Encryption and Privacy under the PRC Laws

Prof. dr. Hong Xue © 2017

Director of Institute for Internet Policy & Law

Beijing Normal University

Abstract

Encryption of online data and communications may serve to protect people's privacy in digital age. However, because of its multiple functions on military, security and commercial operation, encryption is subject to a web of regulations around the world. Since 1999, China has been strengthened the regulation on use of encryption technologies, products and services through a variety of scattered and unsystematic administrative rules, measures and requirements. On June 1, 2017, China's Cybersecurity Law entered into force and provides a more comprehensive legal framework on regulation of encryption. Implementation of the new Cybersecurity Law is expected to impacts particularly the following three critical aspects of encryption and privacy.

1. Encryption Requirements

From 2000, all companies — foreign and domestic — must register any software that uses encryption with the Chinese government, along with details of any person that uses the software, including all Internet-based software (e.g., Web browsers and e-mail packages),

regardless of the strength of encryption. In addition, software used in China must use encryption software manufactured in China. The Cybersecurity Law although modifies the above requirements contains considerable legal uncertainty and ambiguity. According to the Law, network products and services shall comply with the compulsory requirements provided in the relevant State standards; network critical apparatus and products specialized in network security shall not be sold or provided unless their safety or compliance is verified or examined by the qualified organizations according to the compulsory requirements provided in the relevant State standards. The catalogues of network critical apparatus and products specialized in network security will be composed and enacted by the Cybersecurity agencies along with the other agencies. It’s not available at the moment.

2. Virtual Private Networks (VPNs)

VPNs encrypt Internet communications between two points so that even if the data being passed is tapped, it cannot be read. A VPN connection from inside China to outside it means that the user's internet connection effectively starts outside the "Great Firewall" – in theory giving access to the vast range of information and sites that are blocked, including the resources sites such as Twitter, Facebook and Google. Under the Cybersecurity Law, VPNs may be severely punished as the procedures and tools that endanger cybersecurity by disrupting network

normal functions and defensive measures; and, knowingly provision of the technological support, advertisement or payment services for VPNs is also subject to legal punishments.

Once a VPN is charged with violation of the Law, the users' data would be subject to law enforcement actions and there may be privacy concerns over data breach or abuse. The Cybersecurity Law, therefore, provides that Cybersecurity or other governmental agencies shall not use the information acquired from exercise of their duty for any purpose other than safeguard of cybersecurity.

3. Technological Supports and Assistances for Law Enforcement

Apple's decision to resist a court order to unlock a password-protected iPhone belonging to one of the San Bernardino killers has created a worldwide privacy shockwave, with campaigners around the world expecting the struggle to carry major implications for the future of mobile and internet security. If happened in China, the Chinese Cybersecurity Law, however, would have no leniency for Apple to resist any order for law enforcement because any network owner, operator and service provider shall provide technological support and assistance for the activities conducted by the public security and state security agencies to legally safeguard state security and criminal investigation.