LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Privacy & Cyber Practice

21 November 2022 | Number 3034

Hong Kong Proposes Reforms to Address Cybercrime

The reforms aim to address the rise in cybercrime and cyberattacks in an age of rapid digital developments.

The Law Reform Commission of Hong Kong (the LRC), via its Sub-committee on Cybercrime, issued a consultation paper "Cyber-Dependent Crimes and Jurisdictional Issues" (the Paper) in July 2022. The Paper sets out initial proposals for law reform to address the growing number of cybercrimes and cyberattacks and the challenges for cybersecurity in connection with advancements in information technology and the risk of technological exploitation for criminal purposes.

As part of the consultation, the LRC sought responses to questions that primarily focused on the scope of exemptions and defences to new offences. The consultation period ended on 19 October 2022. The LRC has not yet published the conclusions.

The Paper is the first of three consultation papers to be published by the LRC in relation to cybercrime and focuses on cyber-dependent crimes (i.e., crimes that can be committed only through the use of information and communications technology devices, where the devices are both the tool for committing the crime and the target of the crime). The second paper will target cyber-enabled crimes and the macro challenges in the digital age and evidentiary, while the third paper will tackle evidentiary and enforcement issues.

Existing Legislative Framework

At present, Hong Kong does not have any specific legislation that addresses cybercrime or cybersecurity. There are cybercrime-related offences, which are scattered across various pieces of legislation, namely:

- **Telecommunications Ordinance**
  - **s. 25(a):** Any person (not being a telecommunications officer, or a person who, though not a telecommunications officer, has official duties in connection with a telecommunications service) who wilfully secretes, detains or delays a message intended for delivery to some other person.
  - **s. 27:** Damaging, removing or interfering with a telecommunications installation with intent to: (a) prevent or obstruct the transmission or delivery of a message; or (b) intercept or discover the contents of a message (this does not include metadata).
  - **s. 27A:** Gaining unauthorized access to a computer by means of telecommunication.

- **Crimes Ordinance:**
  - **ss. 59 and 60:** Destroying or damaging property, or intending to destroy or damage property, without lawful excuse, including misusing any computer program or data held in a computer.
  - **s. 161:** Gaining unauthorized access to a computer with: (i) intent to commit an offence; (ii) dishonest intent to deceive; (iii) a view to dishonest gain for himself or another; or (iv) a dishonest intent to cause loss to another.

The Paper compares cybercrime laws in seven other jurisdictions, including Australia, Canada, England and Wales, Mainland China, New Zealand, Singapore, and the US. The LRC notes that most of these jurisdictions have bespoke cybercrime legislation, or dedicate part of their codified law to cybercrime.

New Cybercrime Offences

To address the fact that Hong Kong does not have bespoke cybercrime legislation and that offences are scattered across ordinances, the LRC proposes the introduction of five new offences (the Offences):

1. Illegal access to program or data
2. Illegal interception of computer data
3. Illegal interference of computer data
4. Illegal interference of a computer system
5. Making available or possessing a device or data for committing a crime

Whilst the Paper stipulates that the Offences represent the "core species of cybercrime recognised globally that should be addressed", it does not elaborate on how the Offences were identified. Although the existing legislative framework already criminalises the majority of the activities envisaged under the Offences, the Paper aims to cover and consolidate certain discrepancies and overlaps in the framework.

Nonetheless, this raises the question of whether addressing these discrepancies requires a new, bespoke legislative framework, or whether they could instead be addressed by updating the existing legislation.

Scope and Extraterritorial Application

Given the broad, borderless nature of cybercrime, the LRC proposes the extraterritorial application of the Offences — i.e., that Hong Kong courts should assume jurisdiction if factual and causal connections exist between a cyberattack and Hong Kong. Naturally, one of the key challenges in addressing cybercrime is the borderless nature of the internet and how to grapple with jurisdictional restrictions. In light of this, although common law jurisdictions typically limit their laws, these jurisdictions are increasingly looking for solutions to address this cross-border challenge in the advent of the digital age.

The LRC therefore recommends that Hong Kong courts should have jurisdiction if the cybercrime has a connection to Hong Kong, including if:

- the act or omission occurs in Hong Kong;
- the victim is a Hong Kong permanent resident, ordinarily resides in Hong Kong, or is a company carrying on business in Hong Kong;
- the target program or data is in Hong Kong; or

- the perpetrator's act has caused or may cause serious damage to Hong Kong or has threatened or may threaten the security of Hong Kong.

For the summary offence of illegal access to programs or data, the LRC considers that Hong Kong courts should only have jurisdiction if the act constitutes a crime in the jurisdiction where it occurred.

The offence of making available or possessing a device or data for committing a crime presents certain challenges, particularly for organisations not based in Hong Kong. With the extraterritorial application, any organization that carries out business in Hong Kong could be liable, including foreign organisations without a Hong Kong presence. This could include IT platform operators and service providers (e.g., cloud providers) that are based overseas and do not have a Hong Kong presence, but may have users based in Hong Kong or may conduct business with Hong Kong organisations.

Penalties and Sentencing

The Paper recommends an increase in the limitation period for summary offences. It stipulates that the current limitation period for summary offences under s. 26 of the Magistrates Ordinance (which is generally six months from the time when the matter arose) is insufficient for investigations into cybercrime and therefore for the summary proceedings for the Offences. As such, the LRC recommends extending the limitation period to two years from the discovery of any act, omission, or other events, the proof of which is required for conviction of the offence.

On sentencing, given the differing nature of each Offense, the LRC proposes that all Offences carry two maximum sentences — one that applies to summary convictions (two years' imprisonment) and one that applies to convictions on indictment. The maximum sentence under most of the Offences is 14 years, in contrast to the current range of two to 10 years' imprisonment for offences under the existing legislative framework.

If you have questions about this Client Alert, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Kieran Donovan
kieran.donovan@lw.com
+852.2912.2701
Hong Kong

Anthony Liu
anthony.liu@lw.com
+852.2912.2576
Hong Kong

You Might Also Be Interested In

Hong Kong Issues Guidance on Recommended Data Security Measures

China Unveils Draft Standard Contract and Provides Clarifications on Cross-Border Data Transfer Mechanisms

China's New Data Security Law: What to Know

The Evolution of the UK Online Safety Bill: What's Next?
