Mondialisation.ca
Centre de recherche sur la mondialisation

China and the US: Big Brothers-In-Law? Beijing's New « Anti-Terrorism Law »

China's Anti-terrorism Law and the American Debate on Encryption

Par Boen Wang
Mondialisation.ca, 05 février 2016
Who What Why 4 février 2016

Région : Asia
Thème: Intelligence, Police State & Civil Rights

Originally published by WhoWhatWhy

Paging George Orwell…

"Big Brother" is getting even bigger in China. In a development that the author of "1984" would surely have appreciated, China recently passed an "anti-terrorism law" that seems fundamentally an excuse for a clampdown. It also eerily mirrors calls by US officials for access to encrypted communications.

China's law requires telecommunications and other companies to decrypt and hand over data related to "terrorist" investigations.

And who is a "terrorist?" Just about anyone.

"Terrorism" is so vaguely defined in the law, prosecutors could use it to criminalize perfectly innocent activities," Patrick Poon, a Hong Kong-based researcher for Amnesty International, told *WhoWhatWhy*. "These could include posting on social media about sensitive topics, reporting on alleged terror attacks, or any behavior deemed upsetting to "social stability."

Failure to hand over the decrypted data could result in fines of up to 500,000 yuan (a bit over 76,000 USD) and imprisonment of up to 15 days.

Human rights groups have roundly criticized the law for the broad powers it confers to the Chinese government.

It's not just individuals who are in danger. A legal review from Lexology notes that the Chinese law does not define the terms "telecommunications operators" or "internet service providers." This means almost any company, Chinese or foreign, that provides any technological service could be targeted.

China, US Sing the Same Tune on Encryption

Explaining why his government needs such wide-ranging access to Internet communication, Foreign Ministry spokesperson Hong Lei said:

It is imperative for us to prevent and crack down on cyber-enabled terrorist crimes….

teleservice operators and network service providers shall provide technical support such as technical interface and decryption to public and national security organs in their missions to prevent and investigate terrorist activities.

Sounds familiar? Compare it with the congressional testimony of Federal Bureau of Investigation Director James Comey:

[C]hanging forms of Internet communication and the use of encryption are posing real challenges… The United States government is actively engaged with private companies to ensure they understand the public safety and national security risks that result from malicious actors' use of their encrypted products and services.

Poon emphasized that the parallels go only so far: US citizens have "many more legal protections and mechanisms that allow you to challenge the government's actions."

> "If you're trying to find a needle in a haystack, you don't add more hay first," he said. "Unless you want to turn into a mass surveillance police state, being able to look at everything is not going to get you very far. Targeted stuff, narrowing in on the right people, is more likely to get you what you really need."

But the parallels are there. Last March, President Barack Obama criticized a draft version of China's anti-terrorism law for its unseemly overreach. He said US tech companies would not be willing to "turn over to the Chinese government, mechanisms where they could snoop and keep track of all the users of those services."

So Obama should not have been surprised when US tech executives resisted calls by American law enforcement officials for just such mechanisms. Apple CEO Tim Cook, for example, has repeatedly defended the need for unbreakable encryption.

Yet the drumbeat for granting US spy agencies exceptional access to internet communications continues.

"Keys Under Doormats"

In more recent congressional testimony, Comey argued for allowing the government a so-called backdoor into all nominally encrypted Internet communications. He dismissed the "folks who have said… we're going to break the internet, or we'll have unacceptable insecurity if we try to get to a place where court orders are complied with" and insisted that encryption is "not a technical issue."

Steven Bellovin is one of those folks who insists that encryption *is* a technical issue. A computer science professor at Columbia, Bellovin co-wrote a paper with 14 other prominent academics in July called "Keys Under Doormats." The paper detailed the technical infeasibility of "exceptional access mechanisms," in addition to the thorny societal and logistical questions such mechanisms would raise.

"We just don't think people can get this right," Bellovin told *WhoWhatWhy*. "It's just a very, very hard problem."

Attempting to implement exceptional access mechanisms, according to the paper, would

undermine cybersecurity by reversing normal security measures. At risk would be so-called forward secrecy (an added security measure that prevents intruders from decrypting communications) and authentication (think of the little padlock icon that appears in your web browser when you, say, log into your bank account).

In addition, any government backdoor would likely introduce “unanticipated, hard to detect security flaws” due to the sheer “complexity of today’s Internet environment.”

These arguments have not dissuaded American officials from trying to follow in China’s footsteps by insisting on exceptional government access to all encrypted communications — of course always in the name of fighting terrorism and with no acknowledgement that this access could ever be abused.

Whether or not China will be able to implement its law on a technical level remains to be seen.

Bellovin, however, thinks US intelligence agencies should focus on analyzing pre-existing data rather than on trying to collect even more data.

“If you’re trying to find a needle in a haystack, you don’t add more hay first,” he said. “Unless you want to turn into a mass surveillance police state, being able to look at everything is not going to get you very far. Targeted stuff, narrowing in on the right people, is more likely to get you what you really need.”

In George Orwell’s “1984,” the world is divided into three mega-states that are in constant conflict although they are alike in exercising cradle-to-grave control over their citizens.

When it comes to an appetite for keeping an eye on everyone, Big Brother knows no nationality.

La source originale de cet article est Who What Why

Articles Par : **Boen Wang**

Contact média: media@globalresearch.ca