Your potential. Our passion.™

Microsoft®

Asia Pacific Legislative Analysis:

Current and Pending Online Safety and Cybercrime Laws. A Study by Microsoft.

Table of Contents

Legislative Gap Analysis Internet on Safety, Security and Privacy

1. Asia Pacific Regional Overview

The extent and nature of internet safety, security and privacy legislation in the Asia Pacific region varies widely. The purpose of this regional overview is to provide readers with a high-level snapshot of the status of computer security, privacy, spam and online child safety legislation in the Asia Pacific region. Separate detailed analyses of these laws have been prepared for each of the following countries:

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

For more detail on the internet safety, security and privacy legislative framework in a particular jurisdiction, or a more detailed analysis of how a jurisdiction's laws compare to the benchmark legislation, please see the legislative gap analysis that is specific to that jurisdiction.

The Benchmark Legislation

One of Microsoft's objectives in carrying out this regional study was to gain an understanding of how the laws of different jurisdictions compared against a single benchmark. In some areas of Microsoft's study, such as computer security laws and online child safety laws, there exist international norms on the best approach to regulation. For example, the Council of Europe's Convention on Cybercrime is widely regarded as the international norm on the criminalisation of computer-related conduct, and the International Centre for Missing and Exploited Children (ICMEC) has developed authoritative model legislation that criminalises the production of, and certain dealings with, child pornography. In deference to the normative status of these instruments, Microsoft has adopted them as the benchmark legislation for the computer security and online child safety portions of its analysis.

However, for the other areas of Microsoft's study, namely, privacy laws and spam laws, there are no analogous international norms. In the privacy arena, there are numerous regional norms, such as the APEC Privacy Framework and the European Union's Data Protection Directive, but an international consensus on the best approach to data protection regulation has not yet been reached. The absence of an international norm on the regulation of spam-related activities can be explained by the recent nature of this phenomenon. Thus, without the benefit of any international norms in the privacy and spam areas, Microsoft has prepared its own legislation (in the case of privacy) and list of features (in the case of spam) upon which to benchmark each jurisdiction's laws. These benchmarks reflect Microsoft's experience as to what constitutes effective privacy and spam legislation, and its long-standing view that existing and pending laws should be harmonised wherever possible.

Computer Security Laws

BENCHMARK LEGISLATION

Titles 1, 2 and 5 of the Council of Europe's Convention on Cybercrime serve as the benchmark legislation for this part of the analysis.[1] As mentioned previously, the Convention on Cybercrime is widely recognised as an international norm on the criminalisation of computer-related conduct, having been widely adopted by European States and signed by several non-European States, including the United States, Canada, Japan and South Africa.

Title 1 of the Convention contains a number of "core offences" that criminalise unauthorised access to, and illicit tampering with, systems, programs or data.[2] In particular, Title 1 obliges Member States to enact illegal access, illegal interception, data interference, system interference and misuse of device offences.

Title 2 of the Convention, on the other hand, criminalises the computer-facilitated commission of fraud and forgery. Title 5 provides for ancillary liability for those that assist in the commission of the core and computer-related offences discussed above.

DISCUSSION OF THE LEGISLATIVE STATUS IN THE REGION

Enacted legislation

Favourable alignment	Moderate alignment	Weak alignment
Australia	China	India
New Zealand	Hong Kong	Indonesia*
Singapore	Japan	
Taiwan	Malaysia	
Thailand	The Philippines	
	South Korea	
	Vietnam	

*No computer security laws have been enacted.

The Australian, New Zealand, Singaporean, Taiwanese and Thai governments have each enacted robust computer security laws that cover most of the core and computer-related offences found in the Council of Europe's Convention on Cybercrime.

The computer security laws in China, Hong Kong, Japan and South Korea are moderately aligned with the Convention. This degree of alignment is variously due to the range of Convention

1. Title 3 of the Convention requires signatories to criminalise certain types of computer-facilitated dealing in child pornography; these offences are addressed in section 5 (Online Child Safety Laws) of this overview. Title 4 of the Convention requires signatories to criminalise certain types of intellectual property infringement; these offences are beyond the scope of this overview. **2.** Convention on Cybercrime (ETS No. 185) Explanatory Report.

offences covered by the enacted legislation and the restrictive way in which some of the Convention offences are implemented (e.g. requiring that unauthorised access be obtained by use of a telecommunications line). In the case of Hong Kong, although its general criminal law appears to apply in many cases to computer-facilitated conduct of the kind criminalised by the Convention on Cybercrime, Hong Kong has enacted fewer offences that specifically relate to computer security, which is one of the ends to which the Convention is directed.

The enacted laws in Malaysia, the Philippines and Vietnam are moderately to weakly aligned with the Convention. Although Malaysia and the Philippines have enacted some computer security offences, the focus of these offences appears to be on unauthorised access and these countries still rely on their general law to criminalise a number of the acts prohibited by the Convention. Vietnam's implementation of the Convention's core, and computer-related fraud and forgery, offences appears to be piecemeal and arises from the enactment of multiple, overlapping prohibitions in various instruments, including the Law on Information Technology 2006 and the Law on E-Transactions 2005.

Although India's Information Technology Act, 2000 (IT Act) prohibits many of the activities that constitute core offences under the Convention, the IT Act does not, for the most part, criminalise these activities – it merely provides for significant liability in damages. This civil liability approach is unique in the region.

In the absence of comprehensive computer security laws, jurisdictions such as Indonesia rely on the application of their existing laws to regulate acts of the kind criminalised by the Convention.

Pending legislation

Legislatures in Indonesia, India and the Philippines are currently considering comprehensive computer security laws. Of these instruments, the Philippines' proposed Cybercrime Prevention Act of 2005 (HB 3777) appears to be the most closely aligned with the Convention on Cybercrime; indeed, the proposed Philippine Act almost identically reproduces the Convention's core offences, computer-related fraud and forgery offences, and ancillary liability provisions.

India's Information Technology (Amendment) Bill 2006 (IT Amendment Bill) proposes to amend the IT Act to criminalise many of the acts that constitute core offences under the Convention but only where they are done "dishonestly or fraudulently." In September 2007, the Standing Committee on IT submitted its report on the IT Amendment Bill, which makes a number of substantive recommendations in respect of the bill. It is expected that some of these recommendations will be implemented in a revised bill that will be resubmitted to parliament not earlier than November 2007.

Indonesia's Bill on Electronic Information and Transaction is only moderately to weakly aligned with the Convention, in part due to its emphasis on unauthorised access and the protection of government and financial computer systems.

Japan and China have also been considering updated cybercrime laws for some time now. A modest amendment to the Criminal Code to criminalise the preparation, production, dissemination and use of computer viruses and malware has been pending in the Japanese parliament (the Diet) since 2004, along with a separate piece of legislation that seeks to implement Japan's remaining obligations as a signatory to the Convention on Cybercrime. It is understood that China is continuing to draft its National Information Security Regulations, however, neither the content of these regulations, nor the timeframe for their enactment, is known.

Privacy Laws

Benchmark legislation

The Microsoft-drafted Model Privacy Bill serves as the benchmark legislation for this part of the analysis. The Model Bill applies to private sector organisations that collect, store, use or disclose personally identifiable information of more than 5,000 individuals. Regulated organisations must make available a privacy notice prior to collection of personally identifiable information, and in order to be entitled to use or disclose it for a secondary purpose, the regulated organisation must obtain the consent of the data subject (either explicit, opt-out or implied – depending on several factors related to the privacy risk involved). There are several protected disclosures to which the Model Bill's provisions relating to use and disclosure of personally identifiable information do not apply, including where the disclosure is made to service providers and related companies that operate under a common set of internal policies. The Model Bill also contains access and correction, and security-related, provisions, including a breach notification obligation, which is triggered when a security breach results in (or it is reasonably possible that a breach will result in) the misuse of a resident's unencrypted sensitive financial information.

The Model Bill contemplates government-led enforcement, pursuant to which government agencies can recover civil penalties or capped statutory damages.

DISCUSSION OF THE LEGISLATIVE STATUS IN THE REGION

Enacted legislation

Favourable alignment	Moderate alignment	Weak alignment
	Australia	India*
	Hong Kong	Indonesia*
	Japan	Malaysia
	New Zealand	The Philippines
		Singapore*
		South Korea
		Taiwan
		Thailand
		Vietnam

*No data protection laws have been enacted.

Based on the OECD Guidelines on the Protection of Privacy and Transborder Flows, the data protection laws in Australia, Hong Kong and New Zealand are moderately to favourably aligned with the benchmark legislation. The strengths of these regimes vis-à-vis the Model Bill include their broad application to the private sector and their notice, security and access provisions. One aspect of the Model Bill that these regimes have not adopted in full is a tiered consent model that takes account of the privacy risk inherent in secondary use or transfer (i.e. a model that imposes more onerous consent requirements where the associated privacy risk is greater). Furthermore, the imposition of restrictions on transborder data flows in Australia and Hong Kong are departures from the Model Privacy Bill.

Considered on its own, Japan's Act Concerning the Protection of Personal Information appears to be moderately aligned with the benchmark legislation. However, it is possible that the sectoral guidelines that explain the application of the Protection of Personal Information in certain industry sectors may alter this analysis.

South Korea's data protection regime also draws guidance from the OECD Guidelines, but it is less well-aligned with the benchmark legislation. South Korea's alignment with the Model Privacy Bill is affected by a combination of restrictive provisions in the legislation, such as requiring a data subject's consent for transborder data flows within a corporate group, and the way in which the legislation has been interpreted and enforced by the Korea Information and Security Agency (KISA).

Taiwan's Computer-Processed Personal Data Protection Law only applies to certain industries in the private sector. The Law is unique in the region insofar as it establishes a mandatory licensing regime for those regulated entities that collect, use or disclose personal data.

There is no private sector data protection legislation in Thailand. However, the Official Information Act 1997 regulates state agencies in their dealings with personal information.

Although there do not appear to be any comprehensive data protection laws of general application in Vietnam, the Law on Information Technology 2006 contains a limited data protection regime that applies to the collection, use and disclosure of personal information in a networked environment. The E-Transactions Law contains similar provisions that address how to handle personal information collected as part of an electronic transaction.

The Philippine Department of Trade and Industry has recently promulgated an administrative order that contains guidelines for the protection of personal data held by private sector organisations. These voluntary guidelines are a measure of a different kind to the Model Bill; they are aimed at encouraging private sector organisations to adopt privacy policies rather than penalising them for not doing so.

Similarly, in Malaysia there is no comprehensive data protection legislation, but the (generally voluntary) General Consumer Code developed pursuant to the Communications and Multimedia Act 1998 contains provisions that relate to the protection of personal information collected by licensed telecommunications service providers.

China, India, Indonesia and Singapore have not enacted data protection legislation.

Pending legislation

China, India, Indonesia, Malaysia, South Korea, Taiwan and Thailand are currently considering data protection legislation. An impetus for reform in this area has been the endorsement of the APEC Privacy Framework in 2005 and more recent efforts to implement the framework in the region.

If enacted, the Taiwanese legislative proposal would bring that country's existing regime more into line with the ideal advocated by the benchmark legislation. The position in South Korea is less clear; at the date of writing, it is understood that the government is planning to consolidate three of the private sector instruments that were previously vying for enactment into a single bill.

The Indonesian and Indian data protection proposals are minor parts of pending cybercrime legislation and could benefit from further consideration. In that vein, India's Standing Committee on IT recommended in September 2007 that India enact a more comprehensive data protection regime as part of the proposed amendments to the IT Act discussed in the computer security section previously.

1. Asia Pacific Regional Overview

Malaysia, Thailand and China have been considering data protection legislation for some time. The most recent publicly available draft of the Malaysian legislation contemplated a model similar to Hong Kong's Personal Data Privacy Ordinance, which would stand the pending legislation in good stead vis-à-vis the Model Privacy Bill. However, it is understood that a further draft of Malaysia's data protection legislation has been prepared since then. The Thai government is presently considering ways to further align its proposed legislation with the APEC Privacy Framework, and China's State Council Informatization Office (SCITO) is in discussions with data protection experts on the content of the proposed legislation, which it is expected will be placed on the National People's Congress legislative agenda in 2008.

At the date of writing, there were also proposals in Australia, New Zealand and Hong Kong to refine the operation of their privacy laws. Australia's Law Reform Commission released a discussion paper in September 2007, which canvassed a range of proposals for improving Australia's privacy laws, including the introduction of a breach notification obligation and a statutory cause of action for invasion of privacy. It is not known if or when these proposals will be implemented by the Australian government. In addition, a number of minor pieces of privacy-related legislation were under consideration in Australia at the date of writing, and the Standing Committee of Attorneys-General has released a consultation paper on workplace privacy. Finally, the Federal Privacy Commissioner is considering two further privacy codes under the Privacy Act: the Internet Industry Privacy Code and the Australian Casino Association Privacy Code.

New Zealand's Privacy Commissioner proposed draft breach notification guidelines in August 2007. These voluntary guidelines are expected to be finalised in late 2007 or early 2008 after the Commissioner considers the public comment that she has received on the draft guidelines.

Hong Kong's Privacy Commissioner has also announced that he plans to amend the Code of Practice on Consumer Credit Data to better address how positive credit data is being used by credit providers and to redress some operational difficulties that exist in enforcing the Code.

It is understood that the Japanese government has plans to gather research and conduct consultations on Japan's personal information laws with the possibility of considering full-scale amendments in 2009.

Spam Laws

BENCHMARK LEGISLATION

The Microsoft-drafted checklist of features of effective anti-spam legislation serves as the benchmark legislation for this part of the analysis. The checklist contemplates an 'opt-out' anti-spam regime that covers all manner of commercial electronic messages. However, the checklist provides that transactional or relationship messages – such as messages sent to customers in relation to products or services that they have purchased from the sender – should be excluded from the scope of regulation, as should messages that only have an incidental commercial purpose. The checklist contains the usual prohibitions on transmitting commercial electronic messages without an unsubscribe facility or accurate sender and header information, and provides that customers should be able to opt-out from the receipt of commercial electronic messages on a product-line basis as well as on a company-wide basis. The checklist does not contemplate any 'ADV' or other labelling requirement. Effective anti-spam legislation should also include strong anti-address harvesting and dictionary attack measures, as well as service provider liability provisions that preserve the right of ISPs and email service providers to combat spam.

On the enforcement front, the checklist contemplates enforcement by ISPs, email service providers and the government. The available remedies should include: (i) civil liability in damages; (ii) capped statutory damages that may be adjusted to take into account willful violations and implementation of best practice procedures, and (iii) criminal sanctions for intentional and unauthorised acts, including those involving fraud.

DISCUSSION OF LEGISLATIVE STATUS IN THE REGION

Enacted legislation

Favourable alignment	Moderate alignment	Weak alignment
Hong Kong	Australia	India*
	China	Indonesia*
	New Zealand	Malaysia*
	Singapore	The Philippines
	South Korea	Taiwan*
		Thailand
		Vietnam

(Please note that an English translation of the anti-spam legislation enacted in Japan was not available at the time of writing and so a benchmark analysis of that legislation has not been conducted.)

*No spam laws have been enacted.

In recent times, there has been a discernible move in the Asia Pacific region toward the enactment of anti-spam legislation. There are now seven countries in the Asia Pacific region that have enacted comprehensive anti-spam legislation: Australia, China, Hong Kong, Japan, New Zealand, Singapore and South Korea. Of these seven countries, Hong Kong's opt-out regime appears to be the most closely aligned with the checklist, with Australia and New Zealand being positioned not too far behind despite implementing opt-in models. Singapore has enacted an opt-out regime with "bulk" and labelling requirements, while the requirements of South Korea's regime vary depending on the medium by which the advertising is transmitted. China's Internet Email Service Management Regulations 2006 are moderately to weakly aligned with the checklist due in part to their application only to emails and their 'AD' labelling requirement. Hong Kong and New Zealand are currently the only jurisdictions in the region that explicitly exclude transactional or relationship messages from the scope of regulation.

Less comprehensive anti-spam measures have been enacted in the Philippines, Thailand and Vietnam. The broadcast messaging rules implemented in the Philippines appear to be an interim measure designed to address a particular area of concern, namely, spam SMS and MMS, pending the development of a more comprehensive regime. Thailand's spam-related provisions were enacted as part of its 2007 computer security legislation, and are likely to be of limited application to spam that is not fraudulent or designed to interfere with the operation of the recipient's computer system. There are two sources of spam-related obligations in Vietnam: the Law on Information Technology 2006, and Decree 142 Specifying Administrative Penalties in the Field of Post, Telecommunications and Radio Frequency. These instruments apply to "advertisement information" transmitted over networks and "unsolicited messages" (respectively), but neither instrument establishes a comprehensive spam regime.

In the absence of specific anti-spam legislation, jurisdictions such as India, Indonesia, Malaysia, and Taiwan rely on their existing computer security and/or consumer protection laws to regulate spam activity. While this approach goes some way toward alleviating the consequences of spam activity, it is increasingly being accepted by legislatures in the region that specific anti-spam legislation is necessary to reduce spam volumes.

Pending legislation

Legislatures in India, Indonesia, the Philippines and Taiwan are currently considering anti-spam legislative proposals. Of these proposals, Taiwan's 'opt-out' legislation appears to be the most advanced in the legislative process, as well as being the most closely aligned with the checklist. Vietnam's inter-agency taskforce is at the earlier stage of drafting a decree on spam, and it has been reported that a draft of the decree could be submitted to the government in late 2007.

The pending computer security laws in India, Indonesia and the Philippines contain spam-related provisions. If enacted in their current form, the spam-related provisions in India's IT Amendment Bill will apply only to certain limited types of spam, and not mere unsolicited commercial electronic messages. In its report on the IT Amendment Bill, the Standing Committee on IT questioned whether these provisions constituted a sufficient response to the problem of spam, and recommended that India enact specific anti-spam legislation.

Indonesia's Electronic Information and Transaction Bill (EIT Bill) does not propose to regulate spam messages per se. Instead, the EIT Bill proposes to require persons who offer to sell goods and services offered through electronic media to provide complete and correct information in relation to the terms of the contract, the good or service offered and the producer of the good or service. The spam-related provisions in the Philippines' Cybercrime Prevention Act of 2005 (HB 3777) propose to establish a basic opt-out regime. There are also plans to amend Japan's Law Regarding the Regulation of Transmission of Specific E-mail. It is understood that the Ministry of Internal Affairs and Communications is planning to submit a bill to the Diet in 2008 which is expected to create an opt-in regime for spam emails accessed from computers and mobile phones.

Malaysia and China may also enact anti-spam laws in the future. In August 2007, the Malaysian Communications and Multimedia Commission announced that it had issued a tender for the provision of consultancy services for studying legislative responses and drafting anti-spam legislation for Malaysia. As for China, it is understood that the Internet Society of China, with the support of the Ministry of Information Industry, is continuing to conduct research on different approaches to comprehensive spam legislation.

Draft codes of practice are under consideration in both Hong Kong and New Zealand. These codes of practice are expected to provide regulated entities with further guidance on how to comply with the comprehensive anti-spam regimes that have recently been enacted in Hong Kong and New Zealand.

1. Asia Pacific Regional Overview

Online Child Safety Laws

BENCHMARK LEGISLATION

A combination of the child pornography offences in Title 3 of the Convention on Cybercrime and the core elements of ICMEC's[3] model child pornography legislation serve as the benchmark instrument for this part of the analysis. The child pornography offences in Title 3 of the Convention of Cybercrime aim to circumscribe the use of computer systems in the commission of sexual offences against children.[4] As such, the Convention requires signatories to criminalise acts such as the production of child pornography for the purpose of its distribution through a computer system, and offering, making available, distributing or transmitting child pornography through a computer system. Possessing child pornography in a computer system is also subject to criminalisation.

In ICMEC's view, effective child pornography legislation must specifically apply to child pornography and not just pornography in general. Accordingly, the legislation must include a definition of child pornography (where a child is a person under the age of 18 irrespective of the age of consent to sexual relations). Effective child pornography, legislation should also expressly criminalise the possession of child pornography regardless of the intent to distribute, and require ISPs to report suspected child pornography to relevant authorities.

DISCUSSION OF THE LEGISLATIVE STATUS IN THE REGION

Enacted legislation

Favourable alignment	Moderate alignment	Weak alignment
Australia	Hong Kong	India*
	Japan	Indonesia*
	South Korea	Malaysia*
	Taiwan	New Zealand
		The Philippines*
		Singapore*
		Thailand
		Vietnam*

(Please note that an English translation of the online child safety legislation enacted in China was not available at the time of writing and so a benchmark analysis of that legislation has not been conducted)

*No online child safety laws have been enacted.

Of all the areas of law considered by this regional overview, online child safety laws are the least developed in the region vis-à-vis the benchmark legislation. Although most countries have enacted broad obscenity regimes that have some application to online dealing in child pornography, only five of the fourteen jurisdictions – Australia, Hong Kong, Japan, South Korea and Taiwan – have enacted legislation that specifically addresses child pornography, and three of the fourteen jurisdictions – Australia, Hong Kong and Taiwan – have enacted legislation that contains computer-facilitated child pornography offences.

The specific child pornography legislation that has been enacted in the region generally adheres to the applicable ICMEC principles, although only Australia and Hong Kong criminalise the mere possession of child pornography (i.e. possession, irrespective of the intent to distribute). The computer-facilitated child pornography offences enacted in Australia, Hong Kong and Taiwan cover most of the prohibited acts under Title 3 of the Convention; Australia is the only jurisdiction in the region to impose an obligation on ISPs and content hosts to report material that they reasonably believe to be child pornography material (a similar provision exists in US law).

Although New Zealand has not enacted specific legislation to combat child pornography, case law has confirmed that New Zealand's classification regime does apply to child pornography, and certain of the offences under that regime attract more serious sanctions where the offending publication promotes the sexual exploitation of children, among other things. The recent Thai Computer Crime Act criminalises certain computer-facilitated dealings with pornography, but it does not specifically refer to child pornography.

India, Indonesia, Malaysia, the Philippines, Singapore and Vietnam do not have legislation that specifically addresses child pornography. However, the absence of specific child pornography legislation in some of these countries needs to be understood in the context of those countries' approach to content control. In several Asia Pacific jurisdictions, including Malaysia, Singapore and Vietnam, primary responsibility for content control lies with ISPs and content hosts (or in the case of Vietnam, the State, society and schools), and as such, it is these entities that will be held responsible if obscene material is made available using their services or to children for whom they are responsible. While this approach to content control does not oust the need for specific child pornography legislation, it does serve to reduce the availability of child pornography online which is one of the ends to which specific child pornography legislation is directed.

Pending legislation

The Philippine, Indian, Indonesian and Japanese legislatures are currently considering online child safety laws. Most of these pending laws are part of broader proposals to enact computer security laws; only the Philippine legislation specifically applies to child pornography (as opposed to pornography at large). However, the Indian Standing Committee on IT has recommended that the Indian

3. International Centre for Missing and Exploited Children. **4.** Convention on Cybercrime (ETS No. 185) Explanatory Report.

government revise the IT Amendment Bill to criminalise computer-facilitated dealings with child pornography in accordance with the Convention on Cybercrime.

The enactment of the computer-facilitated child pornography offences in the Philippines' Cybercrime Prevention Act would be a welcome development; these offences and the accompanying definitions are taken directly from Title 3 of the Convention on Cybercrime. The Indonesian proposals to enact computer-facilitated pornography offences are less comprehensive than the Philippine proposal and could benefit from further refinement to bring them more into line with the benchmark legislation.

Japan's pending computer security legislation contains offences relating to the possession and distribution of obscene electronic records. It is also understood that the Japanese government has plans to amend the Law for Punishing Acts Related to Child Prostitution and Child Pornography, and for Protecting Children, although the details of the planned amendments are not available at the date of writing.

In 2005, Thailand was considering amendments to its existing online child safety laws, specifically in the area of child pornography. At the date of writing, it is not known if or when this legislative proposal will proceed to enactment.

