereas the US approach is based on relatively stronger rule of law, China's data privacy regulations are characterized by vagueness and ambiguity.

In recent decades, China has emphasized economic growth and prosperity; its goal in cyberspace is to control without jeopardizing economic development. In this regard, the government's cost/benefit calculus associated with cybercontrol measures might change over time. If the perceived risks of state insecurity or social instability increase, the government might adopt stricter enforcement measures.

Among other key forces, the cloud is shaping China's data privacy and security policies and practices. China's experience indicates that cloud-related policies must have a meaningful purpose, and introducing regulations that can't be enforced is counterproductive. However, as indicated by key foreign cloud players' withdrawal from the country and foreign cloud services' unavailability and poor performance, there's a difficult tradeoff in controlling the information in the cloud and encouraging economically productive use of the technology. At the same time, Western technology companies' government-centric activities in China have led to a consumer backlash and even legal sanctions in their home country. Thus, regulatory and policy issues on cybercontrol that arise in the context of the cloud might have strong bearing on foreign technology firms' ability to operate in China. The security risks are especially high for multinational firms handling sensitive information.

Despite recent awareness and understanding of privacy among key actors in China, the level of data privacy awareness is much less developed, and sector-specific regulations and enforcement mechanisms are lacking. For instance, although regulatory and security concerns are major barriers for the healthcare industry's adoption of public clouds in the US and other countries, such barriers are of less concern in China.

A lesson from experience in other areas, such as infringement of intellectual property rights, is that violations involving data privacy in China are likely to be more a problem of enforcement than absence of laws. The ignorance of law enforcement officials is also likely to hamper privacy regulation enforcement. The gap between the law on the books and the law in action will likely be substantial. Thus, companies doing business in China must carefully evaluate their Chinese partners' systems for handling customer data to avoid the privacy and data protection risks and compliance with existing privacy laws.

References

1. V. Lockyer, "New Developments in Data Privacy in China," Orrick, 12 Mar. 2013; www.orrick.com/Events-and-Publications/Pages/New-Developments-in-Data-Privacy-in-China.aspx.

2. A. Winston, A. Zhang, L. Xu, "Data Protection and Privacy in China," White & Case, Mar. 2012; www.whitecase.com/alerts-02142012-1/#.Ue0XmKyTJmc.

3. R. MacKinnon, "Inside China's Censorship Machine," *National Post*, 29 Jan. 2012; http://fullcomment.nationalpost.com/2012/01/29/rebecca-mackinnon-inside-chinas-censorship-machine.

4. "Personal Data Protection," *China Daily*, 6 Apr. 2012; www.chinadaily.com.cn/opinion/2012-04/06/content_14987674.htm.

5. Z. Xinxin, "China to Further Safeguard Cyber Security," 13 Jan. 2012; http://english.peopledaily.com.cn/90882/7704949.html.

6. Z. Yan, "Personal Data Crimes Set to Be Defined," 4 July 2012; www.chinadaily.com.cn/china/2012-07/04/content_15546503.htm.

7. G. Greenleaf and C. Hui-ling, "Data Privacy Enforcement in Taiwan, Macau, and China," *Privacy Laws & Business International Report*, no. 117, June 2012, pp. 11–13.

8. K.E. McLaughlin, "China's Model for a Censored Internet," *Christian Science Monitor*, vol. 97, no. 210, 2005, pp. 1–10.

9. E.G. Kitaev, "China Adopts Privacy Legislation Strengthening Online Personal Data Protection," 8 Jan. 2013; www.dataprivacymonitor.com/online-privacy/china-adopts-privacy-legislation-strengthening-online-personal-data-protection.

10. “Nothing to Fear from New Internet ID Policy,” China.org.cn, 28 Dec. 2012; www.china.org.cn/china/2012-12/28/content_27542923.htm.

11. A. Stevenson-Yang, “China’s Online Mobs: The New Red Guard?,” *Far Eastern Economic Rev.*, vol. 169, no. 8, 2006, pp. 53–57.

12. R. MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom*, Basic Books, 2012, p. 35.

13. “Update: Privacy and the Protection of Personal Information in China,” Hunton & Williams, 16 Feb. 2011; www.huntonprivacyblog.com/2011/02/articles/update-privacy-and-the-protection-of-personal-information-in-china.

14. “China Enacts Online Privacy Framework to Protect Data, but Not User Anonymity,” Bloomberg, 7 Jan. 2013; www.bna.com/china-enacts-online-n17179871719.

15. G. Zhu, “The Right to Privacy: An Emerging Right in Chinese Law,” *Statute Law Rev.*, vol. 18, no. 3, 1997, pp. 208–214.

16. W.H. Myers, “The Emerging Threat of Transnational Organized Crime from the East,” *Crime, Law and Social Change*, vol. 24, no. 3, 1996, pp. 181–222.

17. C. Shu, “Yahoo Shuts Down Its Email Service in China,” 18 Aug. 2013; http://techcrunch.com/2013/08/18/yahoo-shuts-down-its-email-service-in-china.

18. J. Kim, “How to Do Online Business with China,” *Tech-Week Europe*, 22 Feb. 2013; www.techweekeurope.co.uk/comment/how-to-do-online-business-with-china-108291.

19. N. Kshetri, “Cyber-victimization and Cybersecurity in China,” *Comm. ACM*, vol. 56, no. 4, 2013, pp. 35–37.

20. R. Berry and M. Reisman, “Policy Challenges of Cross-Border Cloud Computing,” *J. Int’l Commerce and Economics*, vol. 4, no. 2, 2012, pp. 1–38.

21. D.S. Rauf, “Patriot Act Clouds Picture for Tech,” *Politico*, 29 Nov. 2011. www.politico.com/news/stories/1111/69366.html.

22. M. Finnegan, “Prism Harming US Cloud Provider Business, European Commission Claims,” *ComputerWorld UK*, 5 July 2013; www.computerworlduk.com/news/it-business/3456331/prism-harming-us-cloud-provider-business-european-commission-claims.

23. T. Samson, “Germany Joins in Voicing Distrust of U.S.-Based Cloud Services,” *InfoWorld*, 3 July 2013; www.infoworld.com/t/data-security/germany-joins-in-voicing-distrust-of-us-based-cloud-services-222094.

24. “China: Measures for Security Protection Administration of the International Networking of Computer Information Networks,” Dec. 1997; www.wipo.int/wipolex/en/text.jsp?file_id=182465.

25. “Data Privacy in Telecom Area,” *Int’l Financial Law Rev*., 25 Sept. 2012; www.iflr.com/Article/3093906/Data-privacy-in-telecom-area.html.

26. “China: NPC Decision on Network Information Protection,” *The Library of Congress*, 4 Jan. 2013; www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403445_text.

27. “Measures for the Administration of Internet E-mail Services 2006,” Lehman, Lee & Xu, 30 Mar. 2006; www.lehmanlaw.com/resource-centre/laws-and-regulations/information-technology/measures-for-the-administration-of-internet-e-mail-services-2006.html.

28. D.A.W. Abate, “Privacy Issues under PRC Employment Law,” 19 Jan. 2012; www.mayerbrown.com/publications/Privacy-Issues-under-PRC-Employment-Law-01-19-2012.

Nir Kshetri is a professor in the Bryan School of Business and Economics, University of North Carolina at Greensboro. His research focuses on global cybersecurity issues. Kshetri received a PhD in business administration from the University of Rhode Island. He’s a member of the Pacific Telecommunications Council. Contact him at nbkshetr@uncg.edu.