Microsoft

A perspective on the implementation of the Convention's computer security offences in the Asia Pacific region

Julie Inman Grant, Director Internet Safety and Security

Microsoft Asia Pacific

11 June 2007

Background to Microsoft's "Gap Analysis" of Cybercrime Laws in Asia Pacific

- Regional study of internet safety, spam, privacy and security laws
- Conducted in late 2005; currently being updated
- 13 jurisdictions in the Asia Pacific region

Australia	Japan	South Korea
China	Malaysia	Taiwan
Hong Kong	New Zealand	Thailand
India	The Philippines	
Indonesia	Singapore	

- Also of note: Bangladesh, Sri Lanka and Pakistan have all recently enacted cybercrime bills – none of which have been analysed as part of this study.

Microsoft

Relevant Titles of the Convention

- **Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems**
  - ⇒ Illegal access
  - ⇒ Illegal interception
  - ⇒ Data interference
  - ⇒ System interference
  - ⇒ Misuse of devices

Microsoft

Relevant Titles of the Convention

- **Title 2 – Computer-related offences**
  - ⇒ Computer-related forgery
  - ⇒ Computer-related fraud
- **Title 5 – Ancillary liability and sanctions**
  - ⇒ Attempt and aiding or abetting
  - ⇒ Corporate liability

Microsoft

Enacted legislation: Alignment of cybercrime laws with Titles 1, 2 and 5 of the Convention

Moderate-strong alignment	Moderate-weak alignment	Weak alignment
Australia	China	India
Hong Kong	Japan	Indonesia
New Zealand	Malaysia	The Philippines
Singapore	South Korea	Thailand
Taiwan		

In terms of the countries with strong to moderate alignment:

- A common weakness involves the implementation of misuse of device offence;
- In some cases, the scope of legislation exceeds the Convention in terms of "mental element" and breadth of offenses targeted;
- These countries are the "low hanging fruit" in terms of becoming a party to the Convention.

Microsoft

Enacted legislation: Moderate-weak Alignment to the Convention

- China
- Malaysia
- South Korea
- Japan
- Where criminal offences exist in current domestic legislation, they are applied more narrowly;
- While Japan was a co-drafter and is a signatory of the Cybercrime Convention, the implementing legislation appears to be stalled in the Diet.
- India's Information Technology Act takes a civil liability approach.

Microsoft

Recently Enacted Legislation: Thailand

- Thailand Computer Offenses Act was passed by the Thai National Legislative Assembly in May, 2007 by a vote of 119 to 1. It apparently:
  - ⇒ Aims to prevent the disabling of computer systems, unauthorised access to computer systems as well as destruction of third party data;
  - ⇒ Establishes a number of criminal offences for input of false or forged data, input of data that threatens the country's security, is obscene or a terrorism offence;
  - ⇒ Makes it a criminal offence to falsify, hide or forge internet protocol addresses;
  - ⇒ Places severe restrictions on ISPs with respect to handing over data to authorities and retaining data for longer periods of time;
  - ⇒ Given recent actions to block YouTube and other "sensitive sites", critics are concerned that this gives the Government more censorship powers.

Microsoft

Pending legislation - Alignment of cybercrime laws with Titles 1, 2 and 5 of the Convention

As at December 2005

Strong alignment	Moderate alignment	Weak alignment
The Philippines	India	Indonesia
	Thailand	

Subsequent developments:

- **India**'s Information Technology Act, 2005 has been superseded by the Information Technology (Amendment) Bill of 2006. The IT Amendments Act contains some offences that correspond to some of the computer-related and ancillary offences.
- **Indonesia**'s **P**arliament is considering the Bill on Electronic Information and Transaction. There have been recent calls high level Indonesian officials that current laws are inadequate and that the Convention should be considered.
- **Sri Lanka** has enacted its first cybercrime law, the Computer Crimes Act.

Microsoft

Concluding remarks

- The Convention on Cybercrime has clearly influenced both enacted and pending cybercrime laws in the Asia Pacific region but there is clearly more work to be done;
- There exists significant variation in the extent to which Titles 1, 2 and 5 of the Convention have been implemented in the region;
- While there is growing awareness of the need to enact stronger cybercrime laws, to achieve Asia Pacific commitment to the Convention, countries will need to understand the benefits of accession;
- The time is right for the upcoming legislative workshop in Vietnam – particularly for drafting assistance and guidance for developing nations;
- Targeted bilateral and multilateral outreach to Governments that already have closely aligned laws – AU, NZ, HK, Chinese Taipei and Singapore – should be a priority.

Microsoft