2. Australia

Part 1 – Snapshot of Legislative Status

Key: (E) Enacted
(P) Pending
(Title [x] COE) Title [x] of the Council of Europe Convention on Cybercrime (COE)

(ACT) Australian Capital Territory
(Cth) Commonwealth of Australia
(NSW) State of New South Wales
(NT) Northern Territory
(Qld) State of Queensland
(SA) State of South Australia
(Tas) State of Tasmania
(Vic) State of Victoria
(WA) State of Western Australia

Area	Topic	Enacted legislation	Pending legislation	Relevant instruments/Comments
Computer Security Laws	**Core offences (Title 1 COE):** illegal access, illegal interception, data interference, system interference, misuse of devices	✓	✓	**Federal:** Criminal Code Act 1995 (Cth) (E); Crimes Act 1914 (Cth) (E); Telecommunications (Interception and Access) Act 1979 (Cth) (E) **State and territory:** Criminal Code Act 2002 (ACT) (E); Crimes Act 1900 (NSW) (E); Criminal Code Act 1983 (NT) (E); Criminal Code Act 1899 (Qld) (E); Criminal Law Consolidation Act 1935 (SA) (E); Criminal Code Act 1924 (Tas) (E); Crimes Act 1958 (Vic) (E); Criminal Code Act Compilation Act 1913 (WA) (E)
	Computer-related offences (Title 2 COE): computer-related forgery, computer-related fraud	✓	✗	
	Ancillary-liability (Title 5 COE): attempt and aiding/ abetting, corporate liability	✓	✗	
Privacy Laws	**Data protection**	✓	✓	**Federal:** Privacy Act 1988 (Cth) (E); Privacy (Data Security Breach Notification) Amendment Bill 2007 (Cth) (P) **State and territory:** Privacy and Personal Information Act 1998 (NSW) (E); Personal Information Protection Act 2004 (Tas) (E); Information Privacy Act 2000 (Vic) (E); Information Act 2002 (NT) (E); Information Privacy Bill 2007 (WA) (P)
	Surveillance (see illegal interception under computer security)	✓	✗	**Federal:** Telecommunications (Interception and Access) Act 1979 (Cth) (E) **State and territory:** Listening Devices Act 1984 (NSW) (E); Surveillance Devices Act 1999 (Vic) (E); Invasion of Privacy Act 1971 (Qld) (E); Surveillance Devices Act 1998 (WA) (E); Listening and Surveillance Devices Act 1972 (SA) (E); Listening Devices Act 1991 (Tas) (E); Surveillance Devices Act 2000 (NT) (E); Listening Devices Act 1992 (ACT) (E); Workplace Surveillance Act 2005 (NSW) (E)
	Sensitive information	✓	✗	**Federal:** Privacy Act 1988 (Cth) (E); Health Records and Information Privacy Act 2002 (NSW) (E); Health Records Act 2001 (Vic) (E); Health Records (Privacy and Access) Act 1997 (ACT) (E)
Spam Laws	**Anti-spam regulation**	✓	✗	**Federal:** Spam Act 2003 (Cth) (E)
Online Child Safety Laws	**General child pornography offences**	✓	✗	**State and territory:** Crimes Act 1900 (ACT) (E); Crimes Act 1900 (NSW) (E); Criminal Code Act 1983 (NT) (E); Criminal Code Act 1899 (Qld) (E); Criminal Law Consolidation Act 1935 (SA) (E); Criminal Code Act 1924 (Tas) (E); Crimes Act 1958 (Vic) (E); Censorship Act 1996 (WA) (E)
	Computer-facilitated child pornography offences (Title 3 COE)	✓	✗	**Federal:** Criminal Code Act 1995 (Cth) (E) **State and territory:** Criminal Code Act 1899 (Qld) (E); Criminal Law Consolidation Act 1935 (SA) (E); Classification (Publications, Films and Computer Games) Enforcement Act 1996 (WA) (E); Criminal Code Act 1913 (WA) (E)

Part 2 – Legal and Regulatory Position

The Commonwealth of Australia is made up of six states (New South Wales, Queensland, South Australia, Tasmania, Victoria and Western Australia) and two self-governing territories (Australian Capital Territory and the Northern Territory). Accordingly, Australia has a federal system similar in many ways to that found in the USA. Most criminal offences are against state laws for acts that take place within the boundaries of the state. Federal laws generally have an international or interstate element or concern special federal issues, such as telecommunications (e.g. interception laws) or intellectual property (e.g. trade in counterfeit goods).

2.1 COMPUTER SECURITY LAWS – CURRENT LEGISLATIVE FRAMEWORK

Federal legislation

In 2001, the federal government amended the Criminal Code Act 1995 (Code) to introduce a range of computer security offences based on Chapter 4 of Australia's Model Criminal Code. Although this regime is broadly equivalent to that found in the Convention on Cybercrime, its application is narrower: for constitutional reasons, the Code's offences only apply in respect of data held by, or on behalf of, the federal government or in relation to acts undertaken by means of a telecommunications service.

State and territory legislation

New South Wales, Victoria, South Australia and the two territories (Australian Capital Territory and the Northern Territory) have implemented the Model Criminal Code and thereby established computer security regimes that are materially similar to their federal counterpart. The Queensland, Tasmanian and Western Australian regimes are less aligned with the Model Criminal Code; they appear to focus on computer hacking and misuse offences. Importantly, all state and territory computer security offences apply generally in the jurisdiction to which they pertain and thereby regulate conduct that falls outside the federal legislation for constitutional reasons.

For brevity, only the federal regime will be discussed below.

Core offences (Title 1 COE): Illegal access, illegal interception, data interference, system interference, misuse of devices

The Code's unauthorised access offence only applies in respect of data that is protected by an access control system (this qualification is permitted by the Convention). The Code's data interference offence is likely to regulate a broader range of conduct than its Convention counterpart due to its application to reckless data interference as well as that caused intentionally.

The act of illegally intercepting communications is not regulated by the Code, although dealing in and possessing interception devices is. See more in section 2.3 for separate federal, state and territory interception legislation.

The Code does not contain an equivalent to the Convention's system interference offence, but its unauthorised impairment of electronic communications offence is targeted at denial of service attacks in the same way that the Convention system interference offence is (at least in part). Similarly, the Code's offences in respect of producing, supplying, possessing or procuring data (which is defined as including computer programs) with intent to commit a computer security offence, are best viewed as a partial implementation of the Convention's misuse of devices offence.

Contraventions of the Code attract terms of imprisonment ranging from 2 to 10 years depending on the seriousness of the offence. Where unauthorised access or data interference is preparatory to the commission of another offence under the Criminal Code, offenders face the penalty associated with the latter offence.

Computer-related offences (Title 2 COE): Computer-related forgery, computer-related fraud

Although the Criminal Code does not contain a specific computer-related forgery offence, its general forgery offences in Part 7.7 of the Code are likely to cover the same conduct. This is principally because "document" is defined in section 143.1 of the Code to include material capable of being responded to by a computer, machine or electronic device, or from which information can be reproduced.

Similarly, the Code's general fraud offences are capable of regulating computer-related fraud; "deception" is defined to include conduct by a person that causes a computer, a machine or an electronic device to make a response that the person is not authorised to cause it to do.

Those who offend the Code's forgery and fraud offences are liable to imprisonment for up to 10 years. These provisions, along with the Code's financial information offences, are likely to assist with the prosecution of credit card and phishing schemes.

Ancillary liability (Title 5 COE): Attempt and aiding/abetting, corporate liability

Generally it is an offence to attempt, aid or abet the commission of each of the above computer security offences. However, there is no accessorial liability for producing, supplying, possessing or procuring data with intent to commit a computer security offence, or in respect of the offence of unauthorised access or data interference that is preparatory to the commission of another offence under the Code.

The Code also addresses corporate criminal liability. In most cases, corporate criminal liability is established by attributing an offence's fault element to the body corporate where the body corporate

can be said to have expressly, tacitly or impliedly authorised the commission of the offence. Bodies corporate can face fines of up to five times the amount that can be imposed on an individual for the same offence.

2.2 COMPUTER SECURITY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

The Model Criminal Law Officers Committee (MCLOC) is currently preparing a final report in which it is expected to propose that all Australian jurisdictions, including the Commonwealth, enact model identity crime offences. It is likely that the model offences will prohibit: (i) identity theft; (ii) identity fraud; (iii) on-selling identity information; and (iv) possessing equipment to manufacture identification information where the offender is reckless with respect to the information being used for an unlawful purpose. It is unclear to what extent any proposed changes will be adopted in the federal Criminal Code and state and territory criminal legislation.

2.3 PRIVACY LAWS – CURRENT LEGISLATIVE FRAMEWORK

Data protection

Federal legislation

The federal Privacy Act 1988 establishes a data protection regime for both the private and federal public sectors in Australia. The regimes apply in respect of dealings with "personal information" – information or an opinion, whether true or not and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Private sector regime

The private sector regime requires "organisations" to comply with either the Act's National Privacy Principles or an approved privacy code in their dealings with the personal information of Australian citizens and residents. An "organisation" can be an individual, body corporate, an unincorporated association or a trust, although small business operators – typically those with an annual turnover of less than AUD$3 million (approximately USD$2.5 million) – are exempt from the regime unless they trade in personal information or hold health information. So too are certain acts and practices by organisations that are otherwise regulated by the regime, including maintaining employee records in respect of current and previous employment relationships, and acts or practices conducted by a media organisation "in the course of journalism."

In the absence of an approved privacy code, organisations subject to the private sector regime are obliged to adhere to the National Privacy Principles (NPPs), which are based on the OECD guidelines with some modifications. The NPPs regulate: (i) the way in which information is collected, used, disclosed and modified; (ii) data quality, security and anonymity; (iii) the use of identifiers; and (iv) transborder data flows. Generally, where an individual has given their consent that a particular action can be taken in relation to their personal information, the organisation is permitted to do the thing permitted by that consent.

At the date of writing, there are three approved privacy codes that replace the NPPs (and sometimes the Act's complaints regime) for those organisations bound by them: the Market and Social Research Privacy Code; the Biometrics Institute Privacy Code; and the Queensland Club Industry Privacy Code. Further, the most recent version of the ASIC-registered Electronic Funds Transfer Code requires subscribers to comply with the NPPs.

Enforcement of the Privacy Act is through the Act's complaints-based regime, although the Federal Court has jurisdiction to issue injunctions to restrain breaches. As a matter of practice, complaints which are not directly resolved between the individual and the regulated organisation are investigated and conciliated by the Office of the Federal Privacy Commissioner. The Commissioner has the power to make a formal determination that an organisation has interfered with the privacy of an individual. Following such a determination, the Commissioner can:

- require the organisation to pay compensation for any loss or damage suffered by the individual (including compensation for hurt feelings or humiliation);
- require the organisation to perform any reasonable act or course of conduct to redress the loss or damage suffered by the person concerned; or
- make a declaration that the organisation should not repeat or continue the offending conduct.

There is a complex and rarely invoked scheme for review of the Commissioner's decisions in the Federal Court or the Federal Magistrates Court.

Public sector regime

The federal Privacy Act 1988 regulates Commonwealth and Australian Capital Territory agencies in their dealings with personal information. The Act establishes 11 Information Privacy Principles (IPPs) that are materially similar to the NPPs discussed above. The public sector data protection regime is also enforced in the same way that the private sector regime is (see above), except that complaints are made to the agency concerned and there is a limited right of appeal to the Administrative Appeals Tribunal for a merits-based review of the Commissioner's decision.

State and territory legislation

New South Wales, Tasmania, Victoria and the Northern Territory have enacted public sector data protection legislation that variously implements the IPPs and the NPPs discussed earlier.

Although Queensland and South Australia have not enacted public sector data protection legislation, a public sector regime of sorts exists in these jurisdictions by virtue of administrative standards and Cabinet instructions respectively.

Surveillance

Federal legislation

At the federal level, the illegal interception of communications is addressed by the Telecommunications (Interception and Access) Act 1979. This Act prohibits both the interception of communications passing over a telecommunications system, and the use of intercepted communications, except in certain limited circumstances (for example, where interception is necessary for the detection of criminal activity and the Act's warrant scheme has been complied with). It is also an offence pursuant to the Telecommunications (Interception and Access) Act 1979 to authorise, suffer or permit another person to intercept a communication passing over a telecommunications system, or to enable them to do so. There are particular provisions addressing access to stored communications (e.g. email, voicemail, SMS) that differentiate between read and unread messages. Offenders are liable to imprisonment for up to 2 years.

State and territory legislation

Each of the states and territories has enacted its own legislation regulating the use of listening devices to record conversations outside the telecommunications system. Some jurisdictions (South Australia, Victoria, Western Australia and the Northern Territory) have enacted broader prohibitions on surveillance devices (video and tracking devices). These regimes all permit surveillance under warrant, but limit the other circumstances in which surveillance of private activities may occur.

In New South Wales, the Workplace Surveillance Act 2005 has been enacted to regulate camera, computer and tracking (location-based) surveillance of employees at work. The general position under the Act is that an employer may carry out, or cause someone else to carry out, surveillance of an employee if the surveillance is either (i) notified surveillance, or (ii) covert surveillance that is either (a) judicially-approved and necessary for the purpose of establishing whether an employee is involved in any unlawful activity or (b) notified to staff prior to its commencement and necessary for security reasons. Contravention of the Workplace Surveillance Act is a criminal offence, with the main offences resulting in fines of up to AUD$5,500 (approximately USD$6,420). Directors and senior managers of a company may be personally liable if they knowingly authorise or permit a contravention by their company.

Sensitive information

The federal Privacy Act 1998 affords special protection to "sensitive information" – information or an opinion about an individual's racial or ethnic origin, religious or political beliefs, professional or trade association membership, criminal, genetic and health information, among other things. National Privacy Principle 10 provides that an organisation must not collect sensitive information unless (i) the individual concerned has consented to its collection, (ii) collection is required by law or (iii) other special circumstances are present.

The Privacy Act also regulates the use of consumer credit information, and the use of tax file numbers – unique numbers issued by the Australian Taxation Office (ATO) to identify individuals and organisations who lodge income tax returns with the ATO.

The New South Wales, Victorian and Australian Capital Territory health sector-specific data protection legislation provides special protection to personal health information. This legislation applies to health entities in both the private and public sectors.

Anti-money laundering

The federal government has enacted anti-money laundering legislation to implement global anti-money laundering standards and attempt to counter terrorist financing. In part, the legislation regulates how the financial sector and the gambling industry, among others, can confirm the identity of their customers. The identity verification requirements are technology-neutral. Reporting obligations, including disclosing an individual's personal information, are imposed on a service provider regulated by the Act if a suspicious event occurs (e.g. if the provider suspects the customer is not who they claim to be).

Do Not Call Register

In 2006, the Do Not Call Register Act was passed by the federal government. The Act prohibits a telemarketing call from being made or caused to be made to an individual's home or mobile telephone number if it is listed on the Do Not Call Register. An exception to this is if the individual has consented, either expressly or through inference, to receiving the call. Telephone calls relating to product recalls, faults in goods or services, appointment rescheduling, appointment reminders or payment obligations are not considered telemarketing calls for the purposes of the Act.

2. Australia

2.4 PRIVACY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

Data protection

Federal legislation

In September 2007, the Australian Law Reform Commission (ALRC) released a discussion paper on Australia's privacy laws after having sought public comment on the efficacy of those laws during 2006. Some of the ALRC's key proposals for reform include:

- the creation of a statutory cause of action for invasion of privacy;
- the consolidation of the Information Privacy Principles and the National Privacy Principles (together, the Unified Privacy Principles or the "UPPs");
- the proposal that the Commonwealth seek to constitutionally exclude inconsistent state and territory privacy legislation affecting organisations;
- the proposal to confer regulation-making power on the Office of the Privacy Commissioner that would allow it to set standards that are higher or lower than the standards imposed by the UPPs in certain circumstances;
- the proposal that the Minister should have power to determine technology-specific standards for handling personal information;
- the proposal to widen the scope of the application of the Privacy Act by including email and IP addresses into the definitions of "personal information" and "record" in certain circumstances;
- new data breach notification provisions that would require organisations to notify affected individuals where there has been unauthorised access to personal information that could lead to a real risk of serious harm;
- removal of the small business and employee information exemptions; and
- new enforcement powers for the Privacy Commissioner, including the power to issue directions to organisations to take specified action within a specified time period.

The ALRC is also seeking feedback on:

- whether there should be a "take down notice" scheme that would require a website operator to remove information that may constitute an invasion of privacy (whether similar to, or an extension of, the co-regulatory online censorship scheme discussed in section 3.7 below);
- whether Voice Over Internet Protocol (VOIP) numbers should be covered by the Do Not Call Register Act 2006; and
- whether the Spam Act 2003 should also cover facsimile and Bluetooth messages.

Submissions on the ALRC discussion paper are due in December 2007 and a final report is expected to be released in March 2008. It is expected that this review will lead to amendments to the federal Privacy Act and possibly state and territory laws.

On a separate note, the Federal Privacy Commissioner's website reports that her office is currently considering two privacy codes: the Internet Industry Privacy Code; and the Australian Casino Association Privacy Code. No timeframe for approval of these codes is provided.

State and territory legislation

The Western Australian parliament is currently considering public sector data protection legislation.

Surveillance

In June 2007, the Standing Committee of Attorneys-General released a consultation paper on workplace privacy laws. The consultation paper canvassed five options for reform: do nothing; implement voluntary guidelines; implement a mandatory code of conduct; adopt a combination of approaches; or implement a legislative regime. Interested parties have made submissions on the consultation paper; at this stage, it is unclear when a final report will be released.

Miscellaneous

Australia's "Access Card" bill is currently before the federal parliament. It seeks to establish the framework for the Government to introduce a health and social services smartcard (the "Access Card"). If the bill proceeds to enactment, most individuals will need to obtain an Access Card in order to use health and social services, including publicly funded health care services. The card will contain basic personal information such as an individual's name, address, digitised photo and signature, gender, concession status and PIN. At this stage, the proposed Access Card will not contain an individual's medical records, tax file number or other financial information.

In August 2007, a private member's bill on the issue of reporting data security breaches was introduced into the Senate. This bill is not expected to proceed to enactment given that the sponsoring Senator has advised that she does not intend to recontest the next election, which is due to be called before the end of 2007.

2.5 SPAM LAWS – CURRENT LEGISLATIVE FRAMEWORK

Federal legislation

Australia's federal Spam Act 2003 establishes an 'opt-in' regime in respect of unsolicited commercial electronic messages that have an "Australian link". A message has an Australian link if it originates from, or is accessed in, Australia. The Act does not contain a bulk requirement and it regulates a broad range of messages: a commercial electronic message is essentially any electronic message where one of its purposes is to promote or offer to supply goods

or services. To avoid contravening the Act, senders of commercial electronic messages must (i) obtain the recipient's consent, (ii) provide accurate sender information and (iii) include a functional unsubscribe facility.

Recipients can either expressly consent to the receipt of commercial electronic messages, or their consent can be inferred from their conduct, and business and other relationships. While this concept of inferred consent provides some recognition of pre-existing business relationships, the Act's Explanatory Memorandum suggests that it will not always be possible to infer consent from a pre-existing business relationship between the sender and the recipient. For example, it may not be possible to infer consent to receipt of emails concerning a type of product offered by an organisation just because the recipient is known to use another unrelated product offered by that same organisation. However, case law on the Spam Act suggests that consent could be inferred where there is a pre-existing relationship and the email relates to a product or similar products already purchased by the customer from an organisation, and the customer has not indicated they do not wish to receive the emails. It is also important to note that consent offered under the Act can be withdrawn. The legislation provides that if the recipient sends a request to the sender to the effect that the recipient does not wish to receive any further commercial electronic messages from the sender, then consent will be taken to have been withdrawn within five business days of receipt of the 'opt-out' request.

The Spam Act expressly prohibits ancillary contraventions of its key offence provisions. It also prohibits the supply, acquisition or use of address harvesting software, and the use of lists generated by such software to send commercial electronic messages.

The Australian Communications and Media Authority (ACMA) is the sole enforcer of the Spam Act regime. It has a wide range of enforcement mechanisms available to it, ranging from encouraging the development of industry codes, through to court action seeking injunctions and damages or recovery of profits. Although there is no private right of action under the Spam Act, a private company or individual could apply for damages once the ACMA takes proceedings in the Federal Court and the Court finds there has been a contravention. In practice, one the ACMA's key enforcement powers is its ability to levy pecuniary penalties: for individuals, these fines can extend up to AUD$44,000 (approximately USD$36,940) per day for a first offence and up to AUD$220,000 (approximately USD$184,620) for repeat offences; corporations can face up to AUD$220,000 (approximately USD$184,620) per day for a first offence and up to AUD$1.1 million (approximately USD$923,090) per day for repeat offences. None of the Spam Act's provisions impose criminal liability for contraventions of the regime.

In June 2006, the Department of Communications, Information Technology and the Arts (DCITA) released a report reviewing the Spam Act. DCITA found that since the Spam Act came into force, the percentage of worldwide spam originating in Australia has decreased. The report did not recommend any changes to the main provisions of the Spam Act, and the federal government has accepted the recommendations of the DCITA report.

The Australian eMarketing Code of Practice is an industry code that is registered under the federal Telecommunications Act 1997. The Code concerns business practices for sending "commercial electronic messages" as defined by the federal Spam Act, including email, instant messages, SMS and MMS messages. It applies to:

- Message Originators (a person who sends electronic messages promoting products they will supply themselves where such messages are the sole or principal means of advertising, marketing or promoting the products); and
- Message Service Providers (a person who sends, under a contract or other arrangement, an electronic message advertising, marketing or promoting products offered by a third party),

when they send communications with an Australian link (as defined in the Spam Act). Although the Code is intended to be explanatory, some of its provisions go beyond the Spam Act, including the Code's detailed complaint-handling procedures and the new obligation it places on Message Originators in respect of age-sensitive communications. Enforcement of the Code is the responsibility of the ACMA and can range from a formal warning through to a direction to comply (breach of which results in a civil penalty of up to AUD$250,000 (approximately USD$209,770)) and Federal Court injunctions. These enforcement options are in addition to the remedies available under the Spam Act for the same conduct.

The IIA Spam Code of Practice is another industry code that is registered under the federal Telecommunications Act 1997. The Code applies to email service providers and carriage service providers that are involved in the generation, transmission or delivery of spam, being commercial emails that (i) are unsolicited, (ii) do not contain accurate sender information and/or (iii) do not contain a functional unsubscribe facility. The Code imposes fewer obligations on 'International ESPs', who are email service providers that:

- have their central management and control located outside Australia;
- host, on computers located outside Australia, the contents of emails received or sent by end users;
- have some end users located in Australia; and
- have a greater number of end users located outside Australia than in Australia.

The Telecommunications Act makes compliance with the Code by email service providers and carriage service providers mandatory.

2. Australia

2.6 SPAM LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

At the date of writing, there are no upcoming legislative developments that relate to spam.

2.7 ONLINE CHILD SAFETY LAWS – CURRENT LEGISLATIVE FRAMEWORK

The age of majority in Australia is 18 years; the age of consent to sexual relations is either 16, 17 or 18 years of age depending on the applicable state or territory laws.

General child pornography offences

State and territory legislation

All of Australia's states and territories have enacted offences that criminalise the production, dissemination and mere possession of child pornography. Typically, it is also an offence to involve a child or someone who appears to be a child in the production of child pornography. Child pornography is generally defined as a description or depiction of a child (a person under the age of 16 or 18 depending on the jurisdiction) engaged in sexual activity or in a sexual context. In some jurisdictions, there is the additional test of whether the description or depiction in question is such that a reasonable person would regard it as offensive.

Corporate liability for general child pornography offences is specifically addressed in some states and territories, and the associated fines are high, extending up to AUD$1.1 million (approximately USD$920,300); in the Northern Territory, directors and high-ranking management staff are liable to be individually prosecuted for child pornography offences that their body corporate is guilty of. Individual offenders can be liable to imprisonment for a term of up to 21 years depending on which jurisdiction's laws apply, although a maximum of 10 years imprisonment for a first offence is the norm.

Computer-facilitated child pornography offences (Title 3 COE)

Federal legislation

The Criminal Code makes it an offence, punishable by 10 years imprisonment, to:

- intentionally use a carriage service (i.e. use the internet or a mobile phone network) to access, transmit, publish, make available or otherwise distribute child pornography material; and
- possess, control, produce, supply or obtain child pornography material with the intent that it be disseminated using a carriage service in contravention of the Criminal Code.

For the purpose of these offences, child pornography material is defined as images that depict or describe a person under the age of 18 engaged in a sexual pose or sexual activity. Sexually motivated images of sexual organs, the anal region or the breasts of a person under the age of 18 will usually be covered. Importantly, material is only considered child pornography material if it is depicted or described in a way that a reasonable person would regard as offensive.

The introduction of these computer-facilitated child pornography offences was coupled with the imposition of reporting obligations on Australian internet service providers (ISPs) and internet content hosts (ICHs). These entities must report to the Australian Federal Police material that can be accessed via their services, and which they reasonably believe to be child pornography material. Failure to comply with this reporting obligation, within a reasonable time of becoming aware of the offending material's existence, is a criminal offence that can attract a fine of up to AUD$55,000 (approximately USD$46,000).

Miscellaneous

Grooming offences

The federal Criminal Code Act 1995 criminalises the use of the internet to procure or "groom" a person under the age of 16 for sexual activity. These offences are punishable by imprisonment for 15 and 12 years respectively.

Similar offences have been enacted in Queensland, Western Australia and South Australia to cover both online and offline grooming. Like the federal legislation, the grooming offence in the Australian Capital Territory only applies online. These offences attract terms of imprisonment of between 5 and 14 years.

Cooperative statutory classification scheme

In addition to the general and computer-facilitated child pornography offences discussed above, there is a cooperative statutory classification scheme in Australia that prohibits dealing in offensive and objectionable material, including child pornography. This scheme comprises central federal legislation, which establishes the classification (ratings system) of publications, films and computer games according to legislated standards of public morality, and complementary state and territory legislation which deals with the enforcement of the national classification scheme (Classification Enforcement Acts). The state and territory Classification Enforcement Acts criminalise the sale, publication, display and delivery of publications, films and computer games, including those with child pornography content. The Victorian, Northern Territory and Western Australian Classification Enforcement Acts also deal expressly with the online distribution of objectionable content.

