

This month we talk with **Bernard Collin** – CEO of SafeComs Co. Ltd. about crimes committed with the use of computer

# Cyber Crime Gets a New Act

*A few weeks after she broke up with her boyfriend, Noi found rude pictures of herself posted on local websites. The pictures had been altered to cause her extreme embarrassment.*

*Somsak, a mid-50s widower, was cheated out of a substantial amount of money by a woman he was corresponding with on an internet chat site.*

*Boris, a small tour operator who relies on his website for bookings, lost thousands of dollars when his site was hit with a week long 'denial of service' attack. He was the target of an organized gang who extort money from people making a living on the internet.*



## Defining crimes

“Every society gets the kind of criminal it deserves. What is equally true is that every community gets the kind of law enforcement it insists on.” Robert Kennedy

Thailand’s Computer Crime Act, or CCA, broadly defines three types of activity as criminal acts. The first covers ‘illegal access and use of computer systems and computer data’, more commonly known as plain old hacking, spamming and virus attacks. In the language of the Act, this includes:

Accessing a computer system and its data without authority or permission:

Giving people passwords and other confidential information that would allow them to gain access to other peoples’ computer systems and data:

- Intercepting electronic communications and data:
- Causing damage to or changing computer data in whole or in part:
- Causing the work of a computer system to be suspended, delayed or disrupted:
- Disguising the source of computer data or electronic mail in a way that disturbs the operation of other peoples’ computer systems.

Hackers, spammers and malicious virus distributors now face the well-deserved opportunity of spending up to 15 years in jail if their activities are considered to be disruptive or threatening to public security or public services.

The second general area of now criminal activities covers fraud; distributing technology or data that could be used to break into computer systems or could affect public security. This includes:

- Introducing forged or false data into a computer system that could cause damage to a third party, the country’s security or cause public panic:
- Introducing forged or false data to a computer system related to an offense against the Criminal Code:

“**W**hat these three, and thousands more like them, have in common,” says Bernard Collin, CEO of SafeComs Co. Ltd., “is that they were victims of crimes committed through or with the use of a computer.” Thanks to Thailand’s new Computer Crime Act (CCA), people like Noi, Somsak and Boris can now hope to identify the perpetrators and prosecute those who caused them financial loss or public embarrassment. And that’s a good thing.

New technologies have always opened up new opportunities, including opportunities for crime. There was no ‘grand theft auto’ and no ‘yield to the right of way’ before the invention of the automobile, no credit card fraud before the invention of plastic, and no cyber crime when the Commodore PET was the pinnacle of computing technology. Just how the new law works, what it means to people like you and I, and what we need to do about it is the subject of vigorous debate here and elsewhere.

AD



Section 26 of the Computer Crime Act makes it mandatory for all service providers to keep records of their users' email, chat, internet usage and personal identification for a minimum of 90 days. The details were left to the Information and Communication Technology (ICT) Ministry. On August 23, 2007, the Ministry issued a Notification defining in more detail exactly who is a service provider and what data records they have to keep. These requirements became effective on 24 August, 2008. Bernard says, "A lot of people are now at risk of becoming accidental criminals."

## Am I a service provider?

Under Section 3 of the CCA and further detail in the Notification, a 'service provider' is anyone who provides internet access or computer communications to other people or a person who provides data storage services to others. "The Ministry paints with a broad brush," says Bernard.

- Introducing data of a pornographic nature that is publicly accessible.

These activities will be justly rewarded with imprisonment for up to five years or a fine of up to 100,000 Baht or both.

The third general category of criminal acts is designed to protect personal privacy rights. The CCA makes it a crime to import into a computer system that is publicly accessible, any data where another person's picture appears either created, edited, added or adapted, "in a manner that is likely to impair the third party's reputation or cause that party to be isolated or embarrassed". This is a wide definition and applies to things like blog discussions and chat rooms or publishing 'amusing' mobile phone video clips on publicly accessible websites like 'YouTube'. Bumping off the offended party won't work because the law applies regardless of the server's location and a victim's next of kin can act in the event of his or her decease. Jilted lovers will have to settle for the traditional smashing of crockery.

## Show me your warrant!

Having defined a criminal act, the police now need evidence that a crime was committed. Just like the Hollywood movies, they have to have a court order or 'search warrant', and they have to show it to you before they can do any of the following:

- Copy data from a computer system or instruct a person to deliver data or computer storage equipment to the police:
- Inspect or access a computer system or data belonging to any person that is or may have evidence relating to an offence under the CCA:
- Decode computer data:
- Seize a suspect computer system for the purpose of obtaining details of an offence under the CCA.

And because they are nice guys, they will not cause any 'excessive interference' with your business operations in the process of doing any of these things and return any equipment and files within 30 days. Whatever the size of your business, if you rely on computers, the best policy is the Boy Scout motto: be prepared.

## Accidental criminals

"It's one thing to give police authority to gather evidence of a crime," says Bernard Collin, SafeComs CEO, the next trick is to make sure there is evidence to gather." That evidence comes in the form of data that internet service providers must now capture and store.

Under this definition, the law applies to any organization or business which has a website or provides access to the internet for their employees or customers. This includes the obvious big telco providers like TRUE, DTAC, AIS and TOT, and a host of other Internet Service Providers from Loxinfo to Mama Wifi. It also includes small business owners like you and I, universities that provide internet services for students, and hotels, coffee shops, apartment complexes and condominiums that provide fixed line or wireless internet access to the public or their employees. All these service providers are now required to track, capture and store a long list of data traffic and maintain personal data identifying users for 90 days or be subject to imprisonment and fines of up to 500,000 Baht.

## Data retention: Nothing new

There is nothing new or particularly difficult about 'data retention'. In Europe and America, governments started officially enacting data retention laws in the late 1990s and early 2000s. Commercial sites like Amazon and Google have been retaining data on customer transactions since Day 1. Governments are interested in combating terrorism and crime. Companies are interested in your shopping habits.

So what, exactly, is this data the Ministry will be asking service providers to retain? To the average reader, it looks like 'geek speak'. To an expert, all those numbers make it possible to:

- Trace and identify the source and content of a communication:
- Trace and identify the destination of a communication:
- Identify the date, time and duration of a communication:
- Identify the type of communication:
- Identify the communication device:
- Identify the location of mobile communication equipment.

Easy to see why it is so appealing to both law enforcement agencies and marketing managers.



SafeComs Network Security Consulting Co., Ltd.  
21/16 Premier Condominium, 4th Floor, Unit 401,  
Sukhumvit 24 road, Klongton, Klongtoey,  
Bangkok 10110, Thailand Tel: 02-259-6281-3  
www.safecom.com  
e-mail: info@safecom.com