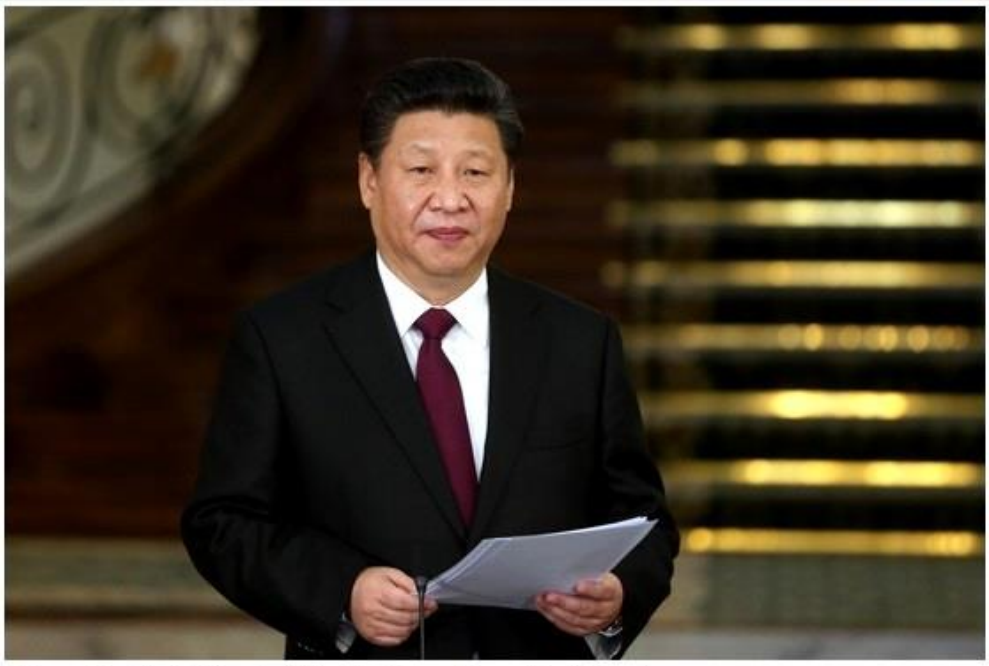
The Washington Post

Government cyber-surveillance is the norm in China — and it's popular



Chinese President Xi Jinping (Ebrahim Noroozi/Associated Press)

By Peter Fuhrman

Peter Fuhrman is chairman and chief executive of China First Capital.

SHENZHEN, China

When they met most recently, President Obama extracted from his Chinese counterpart, Xi Jinping, a solemn pledge to rein in Chinese surveillance and hacking of U.S. government agencies, companies and individuals. The backsliding seems to have begun almost immediately , with new reports of attacks by Chinese hackers in the United States. This conflict is not only a matter of competing national interests. At its heart are radically opposed conceptions of personal privacy and the legality of government monitoring.

Within China, government monitoring of private communication is not only common, but it is also explicit, institutionalized and generally quite popular. How much so? Just about every time I get an international phone call on my Chinese mobile phone, I'm pinged within seconds by a text message. It's an automated message from the anti-fraud department of the city of Shenzhen's Public Security Bureau (PSB), China's version of the FBI.

This message informs me in polite Chinese that the PSB knows I'm on the phone with someone calling from outside China, and so I should be especially vigilant, because the caller could be part of some scheme to steal my money or otherwise cheat me. The phone number for the anti-fraud hotline is included. International fraud is, as of now, the only criminal activity that China's government uses the mobile network to warn me about.

I do like knowing the Chinese police are on the job, warning and protecting the innocent. But I find it a little unsettling that they know immediately when I get an international call and are eager to inform me that they are keeping tabs. There's also the fact that I get these messages every time my 83-year-old father calls from Florida. Does the Chinese security apparatus know something about him that I don't?

China Mobile is the world's largest mobile phone company, with more than 800 million customers. To generate that automatic anti-fraud text message, international calls routed across the network in all likelihood pass through a server layer controlled and monitored by the PSB; calls from certain countries get flagged, and the text message is dispatched as the call is taking place. This isn't cyberspying. This is a deep integration.

It's not only the PSB. Upon landing on a trip to another country, I usually get an automatic Chinese-language text message from the Chinese Ministry of Foreign Affairs reminding me to behave politely and providing me with emergency contact numbers. It's a neat bit of coding. China Mobile reports to the foreign ministry, and perhaps other departments as well, when a user's phone begins seeking a roaming signal outside China. The system then generates the text welcoming the user to that country and populating the message with the number for the nearest Chinese embassy and consulate.

The U.S. National Security Agency has ways, if Edward Snowden's revelations are to be believed, to detect when a U.S. mobile phone is being used anywhere in the world. But it goes to a lot of trouble to keep a user from knowing that. Not so the Chinese state.

I've asked Chinese friends about this, and none expressed the slightest quibble about their government knowing where they travel or when they receive international calls. The government is just trying to be helpful, they explain. There's no real civil liberties debate about it, not even in the online channels where criticisms of Chinese policy are voiced.

In contrast, the United States has gone through a particularly bitter and protracted national debate over whether and how mobile phone companies, along with email providers, should share information and communications metadata with the NSA. It's not certain how much U.S. companies actively assisted the NSA in its domestic surveillance. But it's beyond doubt that none cooperates to the extent China Mobile evidently does with the PSB.

In the past several years, China has introduced some of the world's toughest laws, regulations and guidelines on data privacy. These tightly circumscribe what data companies can collect and introduce strict penalties for privacy breaches. Xi cites the laws as evidence that China has zero tolerance for hacking.

The quizzical result is: E-commerce giant Alibaba must not share anything about my Taobao account and is legally and financially responsible if my account gets hacked. But state-owned China Mobile (along with its two state-owned rivals, China Unicom and China Telecom) will freely share my private data with government departments at the national, provincial and local levels.

According to China's latest cybersecurity law, all companies operating in China, foreign and domestic, must share private data with the government to aid in official investigations. No specific mention is made of state-owned enterprises such as China Mobile. So, we don't know if China Mobile is required, encouraged or expected to share data that isn't part of any official investigation — such as who is getting international calls or traveling outside the country.

Some U.S. companies, including Apple, have introduced encryption techniques that make it harder for the NSA to access user data and conversations. No such effort is underway in China, nor, as far as I can tell, is anyone seriously suggesting it.

I'm no civil-liberties purist, so I don't particularly mind getting these text messages from the Chinese government. But it does serve as a vivid reminder that while living in China I'm subject to a set of rules and an official mind-set that are the obverse of those in the United States. Online and mobile communication privacy as we Americans understand it simply does not exist here.

https://www.washingtonpost.com/opinions/cyber-surveillance-is-a-way-of-life-in-china/2016/01/29/e4e856dc-c476-11e5-a4aa-f25866ba0dc6_story.html