Online censorship regime

The federal government has developed a co-regulatory online censorship regime that builds upon the classification scheme discussed earlier. Previously, this online censorship regime only

applied to stored internet content. However, in July 2007, the Australian Parliament enacted substantial amendments to its earlier regime such that it will shortly apply to both stored internet content and ephemeral internet content, such as live streamed content.

The majority of the recent amendments are due to come into force by no later than 20 January 2008.

The new regime regulates persons offering content services that host stored content, provide links to content, provide live content and provide commercial content services. In all cases, these content services must have an "Australian connection" to fall within the scope of Schedule 7 of the Broadcasting Services Act. A content service will have an "Australian connection" if:

- in the case of a links service or a commercial content service, any of the content provided by the content service is hosted in Australia;
- in the case of a live content service, the live content service is provided from Australia; or
- in the case of a hosting service, the content hosted by the service is hosted in Australia.

The new regime establishes a series of removal notices that may be issued by ACMA requiring:

- hosting service providers to take down prohibited (or potentially prohibited) content from hosting services;
- links service providers to remove links to prohibited (or potentially prohibited) content; and
- live content providers to stop providing live content services which provide prohibited (or potentially prohibited) content.

The concepts of prohibited (or potentially prohibited) content are defined by reference to the federal classification legislation.

ACMA may issue removal notices as a result of complaints made by end users or as a result of its own investigations. Removal notices must be complied with as soon as practicable and by no later than 6pm on the next business day. A failure to comply with a removal notice may result in civil or criminal penalties of up to AUD$55,000 (approximately USD$46,000) per offence.

As was previously the case, the new regime is co-regulatory – it contemplates that industry codes will be registered to regulate various parts of the content industry, including commercial content providers.

Mobile Premium Services Determination

In 2005, the ACMA issued a determination that regulates the provision of premium (i.e. paid content) services to mobile phones via SMS, MMS or 'walled garden' mobile portals; the Broadcasting Services Act continues to regulate content obtained by accessing the internet via mobile phones. The ACMA's determination prohibits carriage and content service providers from supplying a chat service by means of a mobile premium service unless certain safety measures designed to protect children are in place. There are supplementary prohibitions on the supply of a mobile premium service to enable access to content which would be classified X 18+ or RC. For transparency purposes, the determination also requires carriage and content service providers to (i) use the prefixes 195 or 196 in the provision of age-restricted mobile phone services and (ii) provide their customers with appropriate information about the costs and terms and conditions of mobile premium services.

IIA Content Code of Practice

In May 2005, the ACMA registered the IIA Content Code of Practice version 10.4 – which guides ISPs, ICHs, mobile carriage service providers and mobile content providers in the fulfilment of their obligations under Schedule 5 of the Broadcasting Services Act and the ACMA's Mobile Premium Services Determination. Although compliance with the IIA Code is voluntary, the ACMA can direct ISPs and ICHs to do so, and compliance with the Code provides automatic compliance with Schedule 5 of the Broadcasting Services Act. In addition to addressing the practicalities of how ICHs and ISPs can comply with the Schedule 5 regime, the Code requires ISPs to (i) take reasonable steps to ensure that internet access accounts are not provided to minors, (ii) encourage content host subscribers to label content that is inappropriate for children and inform these subscribers that they may not post illegal material on their websites, and (iii) provide information to subscribers about online safety, including information about filtering software and how this can be obtained. The Code's mobile service provisions establish an 'opt-in' regime for adults who seek access to restricted content (material that is classified as MA, MA(15+), R or R18 in accordance with the federal classification scheme), and require mobile carriers and content providers to provide end users with information about supervising minors' access to mobile content, among other things.

2.8 ONLINE CHILD SAFETY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

Mobile Premium Services Determination

In the light of the amendments to the Broadcasting Services Act discussed previously, the ACMA has announced that it plans to amend its determination regulating premium mobile phone content. The amendments are designed to ensure that there is no overlap between the amended Broadcasting Services Act and the determination. The amended determination is expected to come into force around the same time as the amendments to the Broadcasting Services Act (i.e. by the end of January 2008 at the latest).

2. Australia

Part 3 – Benchmark Comparison

Key: Favourable alignment Moderate alignment Weak alignment

(E) Enacted
(P) Pending
(Title [x]) Title [x] of the Council of Europe Convention on Cybercrime (COE)

Area	Legislation to be compared with benchmark	Benchmark legislation	Overall alignment	Areas of strong alignment	Areas of moderate alignment	Areas of weak alignment
Computer Security Laws	**Federal:** Criminal Code Act 1995 (E); Crimes Act 1914 (E); Telecommunications (Interception and Access) Act 1979 (E) **State and territory:** Criminal legislation (see page 1 for complete listing of applicable legislation)	Council of Europe Convention on Cybercrime (Titles 1, 2 and 5)		• Data interference offence • Computer-related forgery and fraud offences • Ancillary liability for attempting, aiding or abetting cybercrimes • Corporate criminal liability for cybercrimes	• Illegal access, system interference and misuse of device offences	

Area	Legislation to be compared with benchmark	Benchmark legislation	Overall alignment	Areas of strong alignment	Areas of moderate alignment	Areas of weak alignment
Privacy Laws	**Federal:** Privacy Act 1988 (E)	Model Privacy Bill (drafted by Microsoft)		• Transparency matters that must be notified to data subjects (e.g. the identity of the entity that collects data and the purposes of use of the personal information) • Obligation to keep personal information free from loss or unauthorised disclosure or destruction • Data subject's right to access and correct personal information	• Definition of personal information • Definition of sensitive personal information • Mode of enforcement (enforcement by individual or Commissioner cf. enforcement by Commissioner) • Consequence of infringement (civil liability cf. statutory & civil liability)	• Separate private and public sector regimes • Restrictions on trans-border data flows • Different models regulating use or disclosure for secondary purposes • No breach notification provisions
Spam Laws	**Federal:** Spam Act 2003 (E)	Anti-spam legislation checklist (drafted by Microsoft)		• Remedies for infringing conduct: capped statutory penalties in addition to civil damages • Transparency requirements (sender identification, functional unsubscribe facility) • No "bulk" requirement • Definition of commercial electronic message • Liability for ancillary contraventions of the regime • Address harvesting and dictionary attack measures • No private right of action for individuals • No 'ADV' or other labelling requirement	• ISP safe harbour for transmitting infringing messages but no express exclusion of obligation on ISPs to carry or block certain electronic messages	• 'Opt-in' regime for unsolicited commercial electronic messages • Limited recognition of pre-existing business relationships • No private right of action for ISPs/email service providers; responsibility for enforcement falls primarily on the ACMA
Online Child Safety Laws	**Federal:** Criminal Code Act 1995 (Cth) (E) **State and territory:** Criminal and censorship legislation (see page 1 for complete listing of applicable legislation)	Council of Europe Convention on Cybercrime (Title 3 COE)/ICMEC principles		• General child pornography offences • Mere possession of child pornography is prohibited • Specific internet-facilitated child pornography offences • ISP and ICH reporting obligation in respect of known child pornography activities	• Definition of child pornography • Inconsistencies between state and territory regimes	

Last Updated: 17 October 2007

3. China

Part 1 – Snapshot of Legislative Status

Key:

(E)	Enacted
(P)	Pending
(Title [x] COE)	Title [x] of the Council of Europe Convention on Cybercrime (COE)
PRC	People's Republic of China

Area	Topic	Enacted legislation	Pending legislation	Relevant instruments/Comments
Computer Security Laws	**Core offences (Title 1 COE):** illegal access, illegal interception, data interference, system interference, misuse of devices	✓	✓	PRC Criminal Code (E); Measures for the Administration of Protecting the Security of International Connections to Computer Information Networks (E) and the Decision of the Standing Committee of the National People's Congress on the Protection of Internet Security (E) Information Security Regulations (P)
	Computer-related offences (Title 2 COE): computer-related forgery, computer-related fraud	✓	✓	PRC Criminal Code (E) Information Security Regulations (P)
	Ancillary liability (Title 5 COE): attempt and aiding/abetting, corporate liability	✓	✗	PRC Criminal Code (E); Administrative regulations may also apply.
Privacy Laws	**Data protection**	✗	✓	The State Council Informatization Office is tasked with preparing data protection legislation.
	Surveillance (see illegal interception under computer security)	✓	✗	Illegal interception of letters and illegal searches of residences are prohibited by the PRC Criminal Code (E), but a web of administrative regulations permits extensive surveillance activity.
	Sensitive information	✓	✗	Various legislation including the Law on the Protection of Minors (E), Law on Lawyers (E), Practising Physician Law (E) and the Provisional Regulations Relating to Bank Management (E).
	Miscellaneous	✓	✗	Constitution of the People's Republic of China (E); General Principles of the Civil Law of the People's Republic of China (E)
Spam Laws	**Anti-spam regulation**	✓	✗	Internet Email Service Management Regulations 2006 (E); Interim Handling Measures on Spam (E); Announcement on the Regulation on the Activities of Utilizing Email to Send Commercial Information [Beijing] (E); Guangdong Measures (E).
Online Child Safety Laws	**General child pornography offences**	✗	✗	Minors Protection Law (E). Administrative regulations may also apply.
	Computer-facilitated child pornography offences (Title 3 COE)	✗	✓	Amendments to the Minors Protection Law have been tabled in the National Assembly, but the likelihood of, and timetable for, their enactment remains unclear.

Part 2 – Legal and Regulatory Position

By way of background, unlawful activities can attract up to three different types of liability in the People's Republic of China (PRC): criminal, administrative and civil. Generally speaking, only unlawful activities of "serious consequence" attract criminal liability under the PRC Criminal Code; less serious unlawful activities that harm the public interest are usually dealt with by administrative authorities (which may give rise to both criminal and administrative liability). As in western jurisdictions, civil liability arises when a party who suffers damage as a result of the conduct of another seeks to recover its loss from the party that has acted unlawfully.

The discussion that follows considers both criminal and administrative regulations that relate to internet safety, security and privacy. This approach acknowledges the unique role that Chinese administrative authorities play as both decentralised lawmaking bodies and enforcement agencies.

2.1 COMPUTER SECURITY LAWS – CURRENT LEGISLATIVE FRAMEWORK

Core offences (Title 1 COE): Illegal access, illegal interception, data interference, system interference, misuse of devices

Criminal regulation

The PRC Criminal Code creates offences in respect of illegal access, data interference and system interference. It only indirectly addresses the Convention's illegal interception offence and does not appear to consider the misuse of devices at all.

The Code's illegal access offence is of limited application – it only applies in respect of computer information systems that concern state affairs, national defence or sophisticated science and technology. Offenders are liable to imprisonment for a term of up to three years or criminal detention.

Contrastingly, the Code's data and system interference offences apply to all computer information systems without restriction. These offences are punishable by a maximum term of five years imprisonment or criminal detention (if the conduct is serious), or a minimum term of five years imprisonment (if the conduct is especially serious). In addition to its general system interference offence, the Code specifically prohibits the creation and dissemination of computer viruses that affect the normal operation of a computer information system.

While the Code does not prohibit the act of intercepting non-public transmissions of data, it prohibits activities that may constitute a pre-requisite thereto. Article 265 makes it an offence to "stealthily" connect a telecommunications line with that of another, duplicate another person's telecommunication code or number, or use telecommunications equipment knowing that it is "stealthily" connected with that of another. To attract criminal liability, each of these acts must be done for the purposes of profit. Offenders are penalised based on the seriousness of their conduct and penalties can extend up to life imprisonment, fines or the confiscation of property.

Administrative regulation

National administrative regulations that impose criminal and administrative liability for acts of the kind regulated by the Convention on Cybercrime include:

- the Measures for the Administration of Protecting the Security of International Connections to Computer Information Networks (Computer Measures); and
- the Decision of the Standing Committee of the National People's Congress on the Protection of Internet Security (Decision on Internet Security).

Article 6(1) of the Computer Measures prohibits the intrusion into, or use of, a computer information network without authorisation. It is also an infringement to interfere with data or an application program that is stored in, processed or transmitted by a computer information network without authorisation. As with the equivalent offence under the Criminal Code, it is a specific infringement of the Computer Measures to deliberately produce or disseminate a computer virus or other harmful program. These infringements attract a range of sanctions including warnings issued by public security agencies, confiscation of illegal income and fines of up to RMB5,000 (approximately USD$670) for an individual and RMB15,000 (approximately USD$2,000) for a corporation.

For the most part, the Decision on Internet Security reaffirms the liability imposed by the Criminal Code for cybercrime activities. However, in some areas, the Decision appears to extend this liability, although it is less than clear that the Decision achieves this objective. For example, the Decision attempts to create criminal liability for the illegal interception of communications by stating that "illegally intercepting, modifying or deleting another person's email or data and information is an illegal act which attracts criminal liability if it constitutes a crime."

Numerous sectoral and local regulations also impose administrative liability for acts of the kind regulated by the Convention on Cybercrime.

Computer-related offences (Title 2 COE): Computer-related forgery, computer-related fraud

Criminal regulation

The PRC Criminal Code criminalises the commission of traditional crimes by use of a computer or computer network. Article 287 makes specific mention of the possibility that the crime of financial fraud may be committed by use of a computer, but since the list of traditional crimes within the scope of this article is not exhaustive, there is a case for arguing that computer-related forgery would also fall within the ambit of this provision. Offenders face the punishment applicable to the traditional crime they commit by their use of a computer or computer network.

Administrative regulation

There do not appear to be any administrative regulations that address computer-related forgery and fraud.

Ancillary liability (Title 5 COE): Attempt and aiding/abetting, corporate liability.

Criminal regulation

Under the PRC Criminal Code, it is an offence to teach another person how to commit a crime. In practice, this provision is likely to embrace those who make viruses or malicious code available over the internet or other networks, as well as more traditional forms of educating others about how to commit a crime.

In China, corporate crime can only be punished when explicit provision is made for it. No such provision is made in the PRC Criminal Code in respect of the core and computer-related offences discussed previously.

3. China

Administrative regulation

Given the proliferation of national, sectoral and local regulations, it is difficult to generalise about the ancillary liability provisions found in administrative regulations. However, it is not uncommon for corporations to face increased fines vis-à-vis individuals for their infringement of administrative regulations.

2.2 COMPUTER SECURITY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

China is in the process of drafting National Information Security Regulations, however, neither the content of these regulations, nor the timeframe for their enactment, is known.

2.3 PRIVACY LAWS – CURRENT LEGISLATIVE FRAMEWORK

Data protection

China does not have any comprehensive data protection legislation.

The Internet Email Service Management Regulations 2006 offer individuals some limited data protection rights in relation to their personal data held by internet email service providers. Article 9 of the Regulations obliges internet email service providers to keep their users' personal registration information confidential, and prohibits them from disclosing this information without the consent of the data subject unless otherwise permitted by law. Service providers can face fines of up to RMB30,000 (approximately USD$4,000) for contravening Article 9. In addition, Article 3 of the Regulations protects the right of citizens to the privacy of their email communications except where authorities are lawfully entitled to censor emails for the purposes of national security or criminal investigations.

Surveillance

Pursuant to China's General Principles of the Criminal Law, it is illegal to hide, destroy or open a person's letters without authorisation; if the offending is sufficiently serious, offenders will be liable to a maximum of one year's imprisonment or criminal detention. Similarly, those who illegally search others' residences commit a criminal offence punishable by a maximum of three years imprisonment or criminal detention.

Despite these protections, surveillance, in its many forms, is not uncommon in China. Law enforcement officials can issue search warrants on their own authority and if legal requirements for oversight exist, these are routinely ignored. China's largest government surveillance operations are conducted online – it has been reported that up to 30,000 people are employed by the Ministry of Public Security to search for online activity that might harm unification of the country, endanger national security or subvert government authority (see more in section 2.7).

The Internet Email Service Management Regulations 2006 oblige internet email service providers to record the time at which emails are sent from, or received by, their email servers, as well as the email and IP addresses for the senders or recipients of those emails. Service providers are required to keep this data for 60 days and provide it to government authorities when requested to do so in accordance with law.

Sensitive information

The PRC has a patchwork of laws and regulations that protect sensitive information. The Law on the Protection of Minors provides that no organisation or individual shall disclose the personal secrets of minors (a person under the age of 18). Solicitor-client confidentiality is preserved by the Law on Lawyers and doctor-patient confidentiality is maintained by the Practising Physician Law. The Provisional Regulations Relating to Bank Management provide that all information concerning the savings of clients shall not be disclosed.

Miscellaneous

The Constitution of the PRC affords citizens three privacy-related rights. It provides that:

- the personal dignity of citizens is inviolable;
- the residences of citizens are inviolable; and
- the freedom and privacy of the correspondence of citizens are protected by law.

Article 101 of the General Principles of the Civil Law, which affirms the personality of citizens, has been interpreted by the Supreme Court as extending protection to citizens' rights of privacy. Tortious rights of privacy have also been recognised.

In the online context, Article 7 of the Measures for the Administration of the Protection of Security for International Connections to Computer Information Network (Internet Security Measures) provides that the freedom and privacy of online users' correspondence is protected by law.

2.4 PRIVACY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

Data protection

For a number of years, China has been in the process of drafting data protection laws. This process has included two summits held by the Chinese Academy of Social Sciences (CASS), which have involved industry members. CASS academics have been taking a lead in undertaking the task of examining data protection laws in other jurisdictions with a view to making recommendations to the State Council Informatization Office (SCITO) as to the appropriate approach to data protection legislation for China. It is understood

that SCITO is also consulting with other data protection experts and will continue these discussions into 2008. It is expected that a draft of China's data protection law will be placed on the legislative agenda of the National People's Congress during 2008.

Miscellaneous

It appears as though China is in the process of drafting the first civil law code, which is expected to clearly recognise and protect an individual's right to privacy. Indeed, proposed article 90 provides that "natural persons shall enjoy the right to privacy". The draft civil law code was tabled with the Standing Committee of China's National People's Congress in December 2002. It remains unclear if and when the civil law code will be enacted.

2.5 SPAM LAWS – CURRENT LEGISLATIVE FRAMEWORK

Administrative regulations

In March 2006, the Internet Email Service Management Regulations came into force. The Regulations apply only to emails and not to other types of electronic communications, such as SMS and MMS messages, and faxes. In addition to containing provisions that address the sending of spam, the Regulations contain provisions that regulate the conduct of internet email service providers. For example, email service providers are required to take steps to strengthen the protection of their email servers to avoid them being used by spammers.

Articles 13 and 14 of the Regulations provide that no person or organisation shall send:

(i) emails that have hidden or falsified address information;

(ii) commercial emails without the express consent of the recipient;

(iii) commercial emails without 'AD' or the equivalent Chinese characters in the subject heading;

(iv) commercial emails after the recipient has opted-out of receipt of the same; or

(v) commercial emails which do not include valid sender contact information, including an email address, so that recipients can, if they wish, inform the sender that they no longer wish to receive commercial emails.

Where Articles 13 or 14 have been contravened, the Ministry of Information Industry and the other relevant regulators have the power to order the correction of such violations and may impose fines of up to RMB10,000 (approximately USD$1,330). These fines can increase to up to RMB30,000 (approximately USD$4,000) where the sender obtains an "illegitimate income" from the contravention.

In addition, Article 12 of the Internet Email Service Management Regulations appears to prohibit the sale, distribution or exchange of email addresses (i) gathered using address-harvesting software or other automated means, or (ii) generated by dictionary attacks. Article 12(1) also prohibits individuals or organisations from sending emails through other people's computers without permission to do so. This provision appears to outlaw at the use of 'zombie' computers to send spam. Contraventions of Article 12 attract the same sanctions as contraventions of Article 13 (as set out in the preceding paragraph).

Internet email service providers and telecommunication business providers are required under the Regulations to make available mechanisms for users to post spam-related complaints. Internet email service providers and telecommunication business providers must also address any such complaints in accordance with the Regulations. One of the complaint-handling requirements of the Regulations is that service providers must report to the relevant authority complaints about emails that contain content prohibited by Article 57 of the Telecommunications Regulations. This includes content that is detrimental to the dignity or interests of the State, and content that disrupts social order or undermines social stability. All other complaints about emails, including those prohibited by Article 12, are to be reported to the Email Reporting Center, which has been established by the Internet Society of China and accredited by the Ministry of Information Industry. The Ministry of Information Industry and the relevant regulators can issue a disciplinary warning or a fine of between RMB5,000 (approximately USD$670) and RMB10,000 (approximately USD$1,330) for contraventions of the complaint-handling provisions of the Regulations.

Sectoral and local regulations

In addition to the Internet Email Service Management Regulations, sectoral and local regulations that contain anti-spam measures are also in place.

China Telecom's sectoral regulations – the Interim Handling Measures on Spam – prohibit the transmission of spam over China Telecom's networks. For this purpose, spam is defined as:

(i) an email advertisement, publication or other information sent to a user who has not asked for it;

(ii) an email that does not specify return methods, and a sender or reply address;

(iii) any activity that utilises China Telecom's network to jeopardise other ISPs' security policies or service clauses; or

(iv) other emails in respect of which complaints are anticipated.

The Interim Handling Measures on Spam provide for sanctions ranging from warnings through to service suspension and account closure. Importantly, the regulations only apply to activity over China Telecom's networks.

3. China

Locally, in Beijing, online users must conform to a series of rules when sending commercial information via email. Commercial information cannot be emailed without the consent of the receiver and the sender cannot distribute "fake" information by taking advantage of email. Moreover, a sender cannot defame another's business reputation by taking advantage of email, and the content of an advertisement transmitted via email must not breach the applicable provisions in the Advertisement Law.

Further, article 11(2) of the Guangdong Measures prohibits an entity or an individual from sending unsolicited messages to others. Like the Beijing regulations discussed above, the Guangdong Measures only apply in the Guangdong province.

2.6 SPAM LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

As at the date of writing, there are no upcoming legislative developments that relate to spam. However, it is understood that the Internet Society of China is continuing its research into different approaches to comprehensive spam regulation. This study has been endorsed by the Ministry of Information Industry.

2.7 ONLINE CHILD SAFETY LAWS – CURRENT LEGISLATIVE FRAMEWORK

General child pornography offences

The age of majority in China is 18 years; the age of consent for sexual relations is 14 years.

Criminal regulation

China does not have any specific child pornography legislation. However, there are general obscenity prohibitions in the PRC Criminal Code. Its definition of "obscene article" specifically mentions pornography and the production, distribution and sale of such items is prohibited. Although it is unclear whether possession of obscene articles is prohibited under Chinese law, the best view seems to be that it is. In any event, it is understood that some courts may regard possession of significant quantities of offending material as evidence of distribution thereof.

Serious instances of dealing in pornographic objects are likely to attract criminal liability under the Criminal Code. The Code's provisions distinguish between distribution of pornographic materials for profit, and distribution for non-profit purposes. In the latter case, the relevant provision of the Code requires that there must be a "serious circumstance" to warrant prosecution; this requirement has been quantified by the Supreme People's Court. According to the Court's interpretation, the number of items that must be disseminated for the legal threshold to be met depends on the medium of distribution – the requirement is less for pornographic material recorded on a video, but much higher for material accessed by a hyperlink. For example, it is a "serious circumstance" where the alleged offender has disseminated more than 400 electronic publications, photos, articles or SMS messages containing pornographic content. This offence is punishable by criminal detention, public surveillance or imprisonment for up to two years. Dissemination of pornographic materials to a minor (a person under the age of 18) attracts a heavier punishment, as does the production or duplication of pornographic audio-video products.

Where distribution of pornographic materials is for profit, there is no "serious circumstance" requirement. Offenders face a range of penalties including criminal detention, public surveillance, fines, confiscation of property and life imprisonment (depending on the seriousness of the conduct). The act of producing pornographic materials for profit is similarly punished.

Note also that the Law of Preventing Minors' Criminal Offences prescribes that publications aimed at minors must not contain contexts that induce a minor to carry out a criminal offence, or which describe violence, erotic acts, gambling or terrorism.

Administrative regulation

Less serious instances of dealing in pornographic objects may be pursued under the PRC Penal Regulations Concerning Security Administration. Under these administrative regulations, making, duplicating, selling, lending or distributing pornographic objects is strictly forbidden. Offenders are liable to detention for a maximum of 15 days and/or a fine of up to RMB3,000 (approximately USD$400) or public surveillance.

Computer-facilitated child pornography offences (Title 3 COE)

In late 2006 the Minors Protection Law was amended to prohibit organisations and individuals from selling, renting, leasing or distributing any publication, book, video, audio compilation or electronic or online publication that contains pornographic or obscene content. We understand that this offence applies to certain computer-facilitated dealings with child pornography.

