Cyber surveillance regulations: Is the United States asking China to accept a double standard?

By Theodore H. Moran April 2015

KEY POINTS

- *China's proposed counterterrorism law, which applies to all information technology (IT) companies operating in China, and US "legal-intercept" regulations, which govern all IT companies operating in the United States, are officially acknowledged frameworks to counter terrorist and criminal behavior.*
- *Despite the similarities in these regulations, President Obama has criticized China's law.*
- *The US must prepare to see practices that it has already adopted become prevalent elsewhere or be ready to modify US surveillance behaviors that US authorities do not want to see spreading around the globe.*

Beijing is abuzz with cybersecurity proposals. Amidst rumored regulations giving preference to companies that use domestically produced technology, and with the removal of Cisco and Apple from the central government's authorized-procurement list, the Chinese government recently made public the draft of a new counterterrorism law that applies to all information technology (IT) companies operating in China.[1] The draft has been published on China's National People's Congress website, and the public is invited to submit comments. President Obama went out of his way to criticize the counterterrorism law, saying that "This is something they are going to have to change if they are to do business with the United States."[2]

Yet, Chinese counterterrorism regulations mirror US "legal intercept" regulations that govern all IT companies operating in the US. Is America calling for other nations—including China—to accept a double standard?

Chinese Counterterrorism Regulations Pertaining to the IT Industry

Articles 15 and 16 of China's counterterrorism law are of particular concern to American and other IT providers. Article 15 states:

> Telecoms business operators and Internet service providers shall during the design, construction, and operation of telecommunications and the Internet preinstall a technical interface, and

> submit for approval to the relevant authorities all cryptographic solutions. All related products or technologies that do not preinstall technical interfaces or obtain pre-approval of their cryptographic solutions will be barred from usage.
>
> All provision of telecommunications and Internet businesses within the People's Republic of China must place related equipment, and store all domestic related user data within the jurisdiction of the People's Republic of China. Upon refusal to store, services cannot be provided within the People's Republic of China.[3]

Commentary indicates that the phrase "preinstall a technical interface" means providing a portal for surveillance by Chinese state authorities. Thus, Article 15 requires all IT operators and Internet service providers to (1) design systems so that Chinese agencies can conduct surveillance, (2) turn over encryption keys, and (3) store all user data within Chinese jurisdiction. Article 16 repeats the surveillance and encryption requirements in the event of possible terrorism cases: "For the purposes of the prevention and investigation into terrorism related activities, public security and state security organs may use telecommunications and Internet technical interfaces, and may also require that service providers or users provide technical support for decryption."[4]

US Legal-Intercept Regulations Pertaining to the IT Industry

The US has mirror-image surveillance provisions (so-called "legal-intercept" regulations) that apply to all IT providers within the United States and are used to counter terrorism and criminal activity. The Communications Assistance for Law Enforcement Act (CALEA) requires all telecommunications carriers to ensure that equipment, facilities, and services enable law enforcement officials to conduct electronic surveillance pursuant to court order. Passed by Congress in 1994, today CALEA requires telecommunications carriers and communications equipment and software providers operating in the US to build back doors into their equipment and software to permit the Federal Bureau of Investigation (FBI) and National Security Agency (NSA) to conduct surveillance. CALEA also forces IT companies to turn over to the US government any encryption keys customers think are protecting them.

The Federal Communications Commission (FCC) provides a succinct description of CALEA's surveillance-portal requirement:

> CALEA is intended to preserve the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities as communications network technologies evolve.[5]

With regard to encryption, CALEA states that "A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication."[6] This is a backhanded way of saying IT companies that provide encryption services must ensure that the US government can decrypt all messages that use the encryption services those companies provide to customers.

