CORPORATE**Counsellor**
TILLEKE & GIBBINS

The Cybercrimes Law

Following a draft that had been originally presented for discussion since 2002, the Thai government has enacted a Computer Crimes Law (CCL) that came into effect on July 19. The final version has incorporated many changes from previously distributed drafts. We provide herein a general overview of the new law and a commentary on significant issues that have been the subject of questions and discussion.

In the past Thai prosecutors were forced to apply general rules of trespass and wrongful conduct to prosecute computer hackers, which oftentimes proved difficult. Now the CCL broadly outlaws any kind of computer hacking, whether or not there is any resulting damage or modification caused to the system being hacked.

Sharing of passwords and dissemination of hacking tools or techniques can also potentially lead to criminal liability, even if the person who does so has not used such passwords or techniques to carry out an unlawful act.

Intercepting data without authorisation is also a crime, regardless of whether such data is intercepted through hacking of protected systems.

An anti-spam section prohibits the transmission of data or e-mail (a) in such a manner that causes nuisance to others (b) by using a concealed or fabricated source. In other words, even transmissions that cause nuisance may not create criminal liability if their source is properly identified.

The CCL makes it a criminal act to post information that is either (a) false, (b) threatens the national security of Thailand or causes a public panic, (c) constitutes an act of terrorism, or (d) contains pornography. This section is directed primarily at users of internet services who post such information on public websites.

Service providers would be relieved to find that they are not liable for any of the above posted through their websites provided they themselves do not "willfully aid or allow" such false and/or unlawful data to be posted.

Posting altered images to defame or expose persons to public ridicule or embarrassment also incurs criminal liability.

Service providers are not expressly excused from liability in these cases.

Penalties provided by the CLL include fines up to 500,000 baht and/or jail time up to 20 years according to the severity of the crime.

Unlike other Thai laws, the CCL is expressly given extraterritorial jurisdiction — applying not only to such unlawful acts conducted within Thailand but also to any act conducted outside Thailand which are either conducted by Thai citizens (regardless of effect within Thailand) or which affect the Thai government or any Thai entity.

The CCL provides powers of search and seizure to the competent officials enforcing the law and addresses the procedures for use of such powers. Officials may request computer traffic data and/or user identification data from service providers without obtaining a court order provided they have "reasonable grounds" to suspect the commission of a crime.

For broader data searches and equipment seizures, reasonable grounds must be presented to the courts as part of an application for a search/seizure warrant.

The courts must consider the application on an expedited basis and issue an appropriate search and seizure warrant before the officials can effect same. This creates a check on government searches and seizures similar to that of western nations that require some level of proof before such searches and seizures can be conducted. Whether the Thai courts will be strict or lax in requiring "reasonable grounds" before authorising a search is something to be seen.

Section 238 of the 1997 Constitution provided that: "In a criminal case, a search in a private place shall not be made except where an order or a warrant of the Court is obtained or there is a reasonable ground to search without an order or a warrant of the Court as provided by law." Contrary to some public criticisms, searches mandated by the CCL do not create any new power that goes beyond what was provided in the 1997 Constitution.

The CCL provides that failure to comply with an official inquiries would result in a fine of up to 200,000 baht per offence, plus a fine of up to 5,000 baht for each day of non-compliance. However, if a party can show that the officials did not have reasonable grounds to make an inquiry and/or obtain a warrant, such penalties would also necessarily fail.

Moreover, notwithstanding the said penalties, the enforcement provisions of the new law cannot supersede a person's right against self-incrimination as provided under the 1997 Constitution (and will likely be incorporated into the new constitution). Still, third parties such as ISPs who are asked to provide data on their subscribers' identification and usage may be obliged to comply with inquiries supported by reasonable grounds.

More detailed commentary and an unofficial English translation of the CCL can be found at www.tillekeandgibbins.com.

John Fotiadis is a consultant for the Commercial Department and Kamil Chaudhary a summer intern with Tilleke & Gibbins International Ltd. Please send comments or suggestions to Marilyn Tinnakul at marilyn.t@tillekeandgibbins.com