Miscellaneous

Censorship of online content is another well-documented means by which the Chinese government restricts the availability of objectionable material online. The Internet Information Services Regulations promulgated by the Ministry of Information Industry (MII) impose obligations on ISPs to monitor certain types of content including material that opposes the principles established by the PRC Constitution, material that undermines state religious policies and material that spreads obscenities, pornography or violence. Under the same regulations, internet cafe patrons must register with software managers (appointed censors who monitor internet usage) and produce a valid ID card in order to log on to the internet. Further, the Computer Information Network and Internet Security, Protection and Management Regulations provide that all those

engaged in internet businesses are subject to security supervision, inspection and guidance by the Ministry of Public Security. This oversight can extend to assistance with cybercrime investigations. Under the current regime, much of the responsibility for content control is placed on ISPs.

In September 2005, the Ministry of Information Industry and the State Council issued new internet content regulations that seek to control content on news websites. It has been reported that these regulations prohibit news media organisations from using websites to spread news or information that undermines state security or the public interest, and that only "healthy and civilised news and information that is beneficial to the improvement of the quality of the nation, beneficial to its economic development and conducive to social progress" can be posted on the internet. Operators of websites that report "false or distorted" information may face fines of up to RMB30,000 (approximately USD$4,000). In addition, it is understood that the new regulations force bloggers and chatroom participants to use their own names and university online discussion groups will be restricted to students. Commentators believe that these new regulations are targeted at individuals and ad hoc journalists that do not work for licensed organisations. For internet café operators, the new regulations are little more than a restatement of existing obligations.

2.8 ONLINE CHILD SAFETY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

There are no upcoming legislative developments in China relating to child pornography.

Miscellaneous

The Chinese government is currently considering adopting measures which would require search engine operators to use technical means to (i) monitor and block specified online information, and (ii) report to the government on this activity. These measures are being considered as a means of controlling objectionable material on the Internet. Among other things, it is expected that these proposals would apply to child pornography and other material affecting online child safety.

3. China

Part 3 – Benchmark Comparison

Key: Favourable alignment | Moderate alignment | Weak alignment

(E) Enacted
(P) Pending
(Title [x]) Title [x] of the Council of Europe Convention on Cybercrime

Area	Legislative regime to be compared with benchmark	Benchmark legislation	Overall alignment	Areas of strong alignment	Areas of moderate alignment	Areas of weak alignment
Computer Security Laws	PRC Criminal Code (E) Measures for the Administration of Protecting the Security of International Connections to Computer Information Networks (E) Decision of the Standing Committee of the National People's Congress on the Protection of Internet Security (E)	Council of Europe Convention on Cybercrime (Titles 1, 2 and 5)		• Data and system interference offences	• Illegal access and interception offences • Ancillary liability for attempting, aiding or abetting cybercrimes	• No misuse of devices offence • No provision for corporate liability under the PRC Criminal Code • No provision for ancillary liability by abetting the commission of a core offence • Combined criminal and administrative regime means that prohibited acts will not always attract criminal liability
Privacy Laws	There is no readily available comprehensive enacted or pending data protection legislation in the PRC upon which a benchmarking analysis can be conducted.					
Spam Laws	Internet Email Service Management Regulations 2006 (E) Interim Handling Measures on Spam (E)	Anti-spam legislation checklist (drafted by Microsoft)		• Transparency requirement (sender identification, unsubscribe facility) • Address harvesting and dictionary attack measures • No private right of action for individuals		• "Opt-in" regime • Regulations only apply to emails • Labelling requirement • No private right of action for ISPs/email service providers • No consideration of ISP safe harbour for transmitting infringing messages • No recognition of pre-existing business relationships
Online Child Safety Laws	PRC Criminal Code (E) PRC Penal Regulations Concerning Security Administration (E)	Council of Europe Convention on Cybercrime (Title 3 COE)/ICMEC principles			• Criminal sanctions for serious dealing in obscene material • Possession irrespective of intent to distribute likely to be prohibited	• Distinction between for-profit and not-for-profit distribution of obscene material • Administrative liability for less serious distribution of obscene material • No legislation specific to child pornography • No definition of child pornography • No computer-facilitated child pornography offences • No scope for ISP reporting of dealing in child pornography
	Minors Protection Law (E)	Council of Europe Convention on Cybercrime (Title 3 COE)/ICMEC principles)	There is no readily available English translation of the legislation upon which a benchmarking analysis can be conducted.			

Last Updated: 24 October 2007

4. Hong Kong

Part 1 – Snapshot of Legislative Status

Key: (E) Enacted
(P) Pending
(Title [x] COE) Title [x] of the Council of Europe Convention on Cybercrime (COE)

Area	Topic	Enacted legislation	Pending legislation	Relevant instruments/Comments
Computer Security Laws	**Core offences (Title 1 COE):** illegal access, illegal interception, data interference, system interference, misuse of devices	✓	✗	Crimes Ordinance (Cap. 200) (E); Telecommunications Ordinance (Cap. 106) (E)
	Computer-related offences (Title 2 COE): computer-related forgery, computer-related fraud	✓	✗	Crimes Ordinance (Cap. 200) (E); Theft Ordinance (Cap. 210) (E)
	Ancillary liability (Title 5 COE): attempt; aiding/abetting, corporate liability	✓	✗	Criminal Procedure Ordinance (Cap. 221) (E); Crimes Ordinance (Cap. 200) (E)
Privacy Laws	**Data protection**	✓	✗	Personal Data (Privacy) Ordinance (Cap. 486) (E)
	Surveillance (see illegal interception under computer security)	✓	✗	Interception of Communications and Surveillance Ordinance (Cap. 589) (E); Registration of Persons Ordinance (Cap. 177) (E)
	Sensitive information	✓	✗	Sensitive financial information is protected by various pieces of legislation, including the Banking Ordinance (Cap. 155) (E) and the Inland Revenue Ordinance (Cap. 112) (E).
Spam Laws	**Anti-spam regulation**	✓	✗	Unsolicited Electronic Messages Ordinance (Cap. 593) (E)
Online Child Safety Laws	**General child pornography offences**	✓	✗	Prevention of Child Pornography Ordinance (Cap. 579) (E); Crimes Ordinance (Cap. 200) (E)
	Computer-facilitated child pornography offences (Title 3 COE)	✓	✗	Prevention of Child Pornography Ordinance (Cap. 579) (E)

Part 2 – Legal and Regulatory Position

Hong Kong was established as a Special Administrative Region (HKSAR) of the People's Republic of China (PRC) when the PRC resumed its sovereignty over Hong Kong in July 1997. At this time, the majority of Hong Kong's laws were incorporated into the Chinese legal system by the enactment of the Basic Law of the HKSAR; those that were not remain in force in Hong Kong under the "one country, two systems" policy. The Basic Law of the HKSAR vests the Special Administrative Region with its own law-making power which is exercised by Hong Kong's Legislative Council.

2.1 COMPUTER SECURITY LAWS – CURRENT LEGISLATIVE FRAMEWORK

Core offences (Title 1 COE): Illegal access, illegal interception, data interference, system interference, misuse of devices

The Crimes Ordinance (Cap. 200) criminalises the act of gaining access to a computer with criminal intent or dishonest intent (dishonest intent is one of the qualifications permitted by the Convention). Under the Telecommunications Ordinance, it is an offence to knowingly cause a computer to perform any function to obtain unauthorised access to any program or data held in a computer. This unauthorised access must be obtained by means of a telecommunications system. Contraventions of the Crimes Ordinance offence can lead to imprisonment for up to 5 years; contraventions of the Telecommunications Ordinance offence are punishable by a fine of up to HKD$20,000 (approximately USD$2,570).

Neither the Crimes Ordinance nor the Telecommunications Ordinance appear to contain an illegal interception offence of the kind contemplated in the Convention. However, the recently enacted Interception of Communications and Surveillance Ordinance 2006 (Cap. 589) does prohibit public officers from directly or indirectly intercepting a communication transmitted via the postal service or a telecommunications system, unless certain circumstances exist. This prohibition is further discussed in section 2.3.

4. Hong Kong

Data and system interference are forms of property damage under the Crimes Ordinance. The Ordinance covers reckless damage as well as that caused intentionally and so it is likely that the Ordinance will regulate a broader range of data and system interference than the Convention's equivalent offences. Further, there is no requirement in the Crimes Ordinance that the system interference must seriously hinder the functioning of a computer – all that is necessary is that the system interference must cause a computer to function other than in accordance with the way it has been established to function. The Crimes Ordinance offence of damage to property is punishable by imprisonment for up to 10 years.

There does not appear to be a general prohibition on the misuse of devices in the Crimes Ordinance. However, it is an offence to possess anything with intent to destroy or damage property, and so the possession of devices that facilitate data or system interference will be covered. Contraventions of this provision can lead to imprisonment for up to 10 years.

Computer-related offences (Title 2 COE): Computer-related forgery, computer-related fraud

The Crimes Ordinance's general forgery offence applies to computer-facilitated conduct by virtue of its broad definition of "false instrument". The Ordinance's separate offence of making or possessing equipment for making a false instrument is also relevant. Both offences are punishable by imprisonment for 14 years.

There does not appear to be a general fraud offence in the Crimes Ordinance that applies to computer-facilitated conduct. However, some types of computer-related fraud will be covered by the Crimes Ordinance's offence of making a false entry in an organisation's books of account with intent to defraud. That offence is punishable by imprisonment for life. The Theft Ordinance (Cap. 210) contains a similar offence of false accounting that applies in respect of computer records. The Theft Ordinance offence is punishable by imprisonment for 10 years.

Ancillary liability (Title 5 COE): Attempt and aiding/abetting, corporate liability

In line with the Convention framework, those who aid or abet the commission of an offence are guilty of the same offence. Further, if a person does an act that is more than preparatory to the commission of an offence, then they are guilty are attempting to commit that offence and face the same punishment.

Corporate criminal liability is established in Hong Kong. In addition, the Criminal Procedure Ordinance (Cap. 221) provides for individual criminal liability for directors and other officers concerned in the management of the company in certain circumstances.

2.2 COMPUTER SECURITY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

At the date of writing, there are no upcoming legislative developments that relate to computer security.

2.3 PRIVACY LAWS – CURRENT LEGISLATIVE FRAMEWORK

Data protection

The Personal Data (Privacy) Ordinance (Cap. 486) establishes a data protection regime of general application to the private sector and Hong Kong (but not PRC) government agencies within the Special Administrative Region. The Ordinance applies in respect of "personal data" – data relating to a living individual from which it is practicable to ascertain the identity of the individual and that is in a form in which access or processing is practicable.

Based on the OECD guidelines, the Ordinance contains six data protection principles:

- **Principle 1 – Purpose and manner of collection:** This principle provides for the lawful and fair collection of personal data. It also sets out the information a data user must provide to a data subject when collecting personal data from that subject.
- **Principle 2 – Accuracy and duration of retention:** This principle provides that personal data should be accurate and kept no longer than is necessary for the purposes for which the data may be used.
- **Principle 3 – Use of personal data:** This principle restricts the use (which is defined to include the disclosure and transfer) of personal data to the purpose(s) for which it was collected or a directly related purpose, unless the data subject consents to the proposed use.
- **Principle 4 – Security of personal data:** This principle requires data users to take all practicable steps to secure personal data against unauthorised access, processing, erasure or other misuse.
- **Principle 5 – Information to be generally available:** This principle requires data users to make available information about its personal data policies and practices. Data users must also be open about the kinds of personal data they hold and the main purposes for which personal data are used.
- **Principle 6 – Access to personal data:** This principle confers upon data subjects the right to ascertain whether a data user holds his or her personal data, and to request access and correction of that data.

At the present time, there are no restrictions on transborder data flows out of Hong Kong. However, once section 33 of the Ordinance comes into force, there will be transborder restrictions on personal data that is (i) collected, held, processed or used in Hong Kong or

(ii) controlled by a data user whose principal place of business is in Hong Kong. It will not be possible to transfer this type of personal data outside Hong Kong unless: (a) the data user has reasonable grounds for believing that the destination country's laws are substantially similar to, or serve the same purpose as, the Personal Data (Privacy) Ordinance; (b) the data subject has consented in writing to the transfer; (c) the data user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not be dealt with in any manner which, if the destination country were Hong Kong, would be a contravention of the Ordinance; or (d) another of the exceptions in section 33 applies.

The Office of the Privacy Commissioner has issued several codes of conduct to provide guidance on compliance with the Ordinance's provisions: the Code of Practice on the Identity Card Number and other Personal Identifiers; the Code of Practice on Consumer Credit Data; the Code of Practice on Human Resource Management; and the Code of Practice on Protection of Customer Information for Fixed and Mobile Service Operators. These codes are subordinate to the Ordinance – non-compliance with a code does not necessarily render a data user liable to civil or criminal proceedings under the Ordinance.

Disputes in relation to the handling of personal data are often resolved among the parties themselves. However, the Ordinance does establish a complaints-based regime that serves as the principal avenue by which the Ordinance is enforced by the Office of the Privacy Commissioner. The Office has developed a complaint handling policy that describes how the Privacy Commissioner is likely to exercise his or her discretion at various points throughout the complaint-handling process, although these exercises of discretion remain subject to review by the Administrative Appeals Board. If a complaint is investigated, and the Commissioner reaches the opinion that a data user is contravening, or has contravened a requirement of the Ordinance and is likely to continue doing so, then the Commissioner may issue an enforcement notice directing the data user to take necessary steps to remedy the contravention. The Commissioner may also instigate a criminal prosecution against the data user in reliance on the Ordinance's criminal offence provisions (which do not apply to contravention of the Ordinance's data protection principles, but do apply to a failure to observe an enforcement notice). Aggrieved individuals can also seek redress by bringing civil proceedings against the data user responsible.

The Office of the Privacy Commissioner for Personal Data, Hong Kong, has an informative website at www.pco.org.hk in both English and Chinese.

Surveillance

Interception of Communications and Surveillance Ordinance

The Interception of Communications and Surveillance Ordinance 2006 (Cap. 589) prohibits public officers from directly or indirectly intercepting a communication transmitted via the postal service or a telecommunications system. There are a number of exceptions to this general prohibition. It does not apply to:

(i) an interception carried out pursuant to a prescribed authorisation under the Ordinance;

(ii) an interception of a telecommunication transmitted via radio unless the communication is transmitted as part of a service provided by a licensed public telecommunications provider; or

(iii) an interception that is authorised by another law.

The Ordinance also prohibits covert surveillance by public officers, except where the surveillance is carried out pursuant to a prescribed authorisation under the Ordinance.

The Ordinance does not prohibit intercepting communications or conducting covert surveillance by private individuals or organisations. However, to the extent that the interception involves the collection of personal information, the Personal Data (Privacy) Ordinance (Cap. 486) will apply.

Guidelines on personal data and workplace monitoring

The Privacy Commissioner has issued non-binding privacy guidelines for monitoring and personal data privacy at work after his Office rejected an earlier proposal to issue a code of practice on the subject. The guidelines neither support nor criticise employee monitoring. Instead, they provide guidance on how to assess whether employee monitoring is necessary, and how to manage personal data obtained in the course of employee monitoring.

Everyone in Hong Kong is required to carry and produce their identity card in certain circumstances. Issuing and use of the card is regulated by the Registration of Persons Ordinance (Cap. 177) and regulations and orders made under it.

Sensitive information

There is no special protection afforded to sensitive information, such as an individual's ethnic or racial origin, in the Personal Data (Privacy) Ordinance. However, those who deal with sensitive financial information are often subject to a duty of secrecy. For example, bankers are subject to a general duty of secrecy under the Banking Ordinance (Cap. 155) as are employees of the Inland Revenue Department (see Inland Review Ordinance (Cap. 112)).

4. Hong Kong

Miscellaneous

The Basic Law of the HKSAR contains several privacy protections: Article 29 protects against arbitrary or unlawful searches of a resident's home or other premises; and Article 30 protects the freedom and privacy of communications by residents of Hong Kong. In addition, Article 14 of the Hong Kong Bill of Rights Ordinance (Cap. 383) states that no person shall be subjected to "arbitrary or unlawful interference with his privacy, family, home or correspondence". Note, however, that the Bill of Rights Ordinance only binds the government and public authorities.

2.4 PRIVACY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

In 2007, the Privacy Commissioner announced that it had plans to amend the Code of Practice on Consumer Credit Data to better address how positive credit data is being used by credit providers and to redress some operational difficulties that exist in enforcing the Code.

2.5 SPAM LAWS – CURRENT LEGISLATIVE FRAMEWORK

Hong Kong's Unsolicited Electronic Messages Ordinance (Cap. 593) was enacted in May 2007. Most of the Ordinance's provisions, apart from Part 2, came into force on 1 June 2007. Part 2 of the Ordinance, which deals with sending, causing or attempting to send unsolicited electronic messages, will commence on 22 December 2007.

The Ordinance regulates all manner of electronic messages, including emails, faxes, SMS, MMS, and voice and multi-media messages generated by automated means (e.g. messages sent through interactive voice response (IVR) systems). It applies to messages that have a Hong Kong link, including those where the sender sent or the recipient receives the message while in Hong Kong, or where the sender is a Hong Kong company or organisation that carries on business in Hong Kong when the message is sent.

Part 2 of the Ordinance creates an opt-out regime for sending unsolicited commercial electronic messages. A commercial electronic message is an electronic message that is sent for the purpose of offering or advertising the supply of goods, services, facilities, land or an interest in land, or to promote or advertise a business or investment opportunity, among other things. Part 2 does not apply to a number of different types of transactional and pre-existing relationship messages, including messages with the primary purpose of:

- facilitating, completing or confirming a previously agreed commercial transaction;
- providing warranty, product recall, safety or security information for a commercial product or service;
- delivering goods or services, including product upgrades or updates that the recipient is entitled to receive under a transaction;
- providing notification of account information, a change in the terms or features of a product, or the recipient's status with respect to that product; or
- providing information in relation to an employment relationship or a related benefit plan in which the recipient is involved.

In addition, the provisions in Part 2 do not apply where a message was sent by mistake or where a person did not know, and could not with reasonable diligence have known, that the message contained a Hong Kong link.

Part 2 of the Ordinance provides that a person cannot send a commercial electronic message (i) without including accurate sender information, (ii) without a functional unsubscribe facility, (iii) with a misleading subject heading, (iv) that conceals the calling line identification number where the message is sent via telephone or fax, (v) to an address where an unsubscribe request was made more than 10 working days before the message was sent, or (vi) to an address on the do-not-call register which the Ordinance provides the Telecommunications Authority can, but is yet to, establish. Unsubscribe requests (or evidence of the contents thereof) must be kept by regulated entities for at least 3 years after receipt.

The Legislative Council has also promulgated regulations under Part 2 of the Ordinance which specify how sender contact information must be displayed, and the type of unsubscribe facilities that must be used, among other things. These regulations are expected to come into force at the same time as Part 2 of the Ordinance enters into force.

Where the Telecommunications Authority suspects that a person has contravened Part 2, it can issue a notice with details of the suspected contravention and specifying actions that the person should take to remedy the non-compliance. A person who does not comply with such a notice commits an offence and is liable for fines of up to HKD$500,000 (approximately USD$64,430) in addition to a daily fine of up to HKD$1,000 (approximately USD$130) for each day that the offence continues.

The Ordinance also contains a private right of action available to anyone who suffers any damage as a result of a contravention of the Ordinance. Claimants can recover compensatory damages as well as a range of other remedies including injunctions and declarations.

The Ordinance prohibits the supply of address harvesting software or a harvested address list for use in connection with, or to facilitate, the sending of commercial electronic messages. Offences also exist for acquiring, using or acquiring the right to use address harvesting software or harvested address lists, and sending an electronic message using automated means. All of these offences are

punishable by a maximum penalty of five years imprisonment and a fine of up to HKD$100,000 (approximately USD$12,890).

The most severe criminal penalties under the Ordinance are reserved for those who (i) send bulk messages by using a telecommunications device accessed without authorisation, (ii) send multiple messages with the intent of deceiving or misleading recipients as to the source of the message, (iii) falsify header information in multiple messages, (iv) obtain electronic addresses or domain names by submitting falsified identity information and use these addresses or domain names to send multiple commercial electronic messages, or (v) falsely represent they are the registrant of electronic addresses or domain names and send multiple commercial electronic messages from those addresses or domain names. Persons who commit any of these acts can be liable for 10 years imprisonment or a fine (maximum amount unspecified).

Under the Ordinance, where an act is engaged in by an employee in the course of their employment, this will be treated as an act that was also engaged in by the employer. So, in these situations, the employer will be liable for the acts of its employees, unless the employer can show it took the steps that were practicable to prevent the employee doing the relevant act in the course of their employment. This vicarious liability provision only applies to acts done in the course of an employee's employment and will not apply to rogue employees who use their employer's IT systems to send spam without authorisation, for example.

Other laws

To the extent that spam involves direct marketing, and an individual's email address is personal data, the Personal Data (Privacy) Ordinance may be relevant. Section 34 of that Ordinance prohibits the use of personal data for direct marketing unless (a) the subject has consented to use of his or her personal data for this purpose and (b) in the initial marketing contact, the recipient is informed of his or her right to 'opt-out'. Contraventions of this provision can be dealt with through the complaints regime discussed in section 3.3 above.

Hong Kong's Crimes and Telecommunications Ordinances, as well as the common law action of trespass to chattels, may also regulate spam activity in some circumstances.

Until the Ordinance comes into full force at the end of 2007, several industry codes of practice approved by the Office of the Telecommunications Authority will remain operational. These include the:

- Code of Practice on Handling Complaints about Inter-Operator Unsolicited Promotional Telephone Calls generated by Machines;
- Code of Practice on the Procedures for Handling Complaints against Senders of Unsolicited Fax Advertisements; and
- Code of Practice for Inter-Operator Short Message Service.

2.6 SPAM LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

The Unsolicited Electronic Messages Ordinance gives the Telecommunications Authority the power to issue and approve a Code of Practice to provide practical guidance on the operation of the Ordinance. In September 2007, the Telecommunications Authority released for public consultation and comment the Draft Code of Practice on Sending Commercial Electronic Messages under the Unsolicited Electronic Messages Ordinance. Submissions on the Draft Code of Practice were due in early October 2007. It is not known when the Code will be finalised or is expected to come into force.

2.7 ONLINE CHILD SAFETY LAWS – CURRENT LEGISLATIVE FRAMEWORK

General child pornography offences

The age of majority in Hong Kong is 18 years; the age of consent to sexual relations is 16 years.

Hong Kong's Prevention of Child Pornography Ordinance (Cap. 579) prohibits the production, mere possession, advertisement and publication of child pornography. The Ordinance's definition of child pornography is broad; it includes visual depictions of a person who is, or appears to be, a child (a person under the age of 16) engaged in explicit sexual conduct, as well as visual depictions of a child's sexual organs in a sexual manner or context. It is immaterial whether the depiction relates to a real person and so altered child pornography images and cartoons depicting child pornography are likely to fall within the ambit of the Ordinance. Contraventions of the Ordinance are punishable by fines of up to HKD$2 million (approximately USD$257,830) and imprisonment for up to 8 years.

The Crimes Ordinance prohibits the use, procurement or offer of persons under the age of 18 for making pornography or for live pornographic performances. Offenders are liable to a fine of up to HKD$3 million (approximately USD$386,750) and imprisonment for a term of up to 10 years depending on the age of the victim.

Computer-facilitated child pornography offences (Title 3 COE)

The Prevention of Child Pornography Ordinance also criminalises the computer-facilitated publication of child pornography by virtue of the definition of child pornography (which includes data stored in a form that is capable of conversion into a visual depiction) and the scope of the publication offence (which includes making a message or data available by means of an electronic transmission). Computer-facilitated possession of child pornography is also criminalised by the Ordinance. Offenders face the same penalties for computer-facilitated dealing in child pornography as they do for offline child pornography offences.

4. Hong Kong

Miscellaneous

In addition to the child pornography offences discussed above, the Control of Obscene and Indecent Articles Ordinance (Cap. 390) prohibits the publication of obscene material and restricts the availability of indecent material. Most forms of child pornography are likely to be considered indecent, if not obscene, under the Ordinance's classification scheme. It is an offence to publish indecent material to a juvenile (a person under the age of 18), and to publish obscene material or to possess or import obscene material for the purpose of publishing it. The indecent material offence is punishable by a fine of up to HKD$800,000 (approximately USD$103,140) and imprisonment for 12 months; the obscene material offence can attract a fine of up to HKD$1 million (approximately USD$128,920) and three years imprisonment.

The Code of Practice for Internet Computer Services Centres Operators was released in July 2003 by the Home Affairs Bureau. It obliges those who operate internet cafes and the like to use up-to-date devices to filter pornographic, violent or gambling content during the facility's business hours. In addition, operators must ensure that customers below the age of 18 are not permitted access to indecent material (as defined in the Control of Obscene and Indecent Articles Ordinance).

2.8 ONLINE CHILD SAFETY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

At the date of writing, there are no upcoming legislative developments that relate to online child safety.

