South China Morning Post

# Why China's draft cybersecurity law has chilling implications for the internet and multinationals

**Proposed legislation steps up data protections as well as government controls online**

Nectar Gan
nectar.gan@scmp.com

PUBLISHED: Wednesday, 08 July, 2015, 3:39pm
UPDATED: Thursday, 09 July, 2015, 1:40pm

China's cybersecurity has been a problematic area in relations with economic partners like the United States. Photo: Reuters

China's top legislature has published a draft cybersecurity law that would cement government control over the internet and data, rules analysts said could further limit online debate and affect multinational companies doing business in China.

The 68-article law was drafted to "safeguard cyberspace sovereignty and national security" from the threat of cyberattack, cybercrime and the spread of "harmful" information online, according to a statement by the National People's Congress.

The full text of the draft, which had its first reading at an NPC Standing Committee session last month, was posted on the legislature's website on Monday for public consultation.

It steps up privacy protections for users' data to prevent it being stolen, leaked or used illegally. But it also beefs up the government's power to obtain records of the dissemination of information deemed illegal.

It also grants the government the right to restrict internet access in places where public security is threatened.

It does not refer to Hong Kong or Macau.

Guangzhou-based rights lawyer Wu Kuiming said the draft law was a legal foundation for the government's established practices on internet control and censorship.

If the draft goes through, censors would have the right to delete information that was counter to laws and regulations, and to stop that information from entering China.

The draft would also impose similar responsibilities on internet operators, including websites and social media platforms, and make it their duty to report breaches to the authorities.

Operators would require users to log in with their real names. Failure to comply could result in fines of up to 500,000 yuan (HK$632,000) and the loss of a business licence.

Wu said although such practices were commonplace, the law - once passed - could still send a chill through the online community and exert extra pressure on activists, critics and dissidents as well as internet operators.

The law lays out special security requirements for all networks and systems in "critical industries" such as telecoms, energy, transport, finance, national defence and military matters, government administration and other sensitive fields. The government will review products or services in these areas that could affect national security.

Stuart Hargreaves, a law professor specialising in technology and internet law with the Chinese University of Hong Kong, said such rules were likely to put overseas companies doing business in China at a disadvantage.

"This rule will benefit domestic manufacturers and programmers as their foreign counterparts are less likely to want to turn over their source code or design specifications to Chinese authorities, and in some cases may even be barred by their own governments from doing so," Hargreaves said.

He warned that the draft could have the opposite of its intended effect to protect China's network security.

"The mandatory insertion of 'backdoors' into networking equipment to allow state access inevitably creates vectors for [others] to snoop on private communications and is thus counterproductive from a 'network security' perspective, let alone a 'user privacy' perspective," he said.