When queried about who must comply with CALEA, the US Department of Justice states, "All telecommunications carriers or other entities engaged in the transmission or switching of wire or electronic communications as a common carrier for hire."[7] This includes Alcatel-Lucent, Nokia, Ericsson, China Telecom (which entered the US market in 2002), and China Unicom (which entered the US market in 2003), and it will apply to China Mobile if it manages to get

FCC Section 214 approval (considered in the next paragraph) to operate in the US.
In addition, any telecommunications provider (including facilities-based carriers, resellers, prepaid calling-card providers, and wireless-service providers) that offers calling services between the US and foreign points must obtain a certificate of authority under Section 214 of the Communications Act of 1934. Each Section 214 application that includes 25 percent direct or indirect foreign ownership is reviewed by the FCC's International Bureau and, as part of the bureau's processing, requires approval from Team Telecom, a working group of representatives from federal agencies outside the FCC. This group scrutinizes the application "for potential national security, law enforcement, and public interest concerns."[8]

Staff from the US Department of Homeland Security, Department of Justice (including the FBI), and US Department of Defense colead Team Telecom. Depending on the risk level assigned to the applicant, Team Telecom may impose certain risk-mitigation measures. One of Team Telecom's most common risk measures is to have the applicant install a repository of its customer data records on US soil, which has the effect of giving US courts jurisdiction over the data for purposes of ordering any disclosures for a national security or law enforcement investigation.[9] Similarly, Team Telecom may ask the applicant to make a resident US citizen available for service of due process from a law enforcement agency that needs to investigate the customer data.

So US surveillance regulations contain all three requirements that are contained in the Chinese counterterrorism law: (1) design systems so that home country agencies can conduct surveillance, (2) turn over encryption keys, and, when demanded, (3) store all user data within home country jurisdiction.

Fearing a loss of sales from allowing the FBI and NSA to decode encrypted messages, some American companies have taken matters into their own hands. In September 2014, Apple announced a new corporate privacy policy in which its latest mobile operating system, iOS8, is designed to prevent Apple—or anyone but the device's owner—from accessing content on the device.[10] Google quickly followed suit for its Android operating system. The heads of US intelligence and the FBI have strongly protested these unilateral company actions.[11]

US and Chinese Surveillance Regulations: Differences and Surprising Similarities

The IT sections of Chinese antiterrorism law differ from US legal-intercept regulations in that the former do not appear to claim to have extraterritorial application. In contrast, American regulations, upheld by American courts, require IT companies with operations in the US to permit extraterritorial access to emails and documents stored outside of the US.

US surveillance regulations contain all three requirements that are contained in the Chinese counterterrorism law.

The most prominent current case pertaining to these regulations features a challenge to Microsoft. Federal agents involved in a criminal or terrorist investigation served a search warrant to Microsoft's US headquarters, requiring Microsoft to find a customer's private emails, copy them, and turn them over to the FBI. The emails, however, are located exclusively on a computer in Dublin, Ireland, where they are protected by Irish privacy laws and the European Union Data Protection Directive. Microsoft refused and is now being held in contempt of court. In December 2014, Microsoft lodged an appeal in New York's Court of Appeals for the Second Circuit, with support from Apple, AT&T, and Verizon.

A second difference is that Chinese surveillance regulations are embedded in a far different setting with regard to the rule of law. The Chinese legal system does not intend to respect individual rights, citizen privacy, or intellectual property in the way the US Constitution demands and legal tradition respects. As for implementation, Chinese courts do not even claim to constitute an independent judiciary that operates free of Communist Party and state control. The World Justice Project has constructed a rule of law index that as of 2014 ranks the US at number 20 and China at number 92.[12]

On the other hand, if the world moves toward negotiating a multinational agreement for legal surveillance (addressed in the next section), the Chinese—and even some US allies—will undoubtedly point out that a large proportion of the warrants issued for surveillance in the US come from the Foreign Intelligence Surveillance Act (FISA) court under Sections 215 and 216 of the Patriot Act (the warrants are secret, meaning the exact number is not publically known).[13] US citizens or other persons whose records are subject to FISA warrants do not have the right to appear before the FISA Court.

Since the surveillance programs are classified, targeted persons generally have no way of knowing that their records are the subject of government scrutiny. Neither the FBI nor NSA needs to show probable cause or even reasonable grounds to believe that the person whose records it seeks is engaged in criminal activity, or have any suspicion that the subject of the investigation is a foreign power or agent of a foreign power. As amended in 2005, the only limitation in the Patriot Act is that the secret warrant has to be "relevant" to a national security investigation.

Other countries are suspected of having nonpublic procedures to issue nonpublic warrants for domestic surveillance as well, so agreement on appropriate standards for rule of law between the United States, China, and other countries (with as diverse approaches to privacy as those of Germany and France) is likely to be tricky in multilateral negotiations.