Part 3 – Benchmark Comparison

Key: Favourable alignment | Moderate alignment | Weak alignment

(E)	Enacted
(E)*	Enacted but not yet in force
(P)	Pending
(Title [x])	Title [x] of the Council of Europe Convention on Cybercrime

Area	Legislative regime to be compared with benchmark	Benchmark legislation	Overall alignment	Areas of strong alignment	Areas of moderate alignment	Areas of weak alignment
Computer Security Laws	Crimes Ordinance (Cap. 200) (E); Telecommunications Ordinance (Cap. 106) (E); Theft Ordinance (Cap. 210) (E); Criminal Procedures Ordinance (Cap. 221) (E)	Council of Europe Convention on Cybercrime (Titles 1, 2 and 5)		• Data and system interference offences • Computer-related forgery offence • Ancillary liability for attempting, aiding or abetting cybercrimes	• Illegal access and misuse of devices offences • Computer-related fraud offence • No express provision for corporate criminal liability but this is established in Hong Kong law	• No illegal interception offence

Area	Legislative regime to be compared with benchmark	Benchmark legislation	Overall alignment	Areas of strong alignment	Areas of moderate alignment	Areas of weak alignment
Privacy Laws	Personal Data (Privacy) Ordinance (Cap. 486) (E)	Model Privacy Bill (drafted by Microsoft)		• Transparency matters that must be notified to data subjects (e.g. the purposes of use of the personal data and the data subjects' right to access and request correction of that data) • Requirement that information about a data user's privacy practices be made readily available and that certain matters therein must be notified to data subjects upon collection of personal data • Obligation to keep personal data free from loss or unauthorised use • Data subjects' right to access and correct personal data	• Definition of personal data • Mode of enforcement (enforcement by individual or Commissioner cf. enforcement by Commissioner or State official) • Consequence of infringement (civil and criminal liability cf. statutory and civil liability)	• Different approach as to what constitutes a primary or secondary purpose of use • "Use" of personal data includes disclosure or transfer of the data • No protected disclosures to affiliates with common privacy practices unless this use is within primary purpose of collection or directly related thereto • No separate regulation of sensitive information • Restrictions on transborder data flows (although these are not in force yet) • No breach notification provisions
Spam Laws	Unsolicited Electronic Messages Ordinance (Cap. 593) (E)	Anti-spam legislation checklist (drafted by Microsoft)		• 'Opt-out' regime • Transparency requirements (functional unsubscribe facility, accurate sender information) • Exclusion of messages relating to pre-existing business relationships from Part 2 of the Ordinance, which contains the rules for sending commercial electronic messages	• Definition of unsolicited electronic message • Remedies for infringing conduct (enforcement notices, civil damages and criminal sanctions)	• Originating requirements for unsolicited electronic messages to be subject to the proposed framework • No ISP safe harbour for transmitting infringing messages • Private right of action for all persons affected by spam (and not just ISPs/email service providers) • Obligation to retain unsubscribe requests for 3 years after receipt
Online Child Safety Laws	Prevention of Child Pornography Ordinance (E); Crimes Ordinance (E)	Council of Europe Convention on Cybercrime (Title 3 COE)/ICMEC principles		• Definition of child pornography • General child pornography offences • Mere possession of child pornography is prohibited	• Some forms of computer-facilitated dealing in child pornography are criminalised	• No scope for ISP reporting of dealing in child pornography

Last Updated: 24 October 2007

5. India

Part 1 – Snapshot of Legislative Status

Key: (E) Enacted
(P) Pending
(Title [x] COE) Title [x] of the Council of Europe Convention on Cybercrime (COE)

Area	Topic	Enacted legislation	Pending legislation	Relevant instruments/Comments
Computer Security Laws	**Core offences (Title 1 COE):** illegal access, illegal interception, data interference, system interference, misuse of devices	✓	✓	Information Technology Act, 2000 (E) but prohibited activities mainly attract civil liability only. Information Technology (Amendment) Bill, 2006 (P)
	Computer-related offences (Title 2 COE): computer-related forgery, computer-related fraud	✓	✓	Information Technology Act, 2000 (E) but prohibited activities mainly attract civil liability only. Information Technology (Amendment) Bill, 2006 (P); Concurrent amendments to the Indian Penal Code (P)
	Ancillary liability (Title 5 COE): attempt and aiding/ abetting, corporate liability	✓	✓	Information Technology Act, 2000 (E) Information Technology (Amendment) Bill, 2006 (P)
Privacy Laws	**Data protection**	✗	✓	No comprehensive data protection legislation as yet. However, some of the provisions proposed in the Information Technology (Amendment) Bill, 2006 (P) relate to data protection.
	Surveillance (see illegal interception under computer security)	✓	✓	Telegraph Act, 1885 (E); Information Technology (Amendment) Bill, 2006 (P)
	Sensitive information	✗	✓	Information Technology (Amendment) Bill, 2006 (P)
Spam Laws	**Anti-spam regulation**	✗	✓	No comprehensive spam legislation as yet. However, some of the provisions proposed in the Information Technology Amendment Bill, 2006 (P) could be used to impose liability on those who send certain types of spam.
Online Child Safety Laws	**General child pornography offences**	✗	✗	No general child pornography legislation, but it is an offence to distribute obscene material (Indian Penal Code, 1860 (E), Young Persons (Harmful Publication) Act, 1951 (E)), profit from a person's involvement in prostitution (Immoral Traffic (Prevention) Act, 1956 (E)) or make an indecent representation of a woman (Indecent Representation of Women (Prohibition) Act, 1986 (E))
	Computer-facilitated child pornography offences (Title 3 COE)	✗	✓	Information Technology Act, 2000 (E) prohibits the computer-aided dissemination of obscene material, but not child pornography material in particular. Information Technology (Amendment) Bill, 2006 (P)

Part 2 – Legal and Regulatory Position

2.1 COMPUTER SECURITY LAWS – CURRENT LEGISLATIVE FRAMEWORK

The Information Technology Act, 2000 (IT Act) is the primary piece of computer security legislation in India. In December 2006, the Information Technology (Amendment) Bill, 2006 (IT Amendment Bill) was introduced into Parliament to amend the IT Act. The Bill was subsequently referred by Parliament to the Standing Committee on Information Technology (Standing Committee), which submitted its report to Parliament in September 2007 outlining its views and recommendations on the IT Amendment Bill. It is expected that the government will reintroduce a revised version of the IT Amendment Bill after taking into consideration the Standing Committee's report and feedback from other stakeholders such as trade associations. It is not known when these further amendments will be finalised and when the Bill will be resubmitted to Parliament but the earliest possibility is November 2007.

Core offences (Title 1 COE): Illegal access, illegal interception, data interference, system interference, misuse of devices

While section 43 of the IT Act prohibits many of the activities that constitute core offences under the Convention on Cybercrime, the

IT Act does not, for the most part, criminalise these activities – it merely provides for significant civil liability in damages (of up to INR 10 million [approximately USD$252,210] at the suit of the person affected by the infringing conduct). The absence of criminal liability for offences relating to illegal interception, system interference, misuse of devices, and most forms of illegal access is a well-recognised weakness of the Indian legislation and there have been calls for reform to address these deficiencies. The activities which attract civil liability under the IT Act include:

- unauthorised access to a computer, computer system or network;
- unauthorised introduction of computer viruses onto a computer, computer system or network;
- unauthorised damage to a computer, computer system or network as well as data or software;
- unauthorised disruption of a computer, computer system or network; and
- unauthorised denial of access to a computer, computer system or network.

In terms of criminal liability under the IT Act, section 70 establishes an offence in respect of unauthorised access to computer systems. However, that section is restricted in its operation to systems which are declared by an appropriate government (the central government as well as any of the state governments can qualify as an 'appropriate government') to be a "protected system" and such system need not necessarily be a government system per se. At the date of writing, no systems appear to have been declared as such.

There is no specific provision in the IT Act that imposes liability on those who illegally intercept data.

Section 66 of the IT Act also makes it a criminal offence to interfere with data residing on a computer resource. The drafting of this offence is comparable to the data interference offence found in the Convention on Cybercrime and in practical terms, section 66 is likely to cover the introduction of viruses that manipulate data, but not denial of service attacks (since this latter method of system interference does not typically damage or interfere with data). Offenders under section 66 can be punished with a term of imprisonment of up to 3 years or with a fine of up to two lakh rupees (approximately USD$5,040) or both.

Computer-related offences (Title 2 COE): Computer-related forgery, computer-related fraud

Computer-related fraud and forgery are both covered by the civil liability sections of the IT Act. These activities may also attract criminal liability under section 66 of the IT Act if the defrauder has the requisite intention and his or her activities interfere with data.

Ancillary liability (Title 5 COE): Attempt and aiding/abetting, corporate liability

Although there are no pre-emptive legal provisions in the IT Act to address situations where an offence has not yet been committed, there is scope for civil liability where a person provides assistance to another to facilitate unauthorised access to a computer system or network. Corporate liability under the IT Act is particularly onerous for CEOs and other high-ranking officers – liability for corporate contraventions of the Act is imposed on those in charge of the company unless those persons can prove that the contravention took place without their knowledge (and they were not negligent) or that they exercised all due diligence to prevent the contravention in question (and they did not tacitly consent to its commission). The practical implications of this section caused an international stir in December 2004 when the then CEO of eBay India (known as Baazee at the time) was arrested and imprisoned for four days for enlisting an objectionable video clip on its site.

2.2 COMPUTER SECURITY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

Core offences (Title 1 COE): Illegal access, illegal interception, data interference, system interference, misuse of devices

The IT Amendment Bill proposes to criminalise the acts set forth in section 43 where they are done "dishonestly or fraudulently". These new offences would replace the existing 'hacking' offence in section 66 of the IT Act and would be punishable by up to two years imprisonment and/or a fine of 5 lakh rupee (approximately USD$12,620). While the enactment of these proposed offences would have the effect of bringing the IT Act more into line with the Convention on Cybercrime, the requisite mental element – "dishonestly or fraudulently" – attaching to these offences means that the majority of the proposed offences will apply much more narrowly than their Convention counterparts. This is because the Convention only permits the mental element of "dishonest intent" in respect of its illegal access and illegal interception offences, and not in respect of the other core offences set forth in Title 1 of the Convention.

The proposed criminalisation of the acts set forth in section 43 does not disturb the existing civil liability that those acts attract. In other words, if the IT Amendment Bill is enacted in its current form, the acts set forth in section 43 will continue to attract civil liability; it will only be where those acts are committed dishonestly or fraudulently that they will also attract criminal liability.

The IT Amendment Bill also proposes to extend section 43 to regulate anyone who, without permission of the owner of a computer system, destroys, deletes or alters "any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means" (see proposed paragraph

(i) of section 43). This provision could be used to apply to those who, without authorisation, modify or destroy computer data (e.g. hacking) or to acts which do not involve the modification of data but still interfere with a computer system (e.g. denial of service attacks).

The Standing Committee has made a number of recommendations in respect of the core offences proposed in the IT Amendment Bill. These include that:

- due to their serious consequences, the majority of the acts set forth in existing section 43 of the IT Act should only attract criminal liability and not civil liability. The acts of unauthorised access to a computer, computer system or network, and unauthorised downloading of data should only attract civil liability under existing section 43;
- the terms "dishonestly" or "fraudulently" should be defined within the IT Act by reference to the cybercrime context; and
- the hacking offence in existing section 66 of the IT Act should be retained.

Unlike the Cybercrime Convention, the IT Amendment Bill does not contain any provisions that address the misuse of devices.

Computer-related offences (Title 2 COE)

The IT Amendment Bill does not contain any offences that are equivalent to the computer-related fraud and forgery offences in the Cybercrime Convention. However, the Bill does contemplate the enactment of identity theft offences in the Indian Penal Code. It is proposed to make it an offence to (i) "cheat" by using an electronic signature or other unique personal identifier (maximum penalty: two years imprisonment and a fine (amount unspecified), and (ii) use a communication device or computer resource to "cheat" by impersonating another person (maximum penalty: five years imprisonment and a fine (amount unspecified)). These offences are much narrower in scope than the computer-related fraud and forgery offences in Title 2 of the Cybercrime Convention.

Ancillary liability (Title 5 COE): Attempt and aiding/abetting, corporate liability

The onerous corporate liability position under the enacted IT Act is not changed by the IT Amendment Bill.

Miscellaneous

Service provider safe harbour

The IT Amendment Bill rewrites the existing safe harbour for network service providers in section 79 of the IT Act. The terms of proposed section 79 are controversial and certain elements of industry are seeking substantial amendments.

2.3 PRIVACY LAWS – CURRENT LEGISLATIVE FRAMEWORK

Data protection

India does not have any specific data protection legislation. However, under the Special Relief Act, 1963, temporary and permanent injunctions can be obtained to prevent the unauthorised disclosure of confidential information and damages can be obtained if unauthorised disclosure results. There is also recognition of constitutional and tortious rights of privacy, although India's constitutional right to privacy is enforceable only against the State and not against private individuals.

Surveillance

The Telegraph Act, 1885 regulates the surveillance of communications in India and covers methods such as wiretapping and the interception of personal mail. Supplementing this legislative regime, the Supreme Court has laid down restrictive guidelines on when and how the government may engage in wiretapping: only the Union Home Secretary or his or her state counterpart can issue an order for a tap and the government is required to show that the information sought cannot be obtained through any other means. Although tapped phone calls are not accepted as primary evidence in Indian courts, the practice of wiretapping is not uncommon and Privacy International has observed that there continues to be a gap between the regime established by the Telegraph Act and its enforcement.

Sensitive information

India does not have any general legislation that addresses sensitive information. However, the Telecom Regulatory Authority of India (Access to Information) Regulations, 2005 cover access by the telecommunications regulator and service providers to information held by service providers about interconnection issues. Under regulation 6, service providers are exempted from furnishing commercially or financially sensitive information if disclosure of this information is likely to cause unfair gain or unfair loss to the service provider so as to compromise its competitive position.

2.4 PRIVACY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

Data protection

The IT Amendment Bill proposes the enactment of a criminal offence that applies where a person, including an intermediary, discloses personal information that has been accessed in the course of providing services under the terms of a lawful contract, where that disclosure is made (i) without the consent of the data subject or in breach of a lawful contract, and (ii) with intent to cause, or knowing that the disclosure is likely to cause, wrongful loss or wrongful gain. This offence is punishable by imprisonment for up to two years, a fine of up to two lakh rupees (approximately USD$5,040) or both.

The concept of 'personal information' is not defined in the Bill.

In commenting on this new offence, the Standing Committee urged the Department of Information Technology to consider whether service providers should be required to maintain subscriber and log data (including 'traffic data' within the meaning of the Cybercrime Convention) for law enforcement purposes.

The Standing Committee also recommended that India enact data retention and data protection provisions (ostensibly extending to the protection of citizen data) as part of the amendments to the IT Act. The report notes that the Department of Information Technology, which is responsible for overseeing drafting of the IT Amendment Bill, supports the introduction of provisions that protect the privacy of individuals.

The Standing Committee has also suggested the introduction of specific provisions in the IT Amendment Bill that impose punitive measures on the recipients of stolen data. This suggestion appears to be a response to recent data leaks in India that have arisen in the outsourcing context.

Self-regulatory organization for data protection

In 2007, NASSCOM (National Association of Software and Service Companies) announced that it would establish an independent data privacy organization, the Data Security Council of India (DSCI), to oversee the data protection practices of India's IT industry and develop frameworks, best practices, audit and capacity building. Further details as to the nature of the Data Security Council of India's activities, and the timeframe for its establishment, are not available at the time of writing. The Center for Information Policy Leadership and the United States India Business Council have provided some guidance to DSCI and urged it to develop a 4-phase developmental plan focused on light-touch regulation and developing a flexible yet benchmarkable framework to assist its membership as well as overseas clients. The basic premise of this developmental plan is that data protection obligations must flow alongside the data flow even in the cross-border scenario.

Surveillance

The IT Amendment Bill proposes to require subscribers, intermediaries or any person in charge of a computer resource to "extend all facilities and technical assistance" to an agency acting under an order to intercept electronic communications to (i) provide the agency with access to the computer resource containing the information, (ii) intercept, monitor or decrypt the information, and/or (iii) provide the information contained in a computer resource to an agency. A failure to assist an agency in this manner is punishable by a term of up to seven years imprisonment. There is no immunity offered to those who assist an agency in accordance with this proposed section.

In 2001, the Indian government introduced a significant piece of legislation – the Communications Convergence Bill, 2001 – to create a "super regulator", namely, the Communications Commission of India (similar to the United States' Federal Communications Commission and the United Kingdom's Office of Communications [Ofcom]), to oversee all voice and data (including telecom, broadcasting and internet) communications licensing as well as regulation. The Bill also proposed to repeal the Indian Telegraph Act, 1885 and establish a new offence for the unlawful interception of communications. Although several drafts of the proposed legislation have been prepared, this Bill has lapsed, and of late, no renewed efforts are being taken to revive this concept.

Sensitive information

Proposed section 43A of the IT Amendment Bill provides a basis for civil liability in damages if a body corporate is negligent in implementing and maintaining reasonable security practices and measures in respect of sensitive personal data or information it possesses or handles, and that negligence causes wrongful loss or wrongful gain to any person. Bodies corporate can be liable in damages for up to five crore rupees (approximately USD$1.26 million).

The scope of proposed section 43A turns on the definitions of its key concepts:

- "Sensitive personal data or information" is defined as any personal information that may be prescribed by the government in consultation with professional bodies as it deems fit;
- "Reasonable security practices and measures" is defined to include security measures designed to protect sensitive personal data or information from unauthorised access, use or modification which may be specified in an agreement between the parties or in the absence of any such agreement, may be (i) specified by law or (ii) proscribed by the government in consultation with professional bodies; and
- the terms "wrongful loss" and "wrongful gain" are taken from the Penal Code, but the Standing Committee has urged the Department of Information Technology to expressly define these terms in the IT Act by reference to the information technology context in which they will be applied.

Miscellaneous

The IT Amendment Bill also proposes an amendment to the Penal Code to create an offence where a person intentionally or knowingly captures, publishes or transmits an image of the private areas of a person without that person's consent and in circumstances violating the privacy of that person (maximum penalty: two years imprisonment and/or a fine not exceeding two lakh rupees [approximately USD$5,040]).

5. India

2.5 SPAM LAWS – CURRENT LEGISLATIVE FRAMEWORK

India does not have any spam legislation.

2.6 SPAM LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

Two sections in the IT Amendment Bill could be applied in certain circumstances to impose liability on those who send certain limited types of spam. The first of these sections is proposed sub-section 43(i), which applies to persons who, without permission of the owner of a computer system, destroy, delete or alter "any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means". Proposed sub-section 43(i) will ordinarily attract civil liability in damages of up to one crore rupee (approximately USD$252,210). However, where the acts in sub-section 43(i) are committed dishonestly or fraudulently, the perpetrator will have committed an offence punishable by up to two years imprisonment and/or a fine of 5 lakh rupee (approximately USD$12,620).

The second spam-related provision in the IT Amendment Bill is proposed section 66A, which criminalises the act of sending via persistent use of a computer resource or communication device content that (i) is grossly offensive, (ii) has a menacing character, or (iii) they know to be false and the message is sent for the purpose of causing, among other things, annoyance, inconvenience, obstruction, insult, injury, hatred or ill will. This offence is punishable by up to two years imprisonment and a fine, the amount of which is unspecified.

In its report on the IT Amendment Bill, the Standing Committee rejects the Department of Information Technology's submission that these provisions constitute a sufficient response to the problem of spam. The Committee instead recommends the enactment of specific provisions to impose liability on those who send spam.

2.7 ONLINE CHILD SAFETY LAWS – CURRENT LEGISLATIVE FRAMEWORK

General child pornography offences

The age of majority in India is 18 years; the age of consent to sexual relations is generally 16 years.

India has not enacted specific legislation to combat child pornography. Instead, child pornography falls under a general ban on obscene material in the Indian Penal Code, 1860. Obscene material is defined broadly – it appears to include digitally stored material – and the Code only prohibits the distribution (and not possession) of such materials. Distribution of obscene material is punishable by a fine and imprisonment for up to two years and there is provision for lengthier terms of imprisonment where the obscene material is distributed to a minor (a person under 18 years of age). This offence is also mirrored in the Young Persons (Harmful Publication) Act, 1951. Under section 367 of the Penal Code it is also an offence to bring a girl under 21 years of age into a situation with the intention or awareness that it is likely that the girl may be forced or seduced to have intercourse with another person.

Under the Immoral Traffic (Prevention) Act, 1956 it is illegal to procure, cause or induce a person to engage in prostitution or to profit from someone's engagement in prostitution. Although this law is targeted at landlords, owners and lessees of brothels, it may have broader applications including online solicitation. The penalty for inducing someone to engage in prostitution is imprisonment for seven years, up to life if the victim is a child (a person under the age of 16), and between seven and 14 years if the victim is a minor (a person between the ages of 16 and 18).

Finally, the Indecent Representation of Women (Prohibition) Act, 1986 prohibits indecent representations of women in any form including advertisements, publications, writings, paintings or figures. It is likely that girls would be included in the undefined term "women" that is used in the Act. Contraventions of this Act are punishable with up to two years imprisonment and a maximum fine of two thousand rupees (approximately USD$50).

Computer-facilitated child pornography offences (Title 3 COE)

The IT Act prohibits the electronic publication or transmission of "material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons". Offenders may be subject to between five and 10 years imprisonment and a fine of between one to two lakh rupee (approximately USD$2,520 to USD$5,040). There is a limited safe harbour for network service providers (see section 2.2 previous).

2.8 ONLINE CHILD SAFETY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

General child pornography offences

In 2005, a group of ministers was asked to look at a proposed amendment to the Immoral Traffic (Prevention) Act, 1956 to strengthen the law by recommending stringent punishment to hold the traffickers and patrons who partake in the services or sexual exploitation of trafficking victims through both significant fines and potential imprisonment. The amendments also propose an increase in the age of a "child' from 16 to 18 years to bring it on a par with other laws. Enhancement of punishment was also recommended for keeping, managing or assisting in the running of a brothel with up to three-year rigorous imprisonment on first conviction and seven years for a subsequent offence.

Computer-facilitated child pornography offences (Title 3 COE)

The IT Amendment Bill does not contain any computer-facilitated child pornography offences. However, previous drafts of legislation to amend the IT Act did criminalise publishing and transmitting child pornography through electronic communications. The Standing Committee has recommended that the IT Amendment Bill be amended to include specific provisions to address computer-facilitated dealings with child pornography in line with Article 9 of the Cybercrime Convention.

The IT Amendment Bill also proposes amendments to the IT Act's existing electronic transmission offence discussed earlier in section 2.7. These amendments ensure that the provision applies to those who cause the transmission of material prohibited by the section (in addition to persons who actually transmit the offending material), and reduces the penalties applicable to offenders to between two and five years imprisonment and a fine of between 5 to 10 lakh rupees (approximately USD$12,620 to USD$25,230).

The IT Amendment Bill also proposes the introduction of a new section to the IT Act which would impose a term of up to seven years imprisonment and a fine of up to 10 lakh rupees (approximately USD$25,230) on those who publish, transmit or cause to be published or transmitted material which contains a sexually explicit act or conduct. This provision does not apply where the publication can be justified as being for the public good on the grounds that it is in the interest of science, art, literature or learning or it is kept for use for religious purposes. To the extent that this exception does not apply, the ambit of this provision is broad enough to cover material that would be considered child pornography. Nevertheless, the Standing Committee has recommended that this provision be amended to specifically refer to child pornography, and to criminalise computer-facilitated dealings with child pornography in accordance with Article 9 of the Convention on Cybercrime.

Miscellaneous

There are no specific provisions in the IT Amendment Bill that address online grooming. However, the Standing Committee has recommended that the IT Amendment Bill be amended to criminalise online grooming, and the Department of Information Technology appears inclined to implement this recommendation.

