The following article does not purport to offer legal advice. The observations it offers are based on unofficial translations of the Thai laws and regulations.

Ensuring compliance with Thai Computer-Related Crimes Act

By Nic Garnett

The Computer-Related Crimes Act ("CCA") of Thailand came into force in July 2007. It was followed a month later with the publication of a Notification of the Ministry of Information and Communications Technology providing more detail relative to the scope and application of the law.

The law has attracted a certain amount of controversy particularly with regard to freedom of speech issues. That is not the focus of this article. The purpose here is to introduce the basic content of the law and consider what businesses and their staff need to do to comply with its requirements – and, of course, to avoid committing any offences.

First, a word about context. It is now obvious that the internet is transforming society and the business world to a far greater extent than was imaginable a mere 15 years ago. Gutenberg's printing press pales in comparison in terms of impact. From a lawyer's point of view this dramatic online evolution (which is ongoing) creates, at a very high level, two primary areas of concern:

- the internet as a new "venue" for committing unlawful acts
- the internet as means to expand the reach of acts which are already classed as unlawful

Between these two poles, a vast number of issues stand to be regulated, including such issues as contract, service responsibilities, security, consumer protection and fraud and, of course, jurisdiction. The list is extensive. In Europe, there is a growing corpus of law aimed at making the internet safe for social interaction and commerce. The CCA in Thailand seems perhaps more stark in terms of its remit because it forms part, for the present, of a smaller body of computer-related law. Its genesis and objectives are however both recognisable and logical.

Scope

The key parts of the CCA for the purposes of this article can be broken down as follows:

- Definitions: important, particularly in relation to who may be considered a "service provider"
- Cybercrimes: they track for the most part the crimes enumerated in Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems of the 2001 Convention on Cybercrime
- Content crimes: these relate to unlawful activities already dealt with under Thai law as they may be conducted online. This includes defamation, offences against the honour, dignity and reputation of the Royal Family and its institutions (lèse-majesté), and the dissemination of pornography or indecent information
- Enforcement: primary responsibility lies with the Ministry of Information and Communications Technology
- Service provider responsibilities: maintaining computer traffic data

Foreign entities conducting business in Thailand through local subsidiaries are of course subject to the provisions of the law. And importantly, a content crime does not have to be committed in Thailand to constitute an offence under the CCA. In 2011 a Thai-born US citizen published online, from the US, a translation of Thai text that was judged offensive to the Royal Family. On his next visit to Thailand the US citizen was arrested, charged and convicted under the CCA. (He subsequently received a Royal pardon).

Impact of the law

So what should foreign businesses worry about with regard to the law? Essentially, three things:

- Doing something that may be held to constitute a crime under the CCA
- Being held liable as a service provider for a crime committed by an

employee – or a guest in a hotel or a customer (for example, using the Wi-Fi connection in a coffee shop). CCA s.15 provides that a service provider who intentionally supports or consents to a content offence under s.14 shall be liable to the same penalty as the primary offender
- Failing to comply with traffic data retention requirements: a hefty fine of up to THB 500,000 can be imposed for each instance of non-compliance

In response, prudent managers should consider the following:

- Read the CCA – it's widely available in translation online. Consider the content offences in particular. Act accordingly and sensitively, particularly in relation to online expression of matters touching on the dignity of the Royal Family, public morality or local politics. Avoid defamatory statements regardless of truthfulness/veracity
- Understand that the definition of service provider includes any entity which provides internet access, a local area network or server facilities. Ensure the necessary workplace, estate or occupancy policies are in place. Be alert as managers: individuals from Directors to webmasters could be personally liable under the CCA if they have actual knowledge of any offence committed through the system they manage but do nothing about it
- Review the computer traffic data retention requirements thoroughly with the CIO or an appropriate external advisor. They are extensive yet non-exhaustive as set out in the regulations
- If in doubt, have no doubt: seek the advice of expert Thai counsel. This is a serious matter

Service Provider requirements

The basic structure of the service provider traffic data retention requirements is as follows:

- CCA s.3 defines the service provider to include any entity which provides internet access, services for communicating between computers or computer data storage whether in its own name or via a third party
- CCA s.26 stipulates that a service provider shall retain computer traffic data for not less than 90 days (or up to 1 year if so ordered by a competent official) relating to identified, individual users from the start to the end of the use of the service
- The regulations provide further details about what data to store and how to store it

The regulations are in three parts: the body of the regulatory text and two annexes. First, through Annex A they identify different categories of service providers, offering examples within each category. Then, in Annex B, the regulations set out the particular data that must be retained by the different categories of service providers. The lists of data are extensive but, reportedly, not exhaustive.

Finally, as general provisions, the regulations stipulate arrangements for maintaining the integrity of the data, storing it securely and in a way that makes it readily deliverable to competent officers who require it. They also require the setting of equipment to a single international reference time.

Conclusion

It is surprising that, given the importance of the law, information regarding its application in practice remains somewhat limited. This may be partly due to the fact that, in addition to the Ministry of Information and Communications Technology, a number of different enforcement agencies have been involved in enforcement of the law, including the Technology Crime Suppression Division of the police and the Department of Special Investigation.

What is known is that the number of prosecutions for both cybercrime and content offences is growing – confirming both our increasing reliance on the internet and our growing need to know about its regulation as a matter of basic prudent business practice.

** This article does not purport to offer legal advice. The observations it offers are based on unofficial translations of the Thai laws and regulations*

Nic Garnett is a consultant in the intellectual property group at Tilleke & Gibbins.
Tel: +66 2653 5841
Email: nic.g@tilleke.com