Bangkok Post The world's window on Thailand

CORPORATE COUNSELLOR

IT law update, part 2: Amending the Computer Crimes Act gives cause for concern

Published: 30/01/2015 at 06:00 AM
Newspaper section: Business

The cabinet of Thailand recently approved a series of bills that aim to reflect the importance of information technology in the economy. They relate to computers, cybersecurity, personal data, information technology and telecommunications. Among them is the Bill to Amend the Computer Crimes Act, which proposes several changes to the existing law.

Some of these changes, however, may be cause for concern. Following on from last week's article, which focused on the changes being introduced by the Cybersecurity Bill, this article will address the proposed changes to the Computer Crimes Act.

Certain changes proposed by the bill are organisational in nature, accounting for the creation of the Ministry of Digital Economy and Information Technology, as well as the new National Cybersecurity Committee. Sections on who has the authority to act under the Computer Crimes Act and confidentiality obligations would also be expanded.

As for operative provisions, there are adjustments to penalties for several of the computer-related offences in the Act, which are meant to reflect their relative seriousness. There is also an entirely new section dealing with child pornography. Another notable change is an amendment that expands the circumstances in which a court can be petitioned to block dissemination of content. All of these amendments are important, but Sections 11, 14, and 26 are particularly noteworthy.

Section 11 currently provides that any person sending computer data or electronic mail to another person and covering up the source of such data in a manner that disturbs the normal operation of the other person's computer system shall be subject to a fine. The amendment would add an element to the offence, i.e., that the sender fails to provide an opportunity for the recipient to cancel or reject the unwanted data or electronic mail.

The amendment also envisages that the minister would promulgate regulations on sending such data and email, and require compliance. This would provide a means of fighting spam email and messages, and depending on the content of the ministerial regulations, perhaps online marketers would be required to provide an opt-out or possibly an opt-in mechanism. While some online marketers may have concerns, in general, this is a much-welcomed change.

A change has also been proposed to Section 14, which addresses service provider liability. The current wording provides that any service provider intentionally supporting or consenting to particular offences within a computer system under its control shall be subject to the same penalty as the person committing the offence.

Section 14 has long worried service providers all over Thailand, as it left open the possibility that they could be held liable for content posted by their customers or service users. The bill would potentially lessen these concerns by providing for the minister to promulgate regulations on actions to be taken by service providers in preventing the dissemination of objectionable computer data, and for the minister to order the destruction of particular computer data.

In line with this, under the amended Section 14, if the service provider proves that it followed such instructions of the minister, the service provider would not be liable. Assuming the ministerial regulations are sensible, this has the potential to be quite beneficial in limiting liability not only for internet service providers but also for all others that are deemed "service providers" under the law.

In addition, a change has been proposed with respect to data retention obligations. Under Section 26 of the current law, computer traffic data must be retained for 90 days, unless a competent official instructs service providers to store data longer, i.e., up to one year on a special case-by-case basis or on a temporary basis. The bill would amend this section to allow a competent officer to order that it be kept for up to two years, where necessary.

One would expect privacy advocates to have concerns about these amendments, but it should be noted that maximum period of data retention is but one of the variables in the overall data retention regime.

Different countries have very different data retention regimes, so it is difficult to generalise about what is normal. On the whole, however, Thailand's data retention regime is in line with that of several other major jurisdictions, and this remains the case even if the maximum retention period is extended to two years, as is proposed.

Most of the proposed amendments to the Computer Crimes Act would be improvements over the current Act. As always, however, success will depend on the regulations to be promulgated under the Act.

Assuming the regulations are sensible, most of these amendments will operate to the benefit of service providers and internet users alike.

This article was prepared by David Duncan, consultant, and Jeffrey Blatt, counsellor, in the corporate and commercial department at Tilleke & Gibbins. Please send comments to Andrew Stoutley at andrew.s@tilleke.com