5. India

Part 3 – Benchmark Comparison

Key: Favourable alignment | Moderate alignment | Weak alignment

(E) Enacted
(P) Pending
(Title [x]) Title [x] of the Council of Europe Convention on Cybercrime (COE)

Area	Legislation to be compared with benchmark	Benchmark legislation	Overall alignment	Areas of strong alignment	Areas of moderate alignment	Areas of weak alignment
Computer Security Laws	Information Technology Act, 2000 (E)	Council of Europe Convention on Cybercrime (Titles 1, 2 and 5)		• Data interference offence	• Liability for some types of aiding and abetting but only civil • Illegal access offence (but note its narrow application)	• No illegal interception, system interference, computer-related fraud and forgery, or misuse of device offences • No attempt offences • Onerous corporate liability provisions • Limited safe harbour for network service providers
	Information Technology (Amendment) Bill, 2006 (P)	Council of Europe Convention on Cybercrime (Titles 1, 2 and 5)			• Illegal access, data interference and system interference offences (but note the restrictive mental element – "dishonestly or fraudulently")	• No illegal interception, computer-related fraud and forgery, or misuse of device offences • Intention to commit offence may be sufficient to attract civil liability (as opposed to attempt) • Onerous corporate liability provisions • Limited safe harbour for network service providers
Privacy Laws	There is no enacted or pending comprehensive data protection legislation in India upon which a benchmarking analysis can be conducted.					
Spam Laws	There is no enacted or pending comprehensive spam legislation in India upon which a benchmarking analysis can be conducted.					
Online Child Safety Laws	Indian Penal Code, 1860 (E) Young Persons (Harmful Publication) Act, 1951 (E) Information Technology Act, 2000 (E)	Council of Europe Convention on Cybercrime (Title 3 COE)/ICMEC principles			• Criminal sanctions for distributing, transmitting and making available obscene material electronically	• No legislation specific to child pornography • No definition of child pornography • No computer-facilitated child pornography offences • No scope for ISP reporting of dealing in child pornography
	Information Technology (Amendment) Bill, 2006 (P)	Council of Europe Convention on Cybercrime (Title 3 COE)/ICMEC principles			• Criminal sanctions for distributing, transmitting and making available obscene material electronically	• No legislation specific to child pornography • No definition of child pornography • No computer-facilitated child pornography offences • No scope for ISP reporting of dealing in child pornography

6. Indonesia

Part 1 – Snapshot of Legislative Status

Key: (E) Enacted
(P) Pending
(Title [x] COE) Title [x] of the Council of Europe Convention on Cybercrime (COE)

Area	Topic	Enacted legislation	Pending legislation	Relevant instruments/Comments
Computer Security Laws	**Core offences (Title 1 COE):** illegal access, illegal interception, data interference, system interference, misuse of devices	✓	✓	Criminal Code (E); Telecommunications Law (E); Law No. 30 of 2000 regarding Trade Secret (E) Bill on Electronic Information and Transaction (P)
	Computer-related offences (Title 2 COE): computer-related forgery, computer-related fraud	✓	✓	Criminal Code (E) Bill on Electronic Information and Transaction (P)
	Ancillary liability (Title 5 COE): attempt; aiding/abetting, corporate liability	✓	✗	Criminal Code (E); Anti-Corruption Law (E); Economic Criminal Law (E); Environmental Law (E)
Privacy Laws	**Data protection**	✗	✓	Bill on Electronic Information and Transaction (P)
	Surveillance (see illegal interception under computer security)	✓	✗	Criminal Procedure Law (E)
	Sensitive information	✓	✓	Law of the Republic of Indonesia No. 6/1963 (E); Law of the Republic of Indonesia No. 18/2003 (E); Telecommunications Law (E); Law of the Republic of Indonesia No. 7/1992 (E); Criminal Code (E); Human Rights Law (E) Draft Law on Freedom of Obtaining Public Information (P)
Spam Laws	**Anti-spam regulation**	✗	Partial	The Bill on Electronic Information and Transaction (P) does not regulate the sending of spam messages per se, but contains a provision that regulates the content of commercial electronic messages which would also apply to spam.
Online Child Safety Laws	**General child pornography offences**	✗	✓	No general child pornography offences, but Indonesia's Criminal Code (E) contains obscenity provisions. Sexual exploitation of a child for gain, and indecent behaviour with a child, are also criminalised (Child Protection Act (E)). Draft Law on the Act Concerning Anti-Pornography and Porno-Action (P)
	Computer-facilitated child pornography offences (Title 3 COE)	✗	✓	Draft Law on the Act Concerning Anti-Pornography and Porno-Action (P); Bill on Electronic Information and Transaction (P)

Part 2 – Legal and Regulatory Position

2.1 COMPUTER SECURITY LAWS – CURRENT LEGISLATIVE FRAMEWORK

Indonesia has not enacted specific computer security laws. However, general provisions in Indonesia's Criminal Code and the Telecommunications Law may provide some recourse for those affected by cybercrimes.

Core offences (Title 1 COE): Illegal access, illegal interception, data interference, system interference, misuse of devices

The broad principle in Article 489 of the Criminal Code that "any mischief resulting in a loss or difficulty to another person is punishable as a misdemeanour" can potentially be used to sanction the acts prohibited by the Convention on Cybercrime's core offences. More specifically, Article 22 of the Law No 36 of 1999 regarding Telecommunication (Telecommunications Law) prohibits unauthorised or unlawful access to a telecommunications network or service. This latter offence is punishable by imprisonment for up to six years, a fine of up to IDR 600 million (approximately USD$66,170) or both. Illegal access to data may be punishable under the Trade Secret Law in which case offenders will be liable to imprisonment

for up to two years and/or a fine of up to IDR 300 million (approximately USD$33,090).

If data is considered a form of property under the Criminal Code, then data and system interference may be punishable under Article 406. This Article stipulates that a person who either intentionally or without authorisation destroys, damages or loses another's property is liable to imprisonment for a term of up to two years and eight months, or a fine. Although the Code's maximum fine in respect of this offence is set at IDR4,500 (approximately USD$0.50), it is understood that Criminal Code judges routinely hand down fines that exceed this limit.

Computer-related offences (Title 2 COE): Computer-related forgery, computer-related fraud

Once again, the broad principle in Article 489 of the Criminal Code that "any mischief resulting in a loss or difficulty to another person is punishable as a misdemeanour" could be used to sanction acts that amount to computer-related forgery and computer-related fraud under the Convention.

In principle, Indonesia's general forgery and fraud offences are capable of application to computer-related forgery or fraud.

Ancillary liability (Title 5 COE): Attempt and aiding/abetting, corporate liability

Attempts to commit a criminal offence are punishable for all offences in the Criminal Code unless this type of liability is expressly excluded. However, attempts to commit a misdemeanour are not punishable. Those who aid or abet the commission of a crime under the Criminal Code are also liable to punishment.

Although the Criminal Code does not expressly address corporate criminal liability, other Indonesian legislation does. In particular, corporate criminal liability is provided for under Law No 31 of 1999 regarding Anti Corruption, Law No 7 of 1955 regarding Economic Criminal Crimes and Law No 23 of 1997 regarding Environmental Management. Violations of these laws are subject to criminal and civil sanctions.

2.2 COMPUTER SECURITY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

As at April 2007, the Bill on Electronic Information and Transaction (EIT Bill) was being considered by the House of Representatives. It is believed that the Indonesian government is considering amending the EIT Bill to more closely align it with the Council of Europe's Convention on Cybercrime (Cybercrime Convention). It is unknown when the EIT Bill is expected to be finalised or enacted.

None of the computer security offences in the EIT Bill expressly require the acts that they prohibit to be committed intentionally. By contrast, it is an element of all of the offences in the Cybercrime Convention that the prohibited acts be committed intentionally.

Core offences (Title 1 COE): Illegal access, illegal interception, data interference, system interference, misuse of devices

Article 27 of the EIT Bill provides that a person is prohibited from using or having access to a computer or electronic system without right to obtain, change, damage or delete information in that system (maximum penalty: four years imprisonment and/or a fine of IDR 1 billion (approximately USD$109,490)). The terms of Article 27 appear to present an additional evidentiary hurdle for prosecutors when compared to the Convention's basic illegal access offence – under Article 27, it must be shown that a person accessed a computer without right to obtain, change, damage or delete information in that system, whereas under the Convention, mere illegal access is criminalised. Persons who contravene Article 27 of the EIT Bill are liable to more serious penalties where the information they seek to obtain or interfere with belongs to the government or relates to national defence or international relations. It is also worth mentioning that Article 30(1) of the EIT Bill contains an illegal access offence that reflects the Convention requirements (i.e. it criminalises mere access to a computer without right), but this offence only applies to information contained in a protected government computer system.

The EIT Bill does not appear to include an illegal interception offence of the kind contemplated in the Convention.

Article 28 of the EIT Bill prohibits persons from performing any act without right that would cause damage to the transmission of a government-protected program, code, instruction or information stored on a computer or an electronic system. Offenders are liable to imprisonment for up to 8 years and a fine of up to IDR 2 billion (approximately USD$218,960). In addition, paragraphs (2) and (3) of Article 30 prohibit the unauthorised use of, and/or access to, a protected government or public computer or electronic system where that use or access causes the computer or electronic system to be "managed" (maximum penalty: eight years imprisonment and a fine of up to IDR 2 billion (approximately USD$218,960)). It is unclear what would constitute management of a computer or electronic system, but it is possible that this offence will cover some instances of system interference. Under Article 30(4), it is also an offence to affect or cause a disturbance to a computer or electronic system used by the government (maximum penalty: eight years imprisonment and/or a fine of up to IDR 2 billion (approximately USD$218,960).

Setting aside the narrow application of Articles 28 and 30(2) – (4) to public sector computers or electronic systems, these offences broadly equate to the Convention's system interference offence.

The Cybercrime Convention's data interference offence provides that it is an offence to damage, delete, deteriorate, alter or suppress computer data without right. Many of these prohibited acts are

reflected in the EIT Bill which provides that it is an offence to damage, delete or change information in a computer or electronic system. This offence is punishable by imprisonment for up to four years and a fine of up to IDR 1 billion (approximately USD$109,490). Offenders are liable to more serious penalties where the data they seek to obtain or interfere with belongs to the government or relates to national defence or international relations.

Article 33 of the EIT Bill implements the Convention's misuse of device offence insofar as it criminalises the distribution of passwords and similar information to gain unauthorised access to the computer or electronic systems of the Central Bank, banking, financial and commercial institutions, and protected government systems. Offenders are liable to imprisonment for up to eight years (in the case of protected government systems) and 10 years (in all other cases), as well as a fine of up to IDR 2 billion (approximately USD$218,960).

Computer-related offences (Title 2 COE): Computer-related forgery, computer-related fraud

The EIT Bill does not contain offences that criminalise computer-related forgery and fraud in the manner that they are dealt with in the Cybercrime Convention. However, there are some offences in the EIT Bill which are narrower in application that deal with particular instances of computer-related fraud. For example, it is an offence to, without right or authority, use or have access to a computer or electronic system of the Central Bank or a banking or financial institution, and abuse or profit from this access. This offence could cover computer-facilitated credit card fraud and the fraudulent use of the computer or electronic systems of the Central Bank or banking and financial institutions. This offence is punishable by imprisonment for up to 10 years and a fine of IDR 2 billion (approximately USD$218,960).

Ancillary liability (Title 5 COE): Attempt and aiding/abetting, corporate liability

Ancillary liability and corporate criminal liability for the commission of computer crimes do not appear to be expressly addressed in the EIT Bill.

2.3 PRIVACY LAWS – CURRENT LEGISLATIVE FRAMEWORK

Data protection

There is no specific data protection legislation in Indonesia. However, if data is considered to be protected data or information under the Trade Secret Law, then any unauthorised use of that data or information is a contravention of the Trade Secret Law; offenders are liable to imprisonment for up to 2 years and/or a fine of up to IDR 300 million (approximately USD$32,870).

Surveillance

Under the Criminal Procedure Law, police officers must obtain a warrant to intercept mail and other communications transmitted by the postal service or other telecommunication networks. The contents of communications intercepted pursuant to the Criminal Procedure Law must be kept secret.

Sensitive information

The laws of Indonesia do not appear to afford special protection to sensitive information such as an individual's ethnic or racial origin. However, there is some protection for information disclosed in sensitive contexts: doctors are required to maintain doctor-patient confidentiality (Law of the Republic of Indonesia No. 6/1963); lawyers are required to maintain solicitor-client confidentiality (Law of the Republic of Indonesia No. 18/2003); telecommunications service providers are required to maintain the confidentiality of all information transmitted to, or received by, their subscribers (Telecommunications Law); and bankers are obliged to secure the confidentiality of their customers' data (Law of the Republic of Indonesia No. 7/1992). In addition, Indonesia's Criminal Code prohibits the intentional disclosure of confidential information obtained in the course of employment and Indonesia's Human Rights Law protects the secrecy of personal correspondence.

2.4 PRIVACY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

Data protection

The EIT Bill does not contain a comprehensive data protection regime. However, it does afford Indonesians some control over the use of their personal data: pursuant to Article 25 of the EIT Bill, data collectors must obtain the prior consent of data subjects in order to use personal data about them electronically, unless statutory regulations provide otherwise. The explanatory memorandum to the EIT Bill interprets this Article as conferring upon data subjects a very broad privacy right that involves:

- the right to enjoy personal life and to be free from all kinds of disturbances;
- the right to communicate with other persons without being spied on; and
- the right to control access to personal data about oneself.

Failure to comply with Article 25 of the EIT Bill can lead to imprisonment for up to six years and/or a fine of up to IDR 100 million (approximately USD$10,940).

6. Indonesia

Sensitive information

In September 2007, the House of Representatives was debating a draft law on freedom of information that is expected to be passed in late 2007. Drafts of the legislation released in 2005 showed that, once enacted, the draft law would oblige users of public information to protect and not misuse public information in accordance with the provisions of the draft law and other regulations.

2.5 SPAM LAWS – CURRENT LEGISLATIVE FRAMEWORK

Indonesia does not have any legislation that regulates spam.

2.6 SPAM LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

At the date of writing, there are no proposals to enact comprehensive anti-spam legislation in Indonesia. However, there is one provision in the EIT Bill that is likely to have the effect of regulating the content of emails offering to sell goods and services. Article 9 of the EIT Bill provides that where a good or service is offered for sale through electronic media, the person offering to sell the good or service must provide complete and correct information in relation to the terms of the contract, the good or service offered and the producer of the good or service.

2.7 ONLINE CHILD SAFETY LAWS – CURRENT LEGISLATIVE FRAMEWORK

General child pornography offences

The age of majority is 18 for males and 15 for females unless the individual concerned is married earlier (in which case majority is reached at the age of marriage). Officially, the age of consent to sexual relations is 16 years for females; procedural limitations mean that, in practice, the age of consent for females is 12 years. For males, the age of consent to sexual relations is 19 years.

Indonesia's Criminal Code does not specifically address child pornography and its general obscenity regime is of limited application. This is because the Code's regime covers indecent material depicted in writings and portraits, but it is unlikely to regulate videotapes, audiotapes or other forms of digital media. There is also no definition of what constitutes "indecent" material, although it is understood that child pornography involving nudity is likely to be regulated by the Code.

The Code prohibits producing, disseminating, displaying, distributing, storing, importing or exporting indecent material. Mere possession of indecent material is not criminalised; possession with intent to distribute is. The penalty for infringing the Code depends on whether the relevant offence is committed negligently, knowingly, habitually or professionally. At the lowest end of the spectrum, offenders are liable to imprisonment for a term of up to nine months; at the highest end, offenders can face up to two years and eight months in prison. A separate provision specifically prohibits the dissemination of indecent material to children below the age of 17; this offence is punishable by nine months imprisonment or a fine. Finally, Article 295 punishes any person who deliberately causes or facilitates the commission of an obscene act by a minor with another person.

The Child Protection Act provides limited recourse against those involved in the production of child pornography. Article 88 criminalises the sexual exploitation of a child (a person under the age of 18) for gain, while articles 82 and 83 punish sexual intercourse and indecent behaviour with a child. Article 78 of the Child Protection Act also criminalises, to some degree, the failure to act in cases of child sexual exploitation, although only where the omission is intentional. All of these offences are punished by more severe penalties than the indecent material offences mentioned above, and corporate criminal responsibility is expressly provided for.

Computer-facilitated child pornography offences (Title 3 COE)

Indonesia does not have any legislation that creates computer-facilitated child pornography offences.

2.8 ONLINE CHILD SAFETY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

Computer-facilitated child pornography offences (Title 3 COE)

In 2005, the Draft Law on the Act Concerning Anti-Pornography and Porno-Action (Draft Pornography Law) was being considered by the Indonesian parliament. However, as at September 2007, it had not been enacted and it is not known when this is expected to occur. The Draft Pornography Law includes several articles that criminalise the use of children as objects of pornographic activities. If enacted, offenders will be liable for imprisonment for up to 20 years and/or a fine of up to IDR 3 billion (approximately USD$328,380).

The Draft Pornography Law also recognises modern forms of distributing pornographic material by specifically prohibiting the acts of printing, circulating, broadcasting and advertising pornographic material. The proposed regime also provides for severe penalties: imprisonment for a term of up to 20 years and fines of up to IDR 1 billion (approximately USD$109,490).

Article 26 of the Draft Law on Electronic Information and Transaction (EIT Bill) criminalises the computer-facilitated dissemination of electronic information that contains "pornography or porno-action". The terms "pornography" and "porno-action" are not defined in the EIT Bill. Offenders would be liable to imprisonment for up to three years and a fine of up to IDR 1 billion (approximately USD$109,490).

Part 3 – Benchmark Comparison

Key: Favourable alignment | Moderate alignment | Weak alignment

(E) Enacted
(P) Pending
(Title [x]) Title [x] of the Council of Europe Convention on Cybercrime

Area	Legislative regime to be compared with benchmark	Benchmark legislation	Overall alignment	Areas of strong alignment	Areas of moderate alignment	Areas of weak alignment
Computer Security Laws	Criminal Code (E); Telecommunications Law (E); Law No. 30 of 2000 regarding Trade Secret (E)	Council of Europe Convention on Cybercrime (Titles 1, 2 and 5)			• Illegal access offence under the Telecommunications Law	• No specific cybercrime legislation • General Criminal Code principles may criminalise prohibited acts under the Convention (but the application of these principles is generally untested)
	Bill on Electronic Information and Transaction (P)	Council of Europe Convention on Cybercrime (Titles 1, 2 and 5)		• Data interference offence	• Illegal access offence • System interference offences (although note their narrow application to government and/or financial systems) • Computer-related fraud offence	• No requirement for prohibited acts to be committed with intent • Illegal interception, misuse of devices, and computer-related forgery offences (due in some cases to their narrow application to government and/or financial systems) • Limited corporate criminal liability for cybercrimes • Ancillary liability for attempting, aiding or abetting cybercrimes
Privacy Laws	There is no comprehensive enacted or pending data protection legislation in Indonesia upon which a benchmarking analysis can be conducted.					
Spam Laws	There is no comprehensive enacted or pending spam legislation in Indonesia upon which a benchmarking analysis can be conducted.					
Online Child Safety Laws	Criminal Code (E); Child Protection Act (E)	Council of Europe Convention on Cybercrime (Title 3 COE)/ICMEC principles			• Sexual exploitation of a child for gain is criminalised	• General obscenity regime is of limited application to digital media • Mere possession of indecent material is not criminalised • No definition of child pornography • No general or computer-facilitated child pornography offences • No scope for ISP reporting of dealing in child pornography
	Draft Law on the Act Concerning Anti-Pornography and Porno-Action (P); Bill on Electronic Information and Transaction (P)	Council of Europe Convention on Cybercrime (Title 3 COE)/ICMEC principles			• Computer-facilitated distribution of "pornography" and "porno-action" is criminalised	• No definition of child pornography • No general or computer-facilitated child pornography offences • No scope for ISP reporting of dealing in child pornography

Last Updated: 17 October 2007

7. Japan

Part 1 – Snapshot of Legislative Status

Key: (E) Enacted
(P) Pending
(Title [x] COE) Title [x] of the Council of Europe Convention on Cybercrime (COE)

Area	Topic	Enacted legislation	Pending legislation	Relevant instruments/Comments
Computer Security Laws	**Core offences (Title 1 COE):** illegal access, illegal interception, data interference, system interference, misuse of devices	✓	✓	The Act Concerning the Prohibition of Unauthorised (Computer) Access (E); Criminal Code (E) Draft Law for Partial Amendment of Criminal Code in Response to Growing Criminal Internationalization and Organization and More Sophisticated Information Processing (P) The Japanese parliament is considering an amendment to the Criminal Code to criminalise the preparation, production and dissemination of computer viruses and malware.
	Computer-related offences (Title 2 COE): computer-related forgery, computer-related fraud	✓	✗	Criminal Code (E)
	Ancillary liability (Title 5 COE): attempt; aiding/abetting, corporate liability	✓	✗	Criminal Code (E)
Privacy Laws	**Data protection**	✓	✗	Act Concerning the Protection of Personal Information (E); The Law for the Protection of Personal Information Held by Government Organisations (E); The Law for the Protection of Personal Information Held by Independent Public Corporations (E); Law on the Establishment of the Information Disclosure/Personal Information Protection Examination Committee (E); The Law for the Preparation of Relevant Laws Concerning the Enforcement of the Law for the Protection of Personal Information Held by Government Organisations (E)
	Surveillance (see illegal interception under computer security)	✓	✗	Wire Telecommunications Law (E); Telecommunications Business Law (E); Radio Law (E); Communications Interception Law (E)
	Sensitive information	✗	✗	
Spam Laws	**Anti-spam regulation**	✓	✓	The Law Regarding the Regulation of Transmission of Specific E-mail (E); The Law Regarding Specific Commercial Transactions (E) It is understood that the Ministry of Internal Affairs and Communications plans to submit a bill to the Japanese parliament in 2008 to amend the Law Regarding the Regulation of Transmission of Specific E-mail (E).
Online Child Safety Laws	**General child pornography offences**	✓	✗	The Law for Punishing Acts Related to Child Prostitution and Child Pornography, and for Protecting Children (E)
	Computer-facilitated child pornography offences (Title 3 COE)	Partial	✗	The Law for Punishing Acts Related to Child Prostitution and Child Pornography, and for Protecting Children (E); Law Restricting Dating Websites (E) The Draft Law for Partial Amendment of Criminal Code in Response to Growing Criminal Internationalization and Organisation and More Sophisticated Information Processing (P) does not propose to enact computer-facilitated child pornography offences, but it does propose to criminalise certain dealings with obscene electromagnetic records.

Part 2 – Legal and Regulatory Position

2.1 COMPUTER SECURITY LAWS – CURRENT LEGISLATIVE FRAMEWORK

Japan is one of four non-European signatories to the Council of Europe's Convention on Cybercrime, although the Japanese government is yet to ratify this instrument.

Core offences (Title 1 COE): Illegal access, illegal interception, data interference, system interference, misuse of devices

The illegal access offence in the Unauthorised Computer Access Law is committed when a person, without authorisation, makes available a specific use of a computer that is protected by an access control function. The specific use must be made available by (i) inputting another person's username and password via a telecommunications line or (ii) otherwise evading the restrictions imposed by the access control function by sending data via a telecommunications line. Offenders are liable to imprisonment for a term of up to one year or a fine of up to JPY500,000 (approximately USD$4,270). There is no illegal access offence where access is obtained other than via a telecommunications line. Unlike the Convention, mere access is not sufficient – the computer must be operated by the alleged infringer.

It is a separate offence under the Unauthorised Access Law to facilitate unauthorised access by making available, without authorisation, personal identifiers such as usernames and passwords. This offence is punishable by a fine of up to JPY300,000 (approximately USD$2,560).

The Convention's data and system interference offences are enacted in Japan's Criminal Code. Article 234-2 creates an offence of business interference by damaging or otherwise interfering with business computers or electronic records; it is punishable by imprisonment for a maximum term of five years or a fine of JPY1,000,000 (approximately USD$8,530). Separate provisions regulate the destruction of government or private electromagnetic records that relate to rights or obligations. These permutations of the Convention's data interference offence are punishable by imprisonment for between three months and seven years (for interference with government records) or by imprisonment for five years or less (for interference with private records).

The surveillance laws discussed in section 2.3 address the Convention's illegal interception offence.

Computer-related offences (Title 2 COE): Computer-related forgery, computer-related fraud

The Convention's computer-related forgery offence is embodied in article 161-2 of the Criminal Code, while computer-related fraud is addressed in article 246-2 of the same legislation. Both these offences appear to contemplate the creation (rather than manipulation) of electromagnetic records, although it is sufficient to attract liability under the computer-related forgery offence to put into use a forged document that affects another person's affairs. The Code's computer-related forgery offence is punishable with imprisonment for up to 10 years or with a fine of up to JPY1,000,000 (approximately USD$8,530), depending on whether the forged record was prepared for government or private use. Computer-related fraud is also treated seriously, attracting a term of imprisonment of up to 10 years.

Ancillary liability (Title 5 COE): Attempt and aiding/abetting, corporate liability

The Criminal Code appears to contemplate ancillary liability for aiding and abetting the commission of an offence – as an instigator or accessory – as well as ancillary liability for attempt. Corporate criminal liability appears to be established where a corporation's agents, servants or employees commit prohibited acts under the Criminal Code.

2.2 COMPUTER SECURITY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

Core offences (Title 1 COE): Illegal access, illegal interception, data interference, system interference, misuse of devices

The Diet (the Japanese parliament) is currently considering a bill to amend the Criminal Code to address the preparation, production, dissemination and use of files that contain viruses, malware or other records that set out illegal instructions. Specifically, the Draft Law for Partial Amendment of Criminal Code in Response to Growing Criminal Internationalization and Organization and More Sophisticated Information Processing criminalises the acts of:

- preparing or providing, for the purpose of execution on a third party's computer, an electromagnetic record which, when a person uses a computer, gives an illegal instruction to avoid an action or perform an action not intended by the user (maximum penalty: three years imprisonment with labour or a fine of up to JPY500,000 [approximately USD$4,250]);
- acquiring or keeping, for the purpose of execution on a third party's computer, an electromagnetic record which, when a person uses a computer, gives an illegal instruction to avoid an action or perform an action not intended by the user (maximum penalty: two years imprisonment with labour or a fine of up to JPY300,000 (approximately USD$4,250); and
- attempting to commit the crime set out in Article 234 of the Criminal Code, which criminalises the act of intentionally, knowingly and illegally causing disruption to, or interference with, a computer system that is used, or intended to be used, for business transactions.