A Multilateral Agreement for Legal Surveillance?

It should be noted that the subjects of this paper—China's draft counterterrorism law and US legal-intercept regulations—are officially acknowledged frameworks to counter terrorist and criminal behavior. They are quite distinct from secret cyber intrusion programs and hacking behavior that evidently exist in both countries. With the rise of ISIS (or ISIL) alongside al Qaeda, US intelligence and law enforcement agencies say that these legal-intercept regulations are more needed than ever, and the Chinese Ministry of Foreign Affairs points out that China faces terrorism threats too.

China's draft counterterrorism law and US legal-intercept regulations are quite distinct from secret cyber intrusion programs that exist in both countries.

To prevent being discriminated against, US IT companies and suppliers are arguing for creation of a transparent multilateral framework, across jurisdictions, to govern lawful surveillance practices. Eight of the largest US multinational corporations (Apple, Google, Microsoft, Facebook, Yahoo, LinkedIn, Twitter, and AOL) signed a letter to President Obama and members of Congress arguing that "There should be a robust, principled, and transparent framework to govern lawful requests for data across jurisdictions."[14]

How such a multilateral framework for legal IT surveillance might be designed to meet the

legitimate needs of national security authorities and law enforcement agencies while protecting privacy rights of citizens is still an open question.[15] What is already clear is that double standards are unlikely to be tolerated. The US must prepare to see practices that it has already adopted become prevalent elsewhere or else be ready to modify American surveillance behaviors that US authorities do not want to see spreading around the globe.

About the Author

Theodore H. Moran (morant@georgetown.edu) is the Marcus Wallenberg Professor of International Business and Finance at Georgetown University.

Notes

1. The practical challenges of implementing such "buy Chinese" provisions was illustrated recently when China's bank regulator suspended new cybersecurity rules that would have required banks to replace foreign products with domestic alternatives. See Michael Martina and Gerry Shih, "China Suspends Bank-Technology Rules that Sparked Backlash," Reuters, April 17, 2015, www.reuters.com/article/2015/04/17/china-bank-rules-idUSL4N0XE1T120150417; and Simon Denyer, "China Removes Top U.S. Tech Firms from Government Purchasing List," *Washington Post*, February 27, 2015.
2. Jeff Mason, "Exclusive: Obama Sharply Criticizes China's Plans for New Technology Rules," Reuters, March 2, 2015, www.reuters.com/article/2015/03/02/us-usa-obama-china-iduskbnoly2h520150302.
3. "Counter-Terrorism Law (Initial Draft)," November 8, 2014, http://chinalawtranslate.com/en/tag/counter-terrorism-law/.
4. Ibid.
5. Federal Communications Commission, "Communications Assistance for Law Enforcement Act," 2013, www.fcc.gov/encyclopedia/communications-assistance-law-enforcement-act.
6. *Interception of Digital and Other Communications*, 47 USC 1002(b)(3).
7. Ask CALEA, "Frequently Asked Questions," February 2011, http://askcalea.fbi.gov/faqs.html.
8. Federal Communications Commission, "FCC Homeland Security Liaison Activities," 2012, http://transition.fcc.gov/pshs/docs/liaison.pdf.
9. Federal Communication Commission, "FCC Approves Softbank-Sprint-Clearwire Transactions," 2013, www.fcc.gov/document/fcc-approves-softbank-sprint-clearwire-transactions.
10. See Apple Inc., "Privacy," www.apple.com/privacy/privacy-built-in/.
11. Craig Timberg and Greg Miller, "FBI Blasts Apple, Google for Locking Police out of Phones," *Washington Post*, September 25, 2014.
12. World Justice Project, *Rule of Law Index 2014* (2014), http://worldjusticeproject.org/sites/default/files/files/wjp_rule_of_law_index_2014_report.pdf
13. Theodore H. Moran, "US Government Surveillance Regulations for IT Company Networks: Toward a Global Framework," AEI, December 2014, www.aei.org/publication/us-government-surveillance-regulations-for-it-company-networks-toward-a-global-framework/.
14. Reform Government Surveillance, "Global Government Surveillance Reform," www.reformgovernmentsurveillance.com/.
15. For preliminary examination of the challenges to constructing such a multinational framework, see Moran, "US Government Surveillance Regulations for IT Company Networks."