7. Japan

A separate piece of legislation is also being considered by the Diet to implement Japan's remaining obligations as a signatory to the Council of Europe's Cybercrime Convention. The timeframe for the enactment of this piece of this legislation is unknown.

2.3 PRIVACY LAWS – CURRENT LEGISLATIVE FRAMEWORK

Data protection

In May 2003, the Act Concerning the Protection of Personal Information (Protection of Personal Information Act) was enacted by the Diet. This Act establishes the basic ideals and principles that serve as the basis for legislation on the protection of privacy in both the public and private sectors. For this purpose, "personal information" is defined as information relating to a living individual person that permits identification of that person by their name, date of birth or other description.

The sections of the Protection of Personal Information Act that apply to the private sector came into force in April 2005. Only persons and companies that have an office in Japan and handle the personal information of more than 5,000 individuals (including employee personal information) are regulated by the Act's 'opt-out' regime. These "businesses handling personal information" must:

- specify the purpose for their use of the data subject's personal information;
- only use personal information to the extent necessary to achieve their stated purpose(s) of use (or obtain the data subject's prior consent to use their personal information for purposes beyond that stated);
- make available information about the business collecting the data subject's personal information (e.g. contact details and procedures for getting access to personal information);
- not acquire personal information by fraudulent or unfair means;
- ensure that personal information is kept secure from loss and unauthorised access and disclosure;
- refrain from supplying personal information to third parties without the prior consent of the individual concerned, except in certain defined circumstances;
- respond to data subject requests for correction, supplementation or deletion of personal information;
- respond to data subject requests that an entity cease using personal information altogether; and
- endeavour to appropriately and promptly handle individual complaints about the handling of personal information.

The sectoral application of these general principles is explained by guidelines published by Japan's government ministries. As at April 2005, guidelines existed in the health, credit and fine, communications and employment sectors; the Ministry of Economy, Trade and Industry (METI) had also devised guidelines for generic use. Although these guidelines do not have the force of law, most private sector companies in Japan generally follow them, not least because the ministries responsible for promulgating these guidelines are often empowered to sanction conduct that infringes the Protection of Personal Information Act. Possible sanctions under that Act range from admonishment orders to fines of up to JPY300,000 (approximately USD$2,560).

At the same time that the private sector legislation was passed, the Diet enacted four related pieces of legislation: The Law For the Protection of Personal Information Held by Government Organisations; The Law for the Protection of Personal Information Held by Independent Public Corporations; The Law on the Establishment of the Information Disclosure/Personal Information Protection Examination Committee; and The Law for the Preparation of Relevant Laws Concerning the Enforcement of the Law for the Protection of Personal Information Held by Government Organisations. These Acts principally regulate public sector entities that are outside the scope of the private sector legislation.

Surveillance

Article 9 of the Wire Telecommunications Law protects the secrecy of most wire telecommunications. Offenders are liable to a maximum term of imprisonment of two years or a fine of up to JPY500,000 (approximately USD$4,270). Similarly, the Telecommunications Business Law protects the secrecy of communications handled by telecommunications carriers, and the Radio Law makes it an offence to intercept, divulge or take advantage of radio communications in most circumstances. Offenders who violate the Telecommunications Business Law can be punished by a maximum term of imprisonment of up to two years or a fine of up to JPY2,000,000 (approximately USD$17,050); offenders who violate the Radio Law can be punished by a maximum term of imprisonment of two years or a fine of up to JPY1,000,000 (approximately USD$8,530). Each of the Wire Telecommunications Law, Telecommunications Business Law and the Radio Law is understood to apply to electronic communications.

In August 1999, the Diet passed the Communications Interception Law. This law authorises prosecutors and high-ranking police officers to wiretap phones and faxes, and monitor emails, when investigating cases involving narcotics, gun offences, gang-related murders and large-scale trafficking of foreigners. Officers must obtain a warrant to undertake such interception from a district court judge and an independent third party must be present when the taps are being monitored. In addition, police and prosecutors must notify individuals who have been monitored within 30 days after the investigation.

A network of surveillance cameras operates on Japan's major expressways and highways, and video surveillance of public places

is becoming more common. So too is private surveillance in the workplace.

Sensitive information

Japan does not appear to have any legislation that specifically addresses sensitive information.

Miscellaneous

Japanese citizens also enjoy constitutional and tortious rights of privacy.

In June 2004, the Ministry of Internal Affairs and Communications (MIC) and Ministry of Trade, Economy and Industry (MTEI) released joint guidelines on the use of RFID tags on consumer products. Among other things, these regulations provide that (i) the Personal Information Protection Act applies to matching between RFID tag-related data and databases, and (ii) consumers must be provided with access to, and the ability to correct, personal information recorded by RFID tags.

At the same time that the Diet passed the Communications Interception Law, it provisionally approved the Basic Resident Registers Law. This law enables residents of Japan to be issued with an 11-digit number upon registration of certain personal information. Basic personal information such as a resident's name, date of birth, gender and address is made publicly available on a registration card; more sensitive personal information is retained for specific purposes. All registered data is computerised and connected to the nationwide Resident Registry Network System (also known as "Juki-Net"). Despite the initial reluctance of some local governments to log onto the network, uptake of the system is now widespread.

2.4 PRIVACY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

It is understood that the Government has plans to gather research and conduct consultations on Japan's personal information laws with the possibility of considering full-scale amendments in 2009.

2.5 SPAM LAWS – CURRENT LEGISLATIVE FRAMEWORK

Japan has two laws that specifically regulate spam: the Law Regarding the Regulation of Transmission of Specific E-mail (Specific Email Law); and the Law Regarding Specific Commercial Transactions (Commercial Transactions Law).

The Specific Email Law establishes an 'opt-out' regime in respect of unsolicited email advertisements that are sent for business purposes. To avoid liability under this regime, senders must: (i) clearly show that the email is an unsolicited advertisement, (ii) display within the email the correct name, email address and physical address of the sender, as well as an opt-out email address, and (iii) refrain from sending spam to a recipient who has opted-out of receiving such communications. As a result of an amendment passed in May 2005, failure to comply with these requirements may lead to imprisonment for up to one year or a fine of up to JPY1,000,000 (approximately USD$8,775) even for first-time offenders (previously first-time offenders were issued with a warning). The Specific Email Law also prohibits the use of programs that generate random fictitious email addresses, and permits telecommunications carriers to deny service to spammers that seek to transmit communications to random fictitious email addresses over a carrier's network.

To further support this legislative framework, in April 2001, the then Ministry of Public Management, Home Affairs, Posts and Telecommunications (MPHPT) issued an "administrative guidance" to all mobile operators to implement certain countermeasures against mobile spam. These measures include utilisation of domain designation services (which operate to prevent the receipt of spam from forged domains).

The Commercial Transactions Law establishes a consumer-oriented anti-spam regime that applies to mail order, pyramid selling and employment-related advertising that is communicated electronically. Spam communications need not be sent for business purposes to fall within the ambit of this regime. The Commercial Transactions Law has equivalent transparency and opt-out requirements to those outlined above in relation to the Specific Email Law. Its operation is overseen by the MTEI.

2.6 SPAM LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

There are currently plans to amend the Specific Email Law. The Ministry of Internal Affairs and Communications plans on submitting a bill to the Diet in 2008 which is expected to create an opt-in regime for spam emails accessed from computers and mobile phones. The proposed bill is expected to be based on a report to be published in 2008 by an anti-spam working group that has been tasked with investigating measures needed to prevent and suppress spam in Japan. It is also expected the Ministry will adopt measures to increase Japan's involvement in international anti-spam initiatives.

2.7 ONLINE CHILD SAFETY LAWS – CURRENT LEGISLATIVE FRAMEWORK

General child pornography offences

The age of majority in Japan is 20 years; the age of consent to sexual relations is 13 years.

The Law for Punishing Acts Related to Child Prostitution and Child Pornography, and for Protecting Children (Child Pornography Law) targets the commercial sexual exploitation of children. Child pornography is defined as photos, videos and other materials that depict, in a way that can be recognised visually, children in a pose (i) relating to sexual intercourse or similar, (ii) relating to the act of touching genital organs in order to stimulate sexual desire or (iii) where the child is totally or partially naked in order to stimulate

sexual desire. This definition is understood to embrace altered child pornography where the subject is less than 18 years old, although it remains unclear whether cartoons that depict child pornography are also covered. For the purposes of the Child Pornography Law, a child is a person under the age of 18 years, and the onus is on the prosecutor to prove that a depicted child is underage.

Article 7(1) of the Child Pornography Law prohibits the distribution, sale, commercial lending or public display of child pornography. Production, possession, importation or exportation of child pornography for the purpose of distribution is a separate offence. Each of these offences is punishable by imprisonment for up to three years or a fine of up to JPY3,000,000 (USD$25,590).

Further, an intermediary who solicits children to commit child prostitution (sexual intercourse by or with a child) with another person is liable to imprisonment for up to five years or a fine of up to JPY5,000,000 (USD$42,640). Commercial solicitation – the for-profit solicitation of children to commit child prostitution – attracts the higher penalty of imprisonment for up to seven years and a fine not exceeding JPY10,000,000 (USD$85,280).

Local municipals also have local ordinances that restrict the distribution of harmful material to minors.

Computer-facilitated child pornography offences (Title 3 COE)

Although the 2005 amendments to the Child Pornography Law do not create computer-facilitated child pornography offences per se, the use of online examples in their formulation suggests that the offences are targeted at online conduct. For example, the offence of production or possession of child pornography, for the purpose of distribution to an unspecified large number of people or public display, cites posting child pornography on the internet as an example of offending conduct. This offence attracts a maximum term of imprisonment of five years and/or a fine not exceeding JPY5,000,000 (USD$42,640). Similarly, online solicitation of children is used as an example of conduct that will fall within the extended solicitation offence in article 7. This extended solicitation offence is punishable by imprisonment for up to seven years and a fine not exceeding JPY10,000,000 (USD$85,280).

Miscellaneous

Another online child safety law is the Law Restricting Dating Websites. It specifically prohibits the use of internet dating services to seduce minors as partners for sexual relationships or for paid dating. It also requires internet dating service providers to make it clear that children are barred from using their services.

Finally, the Internet Provider Liability Law enables ISPs to delete illegal content, such as child pornography advertised for sale online, without legal risk.

2.8 ONLINE CHILD SAFETY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

There are currently plans to amend the Child Pornography Law, although the details of planned amendments are not yet available.

The Diet is considering a bill to amend the Criminal Code to prohibit a person from distributing or publicly displaying data storage devices or other articles that contain or relate to obscene electromagnetic records. This prohibition extends to the distribution of obscene electromagnetic records using telecommunications services (i.e. over the internet). Possession of obscene electromagnetic records, or articles or data storage devices that contain obscene records, is criminalised where the offender intends to distribute them for consideration. Offenders could face a term of imprisonment and labour of up to 2 years and/or a fine of up to JPY2.5 million (approximately USD$21,260). It is expected that an electronic record containing child pornography would be considered an obscene electromagnetic record under the bill.

Part 3 – Benchmark Comparison

Key: Favourable alignment | Moderate alignment | weak alignment

(E) Enacted
(P) Pending
(Title [x]) Title [x] of the Council of Europe Convention on Cybercrime

Area	Legislative regime to be compared with benchmark	Benchmark legislation	Overall alignment	Areas of strong alignment	Areas of moderate alignment	Areas of weak alignment
Computer Security Laws	The Act Concerning the Prohibition of Unauthorised (Computer) Access (E); Criminal Code (E)	Council of Europe Convention on Cybercrime (Titles 1, 2 and 5)		• Illegal interception offence	• Data and system interference offences • Computer-related fraud and forgery offences • Ancillary liability for attempt, and aiding or abetting under the Criminial Code	• Illegal access offence • Corporate liability for contraventions of the Criminal Code • No misuse of devices offence
Privacy Laws	**Private sector regime:** Act Concerning the Protection of Personal Information (E)	Model Privacy Bill (drafted by Microsoft)		• 'Opt out' regime – consent is not a prerequisite to collection or use of personal information • Threshold amount of personal information that must be collected for the regime to apply • Obligation to keep personal information free from loss or unauthorised disclosure or destruction • Data subject's right to access and correct personal information	• Definition of personal information • Obligation on data user to notify purpose of use • Transparency matters that must be notified to data subject (e.g. the identity of the entity that collects data and the purposes of use of the personal information) • Ability to disclose personal information to service providers to achieve the purpose of use	• Exemptions for some entities e.g. news agencies, universities and political organisations • Mode of enforcement (administrative order by cabinet minister cf. enforcement by Commissioner) • Consequence of infringement (administrative order or fine cf. statutory and civil liability)

Table continues overleaf

7. Japan

Area	Legislative regime to be compared with benchmark	Benchmark legislation	Overall alignment	Areas of strong alignment	Areas of moderate alignment	Areas of weak alignment
Privacy Laws (continued)	**Public sector regime:** The Law For the Protection of Personal Information Held by Government Organisations (E); The Law for the Protection of Personal Information Held by Independent Public Corporations (E); Law on the Establishment of the Information Disclosure/Personal Information Protection Examination Committee (E); The Law for the Preparation of Relevant Laws Concerning the Enforcement of the Law for the Protection of Personal Information Held by Government Organisations (E)	Model Privacy Bill (drafted by Microsoft)	An English translation of this enacted legislation was not readily available to enable a benchmark analysis to be conducted.			
Spam Laws	The Law Regarding the Regulation of Transmission of Specific E-mail (E) The Law Regarding Specific Commercial Transactions (E)	Anti-spam legislation checklist (drafted by Microsoft)	An English translation of this enacted legislation was not readily available to enable a benchmark analysis to be conducted.			
Online Child Safety Laws	The Law for Punishing Acts Related to Child Prostitution and Child Pornography, and for Protecting Children (E); Law Restricting Dating Websites (E)	Council of Europe Convention on Cybercrime (Title 3 COE)/ICMEC principles		• General child pornography offences	• Definition of child pornography	• No specific computer-facilitated child pornography offences • Mere possession of child pornography is not prohibited • No scope for ISP reporting of dealing in child pornography

Last Updated: 23 October 2007

8. Malaysia

Part 1 – Snapshot of Legislative Status

Key: (E) Enacted
(P) Pending
(Title [x] COE) Title [x] of the Council of Europe Convention on Cybercrime (COE)

Area	Topic	Enacted legislation	Pending legislation	Relevant instruments/Comments
Computer Security Laws	**Core offences (Title 1 COE):** illegal access, illegal interception, data interference, system interference, misuse of devices	✓	✗	Computer Crimes Act 1997 (E)
	Computer-related offences (Title 2 COE): computer-related forgery, computer-related fraud	✓	✗	Computer Crimes Act 1997 (E)
	Ancillary liability (Title 5 COE): attempt; aiding/abetting, corporate liability	Partial	✗	Computer Crimes Act 1997 (E)
Privacy Laws	**Data protection**	✗	✓	No general data protection legislation, but the General Consumer Code is relevant. Personal Data Protection Bill (P). This bill is currently being redrafted; the timeframe for its release is not known.
	Surveillance (see illegal interception under computer security)	✓	✗	Communications and Multimedia Act 1998 (E); Computer Crimes Act 1997 (E); Internal Security Act 1960 (E); Anti-Corruption Act 1997 (E); National Registration Act 1959 (E)
	Sensitive information	✓	✗	Various legislation including Banking and Financial Institutions Act 1989 (E) and Anti-Money Laundering Act 2001 (E).
Spam Laws	**Anti-spam regulation**	Partial	✗	No general anti-spam legislation, but the Communications and Multimedia Act 1998 (E) provides limited recourse against spammers. The Internet Access Service Provider (IASP) Sub-Code pursuant to that Act is also relevant.
Online Child Safety Laws	**General child pornography offences**	✗	✗	No general child pornography legislation, but the Penal Code (E) prohibits the dissemination of obscene and offensive material. The Child Act 2001(E) prohibits dealing in children for prostitution and establishes a regime to protect children who have been sexually abused.
	Computer-facilitated child pornography offences (Title 3 COE)	✗	✗	No specific computer-facilitated child pornography offences, but the Communications and Multimedia Act 1998 (E) makes it an offence for applications service providers or those using an application service to provide indecent, obscene or offensive content.

Part 2 – Legal and Regulatory Position

2.1 Computer Security Laws – Current legislative framework

Core offences (Title 1 COE): Illegal access, illegal interception, data interference, system interference, misuse of devices

The focus of Malaysia's Computer Crimes Act 1997 is on unauthorised access to computer systems and its consequences. The Act makes it an offence to:

- cause a computer to perform a function with intent to secure unauthorised access to data or programs stored on a computer;
- commit an act with knowledge that the act will cause unauthorised modification of the contents of a computer; and
- wrongfully communicate a password, code or means of access to a computer to a person who is not authorised to receive the same.

These offences are punishable by maximum fines ranging from RM25,000 (approximately USD$7,250) to RM150,000 (approximately USD$43,510) and maximum terms of imprisonment of between three and 10 years.

In terms of alignment between the Computer Crimes Act and the Convention on Cybercrime, the first two offences above broadly equate to the Convention's illegal access and data interference

offences, although illegal access under the Convention need not be secured by a computer function. In addition, the Malaysian Act does not address illegal interception of data and system interference (seriously hindering the functioning of a computer system by altering or otherwise damaging data), and its unauthorised distribution of password offence only partially implements the Convention's misuse of devices offence. An unusual departure from the Convention framework is the presumption in the Computer Crimes Act that a person has obtained unauthorised access to a program, data or information if he or she has such material in his or her custody or control without authorisation.

Computer-related offences (Title 2 COE): computer-related forgery, computer-related fraud

It is a separate offence under the Computer Crimes Act to secure unauthorised access with intent to commit, or facilitate the commission of, a further offence involving fraud or dishonesty. This extended unauthorised access offence is understood to cover largely the same ground as the Convention's computer-related forgery and fraud offences where the further offence involves forgery or fraud.

Ancillary liability (Title 5 COE): Attempt and aiding/abetting, corporate liability

Although the Computer Crimes Act 1997 does not address corporate liability expressly, the Act does consider liability for attempting, aiding or abetting the commission of an offence – those who attempt, aid or abet the commission of an offence under the Computer Crimes Act face the same penalties as the principal offender, except that any term of imprisonment for these perpetrators must not exceed half the maximum term provided for.

2.2 COMPUTER SECURITY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

At the date of writing, there are no upcoming legislative developments that relate to computer security.

2.3 PRIVACY LAWS – CURRENT LEGISLATIVE FRAMEWORK

Data protection

Malaysia does not have any specific data protection legislation. However, the General Consumer Code developed pursuant to the Communications and Multimedia Act 1998 contains provisions that relate to the protection of personal information (information collected from the consumer and which identifies the consumer). These provisions require licensed telecommunications service providers to collect and maintain consumer data in accordance with certain "good practices" including: data must be fairly and lawfully collected and processed; data must be processed for limited purposes; data must be kept accurate and secure; and data must not be transferred to any other party without prior approval from the consumer. The Code also contains specific rules in respect of adoption and implementation of a "Protection of Consumer Information Policy", notice and disclosure of data collection and use practices, consumer choice/consent, data security, and data quality and access.

Surveillance

The Communications and Multimedia Act prohibits the unlawful interception of communications, establishes rules for searches of computers, mandates access to encryption keys and authorises police to intercept communications without a warrant if a public prosecutor believes a communication is likely to contain information relevant to an investigation. However, Privacy International has reported that, in practice, the interception provisions of the Communications and Multimedia Act 1998 are regularly ignored or overridden by other statutes (such as the Internal Security Act 1960, the Anti-Corruption Act 1997 and the Computer Crimes Act 1997).

The Internal Security Act 1960 allows police to enter and search without warrant the homes of persons suspected of threatening national security. The lack of independent judicial oversight is the most poignant criticism of this Act – judicial reviews of arrests under it are limited to questions of procedure.

The National Registration Act 1959 requires every person within Malaysia to be registered on the national register. The National Registration Department is the lead agency for the MyKad initiative.

Sensitive information

Malaysia has a range of laws that protect sensitive information, including banking secrecy laws and laws that preserve doctor-patient confidentiality. A related piece of legislation is the Anti-Money Laundering Act 2001 which overrides any secrecy obligations that are inconsistent with the reporting obligations contained therein.

2.4 PRIVACY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

Data protection

The Malaysian government has been considering draft data protection legislation for some time. A 2005 draft of the Personal Data Protection Bill revealed that the legislation is modelled on Hong Kong's data protection regime (as is established by the Personal Data (Privacy) Ordinance). It is understood that this draft of the bill imposed a duty on persons controlling the collection, holding or processing of personal data (referred to as "data users") to comply with minimum standards relating to the manner of collection, use, disclosure, accuracy, retention, security and access. It also had a transborder data provision that required destination country regimes to be "substantially similar," "serve the same purpose" or provide an "adequate" level of protection before data transfers would be

permissible. It is understood that a further draft of Malaysia's data protection legislation has been prepared since 2005. The likelihood of, and timeframe for, this bill or any other data protection legislation being introduced into parliament is not known.

2.5 SPAM LAWS – CURRENT LEGISLATIVE FRAMEWORK

Malaysia does not have any specific spam legislation. However, section 233 of the Communications and Multimedia Act offers limited recourse against spammers. This Act makes it an offence for a person to initiate (i) a communication (whether continuously, repeatedly or otherwise) with intent to annoy or harass another person at any number or electronic address or (ii) the transmission of any comment, request, suggestion or other communication which is obscene, indecent or offensive in character with intent to annoy or harass another person. Offenders are liable to a fine of up to RM50,000 (approximately USD$14,510) and imprisonment for a term not exceeding one year. Repeat offenders can face additional fines of RM1,000 (approximately USD$290) for every day on which the offence is committed after conviction.

In June 2005, the Malaysian Communications and Multimedia Commission registered a sub-code that addresses how internet access service providers (that are licensed as application service providers) should deal with spam. Developed by the Communications and Multimedia Consumer Forum, the Internet Access Service Provider Sub-Code obliges service providers to develop a written procedure for handling spam incidents and to make available information about their anti-spamming measures on their website. The Sub-Code also suggests that service providers should consider including (but are not obliged to include) the following in their contracts with consumers "who may have the propensity to produce spam": (i) a prohibition on sending spam messages; (ii) a stipulation that sending spam may result in the suspension or termination of the customer's account; and (iii) an acceptable use policy that obliges customers to ensure that all commercial emails sent by them contain accurate header information, a valid return email address, a functional unsubscribe facility, sender identification and appropriate labelling. Service provider liability for acting in compliance with the Sub-Code does not appear to be addressed.

2.6 SPAM LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

The Malaysian Communications and Multimedia Commission announced in August 2007 that it had issued a tender for the provision of consultancy services for studying legislative responses and drafting anti-spam legislation for Malaysia.

2.7 ONLINE CHILD SAFETY LAWS – CURRENT LEGISLATIVE FRAMEWORK

General child pornography offences

In Malaysia, the age of majority is 18 years. The age of consent to sexual relations is 16 years in Malaysia, however under Shariah (Islamic) law all sexual conduct outside marriage is prohibited.

Malaysia has not enacted specific laws prohibiting the dissemination of child pornography. Instead, the Penal Code prohibits the sale, distribution, importation and exhibition of obscene objects. It is a separate offence to expose a person under the age of 20 to an obscene object and this offence is punishable by imprisonment for up to five years or with a fine or with both.

The Child Act 2001 prohibits dealing in children (persons under the age of 18 years) for the purposes of prostitution and punishes such acts harshly: fines extend up to RM50,000 (approximately USD$14,510) and offenders can face imprisonment for a term of up to 15 years. Paid use of the services of a child prostitute and controlling the prostitution of a child attract a minimum term of imprisonment of three years as well as whipping. Once again, repeat offending is punished more severely.

The Child Act 2001 also establishes a protection regime for children who have been, or are at risk of being, sexually abused by a relative or where the child's parent or guardian knows of the abuse (or risk thereof) and has not (or will not) protect the victim. A child is deemed to be "sexually abused" if he or she has taken part, whether as a participant or an observer, in any sexual activity for the purposes of (i) producing pornographic, obscene or indecent material or (ii) sexual exploitation for another person's sexual gratification. The Act does not consider how this concept applies to the sexual exploitation of children online.

Computer-facilitated child pornography offences (Title 3 COE)

Malaysia does not have any legislation that creates computer-facilitated child pornography offences. However, section 211 of the Communications and Multimedia Act prohibits content application service providers, or other persons using application services, from providing content which is indecent, obscene or offensive in character with intent to annoy, abuse, threaten or harass any person. Offenders are liable to a fine not exceeding RM50,000 (approximately USD$14,510) or imprisonment for a term not exceeding one year or both. Repeat offenders are subject to further penalties.

8. Malaysia

Miscellaneous

In addition to the legislative regimes discussed above, both the Internet Access Provider (IASP) Sub-Code and the Content Code registered by the Malaysian Communications and Multimedia Commission (MCMC) address online child safety. The IASP Sub-Code obliges service providers that have undertaken to adhere to it to take reasonable steps to ensure that post-paid (as opposed to pre-paid) internet access accounts are not provided to a child without the consent of his or her guardian. Service providers should also take reasonable steps to provide customers with information about how to supervise and control children's access to internet content including by way of internet content filtering software.

The Content Code, on the other hand, provides guidance as to the types of content that are prohibited under section 211 of the Communications and Multimedia Act. Child pornography is expressly included within the prohibited category "obscene content", and sex scenes and nudity are considered "indecent content". Section 8 of the Code is targeted at children's content and reminds content providers that "content designed specifically for children of and below 14 years reaches impressionable minds and influences social attitudes and aptitudes." Specific attention should be paid to whether there is a need for the content to depict violence, and the extent to which content may threaten a child's sense of security or encourage children to imitate acts portrayed by the content. Finally, in Part 10 of the Code, it is stated that all content must have due regard to the welfare of children and that all efforts must be made to ensure that any content provided will not result in, cause or encourage physical injury or abuse of a child or expose a child to moral danger.

Service provider adherence to the provisions of the IASP Sub-Code and Content Code is voluntary, unless a service provider is directed by the MCMC to comply with them. If a service provider does not comply with such a direction it could face fines of up to RM200,000 (approximately USD$58,000). In addition, compliance with either code is a defence that can be relied on by a service provider in any proceeding against it, provided that the proceeding is in relation to a matter covered by the relevant code.

2.8 ONLINE CHILD SAFETY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

At the date of writing, there are no upcoming legislative developments that relate to online child safety.

Part 3 – Benchmark Comparison

Key: Favourable alignment | Moderate alignment | Weak alignment

(E) Enacted
(P) Pending
(Title [x]) Title [x] of the Council of Europe Convention on Cybercrime

Area	Legislative regime to be compared with benchmark	Benchmark legislation	Overall alignment	Areas of strong alignment	Areas of moderate alignment	Areas of weak alignment
Computer Security Laws	Computer Crimes Act 1997 (E)	Council of Europe Convention on Cybercrime (Titles 1, 2 and 5)		• Data interference offence • Ancillary liability for attempting, aiding or abetting cybercrimes	• Illegal access offence • Unauthorised distribution of password offence (partial implementation of the Convention's misuse of devices offence) • Computer-related fraud and forgery offences	• No illegal interception of data or system interference offences • Corporate liability not addressed • Deeming provision regarding unauthorised access
Privacy Laws	The latest version of the Personal Data Protection Bill has not been made available to enable a benchmarking analysis to be conducted.					
Spam Laws	Communications and Multimedia Act 1998 (E)	Anti-spam legislation checklist (drafted by Microsoft)			• Increased sanctions for repeat offenders • Criminal sanctions for some forms of spamming envisaged by the benchmark legislation	• Relevance of spammer's intention (this is irrelevant under the benchmark legislation) • No 'opt-out' regime • No scope for prior business relationships • No private right of action for ISPs/email service providers; criminal sanctions only • No consideration of ISP liability for transmission • No transparency requirements (unsubscribe facility, sender identification)
Online Child Safety Laws	Penal Code (E) Communications and Multimedia Act 1998 (E) Child Act 2001 (E)	Council of Europe Convention on Cybercrime (Title 3)/ICMEC principles			• Criminal sanctions for distributing, transmitting, making available indecent, obscene or offensive material	• No legislation specific to child pornography • No definition of child pornography • No computer-facilitated child pornography offences • Possession irrespective of intent to distribute is not prohibited • No scope for ISP reporting of dealing in child pornography

Last Updated: 24 October 2007

9. New Zealand

Part 1 – Snapshot of Legislative Status

Key: (E) Enacted
(P) Pending
(Title [x] COE) Title [x] of the Council of Europe Convention on Cybercrime (COE)

Area	Topic	Enacted legislation	Pending legislation	Relevant instruments/Comments
Computer Security Laws	**Core offences (Title 1 COE):** illegal access, illegal interception, data interference, system interference, misuse of devices	✓	✗	Crimes Act 1961 (E)
	Computer-related offences (Title 2 COE): computer-related forgery, computer-related fraud	✓	✗	Crimes Act 1961 (E)
	Ancillary liability (Title 5 COE): attempt; aiding/abetting, corporate liability	✓	✗	Crimes Act 1961 (E)
Privacy Laws	**Data protection**	✓	✗	Privacy Act 1993 (E) and various codes issued pursuant to the Act
	Surveillance (see illegal interception under computer security)	✓	✗	Crimes Act 1961 (E); Misuse of Drugs Amendment Act 1978 (E); New Zealand Security Intelligence Service Act 1969 (E); Government Communications Security Bureau Act 2003 (E)
	Secrecy and freedom of information	✓	✗	Various laws impose an obligation of secrecy including the Tax Administration Act 1994 (E), Electoral Act 1993 (E) and Ombudsmen Act 1975 (E). Official Information Act 1982 (E); Local Government Official Information and Meetings Act 1987 (E)
	Miscellaneous	✓	✗	Bill of Rights Act 1990 (E)
Spam Laws	**Anti-spam regulation**	✓	✗	Unsolicited Electronic Messages Act 2007 (E)
Online Child Safety Laws	**General child pornography offences**	✓	✗	Films, Videos, and Publications Classification Act 1993 (E)
	Computer-facilitated child pornography offences (Title 3 COE)	✗	✗	

Part 2 – Legal and Regulatory Position

2.1 COMPUTER SECURITY LAWS – CURRENT LEGISLATIVE FRAMEWORK

Core offences (Title 1 COE): Illegal access, illegal interception, data interference, system interference, misuse of devices

In 2003, the New Zealand government revised the Crimes Act 1961 to better address new threats to computer security. This involved the enactment of specific computer-related offences and the extension of existing offences to apply to computer-facilitated criminal activity.

To commit New Zealand's unauthorised access offence, a person must intentionally access a computer system without authorisation and with the requisite mental element: knowledge of the absence of authorisation or recklessness as to whether authorisation exists. In a departure from the Convention framework, it is not an offence to exceed one's authority by accessing a computer system for purposes other than those for which access was given. Offenders are liable to imprisonment for a term of up to two years.

Although the Crimes Act does not contain an offence that specifically contemplates computer-related interception, the broad terms of the general interception offence in section 216B of the Crimes Act will apply to this type of interception, so long as the transmitted data can be said to be a private communication – one where the circumstances indicate the communication's private nature and it is not unreasonable to expect that the communication will not be intercepted. This permutation of the illegal interception offence is punishable by imprisonment for up to two years.

Section 250 of the Crimes Act enacts data and system interference offences that are broadly equivalent to that found in the Convention. If anything, the Crimes Act offences are likely to regulate a broader range of conduct than their Convention counterparts due to their application to reckless data and system interference in addition to that caused intentionally. Those who commit the data and system interference offences in the Crimes Act will ordinarily be liable to imprisonment for up to seven years; higher penalties apply if the offender engages in system interference with actual or constructive knowledge that danger to life is likely to result.

Finally, the Crimes Act contains a limited misuse of devices offence. Section 251 criminalises the sale and possession of software that enables a person to access a computer system for the purpose of (i) committing a crime or (ii) facilitating the commission of a crime. Offenders are liable to imprisonment for a term of up to two years.

Computer-related offences (Title 2 COE): Computer-related forgery, computer-related fraud

Computer-related forgery is criminalised by the general forgery offence in section 256(2) of the Crimes Act, a result made possible by the extension of the definition of "document" to embrace both electronic data and data storage devices.

The Crimes Act offence that criminalises access for dishonest purposes is more akin to the Convention's computer-related fraud offence than it is to the Convention's illegal access offence. Section 249(1) of the Crimes Act makes it an offence to access a computer system and thereby, dishonestly and by deception, and without a belief that the act is lawful, obtain property or any other benefit, or cause any loss to any person. Contrary to the Convention, this offence does not require interference with data or a computer system in the commission of the fraud, and it is irrelevant to liability whether access is authorised or unauthorised. Offenders can face up to seven years imprisonment if a dishonest benefit is obtained or loss caused; the lesser penalty of up to five years imprisonment results if there is intent to dishonestly obtain a benefit or cause loss to another person, but no such gain or benefit results.

Ancillary liability (Title 5 COE): Attempt and aiding/abetting, corporate liability

In line with the Convention framework, the Crimes Act makes it an offence to attempt, aid or abet the commission of an offence. Although corporate criminal liability is established under New Zealand law, no express provision is made for it under the Crimes Act. Instead, case law provides that corporate criminal liability will arise when the individual responsible for the alleged conduct has actual authority within the company in relation to the alleged conduct.

2.2 COMPUTER SECURITY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

At the date of writing, there are no upcoming legislative developments that relate to computer security.

2.3 PRIVACY LAWS – CURRENT LEGISLATIVE FRAMEWORK

Data protection

New Zealand's Privacy Act 1993 establishes a data protection regime which applies broadly to private and public sector organisations that deal with personal information. The Act defines personal information as "information about any identifiable individual", and requires each "agency" under its jurisdiction to comply with the 12 information privacy principles summarised below:

- **Purpose of collection of personal information:** Personal information may only be collected for a lawful purpose connected with a function or activity of the agency, and the collection of personal information must be necessary for that purpose;
- **Source of personal information:** Personal information must be collected directly from the data subject, except in certain limited circumstances (including where collection of the information from someone else would not prejudice the interests of the data subject);
- **Collection of information from subject:** When personal information is collected directly from the data subject, the agency must take reasonable steps to ensure that the data subject is aware of certain matters, including (i) the fact of collection, (ii) the purpose of collection, (iii) intended recipients of the personal information, (iv) details of the collecting and holding agencies, and (v) the data subject's right of access and correction, except in certain limited circumstances;
- **Manner of collection of personal information:** Personal information may not be collected by means that are unlawful, unfair or that intrude on the personal affairs of the data subject;
- **Storage and security of personal information:** Personal information must be reasonably secured against loss, unauthorised access and misuse;
- **Access to personal information:** Where personal information is held in such a way that it can be readily retrieved, the data subject is entitled to confirmation from the agency that the information is held, and to have access to that information;
- **Correction of personal information:** The data subject is entitled to seek correction of his or her personal information or a record to be made of any corrections sought but not made;

9. New Zealand

- **Accuracy of personal information to be checked before use:** Personal information must be checked before use to make sure that it is accurate, up to date, complete, relevant and not misleading;
- **Agency not to keep personal information for longer than necessary:** Personal information must not be kept for longer than is necessary for the purposes for which the information may lawfully be used;
- **Limits on use of personal information:** Personal information obtained for one purpose must not be used for any other purpose, except in certain limited circumstances;
- **Limits on disclosure of personal information:** An agency may only disclose personal information to another person or body in certain circumstances, including where disclosure is within the primary purpose of collection or is directly related to a purpose of collection;
- **Unique identifiers:** An agency must not assign a unique identifier to a data subject unless the assignment of that identifier is necessary to enable the agency to carry out its functions efficiently.

Each of the above information privacy principles is enforceable via the Privacy Act's complaints procedure. Complaints are initially filed with the Privacy Commissioner who attempts to conciliate the matter. If conciliation fails, the Privacy Commissioner may refer the matter to the Director of Human Rights Proceedings who will decide whether proceedings should be instituted before the Human Rights Review Tribunal. An aggrieved individual is also entitled to bring the matter before the Human Rights Review Tribunal without the intervention of the Privacy Commissioner in certain circumstances. In the Tribunal, complainants may seek a range of remedies including damages, declarations and orders. There is a right of appeal from the Human Rights Review Tribunal to the High Court of New Zealand.

The complaints procedure discussed above will not necessarily apply to all disputes in relation to personal information. This is because certain sectors of the economy are regulated by codes of practice issued under the Privacy Act that vary the Act's dispute resolution procedure. More importantly, these codes of practice modify the application of one or more of the information privacy principles by prescribing standards that take account of privacy concerns in the sector to which the code relates. At the time of writing, three sectoral codes addressing all 12 information privacy principles have been issued under the Privacy Act: the Health Information Privacy Code 1994; the Telecommunications Information Privacy Code 2003 (which applies to traditional carriers, ISPs and related businesses such as publishers of phone directories); and the Credit Reporting Privacy Code 2004. A number of more narrowly focused codes have been also issued, such as the Superannuation Scheme Unique Identifier Code 1995, Justice Sector Unique Identifier Code 1998 and the Post-Compulsory Education Unique Identifier Code 2001.

Surveillance

As mentioned in section 2.1 earlier, the Crimes Act makes it an offence to intentionally intercept private communications by means of an interception device. However, police and other security officers may intercept communications in accordance with their powers granted under acts such as the Crimes Act 1961, Misuse of Drugs Amendment Act 1978, New Zealand Security Intelligence Service Act 1969 and the Government Communications Security Bureau Act 2003. Typically these powers require police and other security officers to obtain a warrant from a judge, minister or other high-ranking official who must be satisfied of the need for interception of the kind proposed. Pursuant to the Crimes Act 1961, it is a specific offence to disclose information obtained during the execution of an interception warrant; this offence is punishable by imprisonment for a term of up to two years.

The Crimes (Intimate Covert Filming) Amendment Act 2006 came into force in December 2006. The Act criminalises the making of an intimate visual recording, the possession of an intimate visual recording, and the publishing, importing, exporting, or selling of an intimate visual recording. An "intimate visual recording" is defined as a visual recording (e.g. a photograph, videotape or digital image) that is made in any medium, using any device, without the knowledge or consent of the subject of the recording, where the subject is recorded in a place which would reasonably be expected to provide privacy (e.g. a changing room), and that person is:

- naked, or has the sexual parts of his or her body exposed, or clad solely in undergarments;
- engaged in intimate sexual activity; or
- engaged in showering, toileting, or other personal bodily activity that involves dressing or undressing.

The definition of intimate visual recording also covers acts colloquially known as "up-skirt" or "down-blouse" filming.

The prohibition on making an intimate visual recording uses an extended definition of "intimate visual recording" that captures streamed content and other recordings that are made and transmitted in real time without being stored or retained in (i) a physical form, or (ii) an electronic form from which the recording is capable of being reproduced.

The offences in the Act are punishable by imprisonment for up to three years, other than the offence of simple possession of an intimate visual recording (i.e. possession without intent to distribute), which is punishable by imprisonment for up to one year.

Secrecy and freedom of information

New Zealand has a range of laws that impose obligations of secrecy on persons who handle certain types of sensitive information. These laws include the Tax Administration Act 1994, Electoral Act 1993 and Ombudsmen Act 1975.

The Official Information Act 1982 requires official (i.e. public sector) information to be made available on request unless there is a good reason to withhold it. The regime enacted by this Act reverses the presumption of secrecy that prevailed under the repealed Official Secrets Act 1951, and this principle of availability is repeated in respect of information held by local authorities subject to the Local Government Official Information and Meetings Act 1987.

Miscellaneous

After much speculation, in March 2004, a majority of the Court of Appeal confirmed the existence of a tortious action for the invasion of privacy by publication of private facts. To successfully recover under this new tort, the plaintiff must show (i) a reasonable expectation of privacy in respect of the matter published and (ii) publicity that is highly offensive to a reasonable person. It is a defence to publish private facts of "legitimate public concern" sufficient to outweigh the harm likely to be caused by the loss of privacy. The usual remedy for invasion of privacy will be damages, although an injunction to prevent publication will be available in compelling cases.

Article 21 of the Bill of Rights Act 1990 affirms the right of New Zealand citizens to be secure against unreasonable search or seizure. This article has been interpreted by the Court of Appeal as protecting the important values and interests that make up the right of privacy. However, since the Bill of Rights Act 1990 is not entrenched legislation, and it only applies in respect of acts done by the legislative, executive, or judicial branches of the government, or by a person or body in the performance of a public function, this Act does not provide comprehensive constitutional protection of rights to privacy.

2.4 PRIVACY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

The Privacy Commissioner sought submissions in April and May 2007 on proposed amendments to the Health Information Privacy Code 1994. The proposed amendments include increasing the list of agencies permitted to use the National Health Index numbers used to identify patients, and allowing health practitioners to disclose a person's genetic information to a genetic relative where disclosure is necessary to lessen or prevent a serious threat to the life or health of the person to whom the disclosure is made.

The Privacy Commissioner has also proposed draft privacy breach guidelines, which are, for the most part, harmonised with those recently released by the Canadian Privacy Commissioner. Public comment on these voluntary guidelines is due in late September 2007. The draft guidelines recognise that managing a privacy breach has four stages: (i) containing the breach and preliminary assessment, (ii) evaluating the risks, (iii) considering or undertaking notification, and (iv) implementing prevention strategies. The draft guidelines also recognise that breach notification is not appropriate for all privacy breaches and suggest that individuals affected by a breach should only be notified where there is a risk of harm to that individual. The types of harm mentioned by the Privacy Commissioner in the draft guidelines include humiliation and damage to reputation or relationships that may, for example, arise out of privacy breaches involving mental health, medical or disciplinary records. Where notification is appropriate, the Privacy Commissioner has expressed a preference for notification to be by direct communication (e.g. by email or telephone). The draft guidelines recommend that indirect notification (e.g. by a website notice) should only occur where direct notification could cause further harm, is prohibitive in cost or the contact information for affected individuals is not known.

2.5 SPAM LAWS – CURRENT LEGISLATIVE FRAMEWORK

New Zealand's Unsolicited Electronic Messages Act 2007 (UEM Act) came into force in September 2007. This legislation has essentially the same structure as Australia's Spam Act. The UEM Act prohibits the sending of unsolicited commercial electronic messages with a New Zealand link. A commercial electronic message is defined as an electronic message (other than a voice call or fax message) that:

- markets or promotes goods, services, land, or a business investment opportunity;
- assists a person to dishonestly obtain a financial advantage; or
- links to a message that contains any of the things mentioned in the bullet points above.

The UEM Act also specifies certain types of messages that are excluded from the definition of commercial electronic message, including messages that provide:

(i) a quote where one has been requested;

(ii) warranty or product recall information;

(iii) factual information about a subscription, membership account or similar relationship;

(iv) goods or services including product updates or upgrades that the recipient is entitled to receive under the terms of a transaction; or

(v) content for a purpose specified in regulations under the Act. At the date of writing there are no regulations under the Act.

9. New Zealand

The exclusions in paragraphs (ii) to (iv) correspond to the definition of "transactional or relationship message" in the United States' CAN-SPAM Act.

A message has a New Zealand link if, among other things, it originates from New Zealand, the device used to access the message is in New Zealand, the recipient is an organisation carrying on business in New Zealand, it is sent to an electronic address that ends with '.nz', or it is sent to an electronic address that does not exist but it is reasonably likely that the message would have been accessed using a device located in New Zealand.

Where a user has consented to receiving a commercial electronic message with a New Zealand link, sending that message is permissible so long as it contains (i) accurate sender identity and contact information, and (ii) a functional unsubscribe facility that is presented in a clear and conspicuous manner.

The UEM Act contemplates that a person's consent to receiving a commercial electronic message may be express, inferred or deemed. Express consent can be given by the electronic address-holder or any other person who uses the relevant electronic address. Inferred consent arises from (i) the conduct and the business and other relationships of the persons concerned, and (ii) any other circumstances specified in the regulations. Lastly, deemed consent can, subject to any regulations made under the UEM Act, arise from conspicuous publication of electronic addresses in certain circumstances.

The UEM Act also prohibits the use of electronic address harvesting software or harvested electronic address lists in connection with, or with the intention of, sending unsolicited commercial electronic messages in contravention of the UEM Act. In addition, the UEM Act prohibits aiding, abetting, counselling, procuring, inducing or being concerned with a contravention of the Act.

Turning to the UEM Act's enforcement provisions, people affected by conduct that contravenes the UEM Act can seek an injunction in the High Court, or make an application to the District Court or the High Court (depending on the amount claimed) for compensation or damages.

The UEM Act also contemplates government-led enforcement by the Department of Internal Affairs (DIA). The DIA can commence proceedings against infringers seeking the imposition of pecuniary penalties of up to NZ$200,000 (approximately USD$140,430) for individuals and NZ$500,000 (approximately USD$352,040) for corporations. Those who have suffered loss as a result of spam, including ISPs, can also apply to the District Court or the High Court to join an action initiated by the DIA. The DIA can also issue formal warnings, civil infringement notices (that specify a penalty to be paid), seek enforceable undertakings from spammers, or seek an order from the District Court or the High Court for the undertaking to be enforced.

Finally, the UEM Act contains a 'safe harbour' for ISPs and other service providers whose telecommunications services enable infringing electronic messages to be sent. The UEM Act does not, however, expressly reject any obligation on ISPs to carry or block certain types of electronic messages.

Other laws

New Zealand's existing criminal and harassment laws may also regulate certain spamming techniques. As discussed above, the Crimes Act makes it an offence to intentionally or recklessly, and without authorisation, cause a computer system to fail. Such failure could conceivably result from sending large volumes of spam to a particular system. Further, the Harassment Act 1997 provides that where a person is sending emails as a pattern of behaviour designed to harass another person, action can be taken against the sender.

The content of spam emails may offend the Fair Trading Act 1986, Crimes Act 1961 and the Films, Videos and Publications Classification Act 1993. Finally, the collection and use of personal information in the course of spamming may offend the Privacy Act 1993.

Spam Code of Conduct

InternetNZ (The Internet Society of New Zealand Inc), the TCF (Telecommunications Carriers' Forum), the Marketing Association, and ISPANZ (The ISP Association of New Zealand) have released a self-regulatory code of practice for service providers regulated by the Unsolicited Electronic Messages Act 2007. A service provider is defined, both in the UEM Act and in the Code as someone who provides services, goods or equipment to facilitate telecommunication. The Code sets out minimum acceptable practices for service providers in relation to minimising and managing spam. The Code covers cooperation with law enforcement agencies, making spam filters available, reporting requirements and complaints handling processes, among other things.

The mechanism to be used for implementing the Spam Code has not yet been determined. It is possible that the Code could be approved in accordance with the provisions of the Telecommunications Act 2001. This would make the Code enforceable and service providers could be fined or forced to pay damages if found to be in breach.

2.6 SPAM LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

Apart from the possibility of the Spam Code of Practice mentioned in section 2.5 being approved by the Commerce Commission, at the date of writing there are no upcoming legislative developments that relate to spam.

2.7 ONLINE CHILD SAFETY LAWS – CURRENT LEGISLATIVE FRAMEWORK

General child pornography offences

The age of majority in New Zealand is 20 years; the age of consent to sexual relations is 16 years.

New Zealand has not enacted specific legislation to combat child pornography. Instead, child pornography falls under a general ban on objectionable publications in the Films, Videos, and Publications Classification Act 1993 (Classification Act). The definition of publication is broad and encompasses everything from writings and drawings to sound recordings and digital images. Case law has confirmed that in addition to depictions of real children, cartoons, fictional text, "morphed" images and pictures of adults dressed to appear as children can be found objectionable, and since there is no requirement for actual sexual activity, photographs of nude children in sexual poses are also covered.

Pursuant to the Classification Act, it is illegal to make, supply, give, offer, advertise, display, exhibit, possess, export or import (including by email or fax) an objectionable publication. Both mere possession and possession with intent to distribute are criminalised; case law is progressively clarifying what these offences involve (i.e what constitutes possession). So far, it has been established that electronic evidence of former possession of objectionable material is sufficient to obtain a conviction, and a person can be convicted for the offence of possession if he or she is known to possess material and exercises potential control of the material.

Irrespective of whether the offender knew that the publication in question (i.e. the child pornography material) was objectionable, individual offenders can face fines of up to NZD$10,000 (approximately USD$7,020) and body corporates can face fines of up to NZD$30,000 (approximately USD$21,050) for offending the provisions of the Classification Act. Higher sanctions apply where the offender knew, or had reason to believe, that the child pornography material was objectionable – individual offenders can be liable to imprisonment for up to 10 years or a fine of up to NZD$50,000 (approximately USD$35,100), and body corporates can be liable to a maximum fine of up to NZD$200,000 (approximately USD$140,430). When determining the sentence for these latter knowledge-based offences, courts must take into account as an aggravating factor the extent to which the offending publication (i) promotes the sexual exploitation of children, (ii) depicts sexual conduct with or by children or (iii) exploits the nudity of children.

Finally, to ensure New Zealand's compliance with its obligations under the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography to the UN Convention on the Rights of the Child, sections 145A to 145C of the Classification Act establish extra-territorial jurisdiction in respect of child pornography offences. For that purpose, child pornography is defined as (i) a representation of a person who is or appears to be under 18 years of age engaged in real or simulated explicit sexual activities, or (ii) a representation of the sexual parts of a person under 18 for primarily sexual purposes.

Computer-facilitated child pornography offences (Title 3 COE)

New Zealand does not have any legislation that creates computer-facilitated child pornography offences.

Miscellaneous

New Zealand's Crimes Act 1961 contains a 'sexual grooming' offence that is capable of online application. Section 131B sanctions those who, having communicated or met with a young person (a person under the age of 16) on an earlier occasion, either (i) intentionally meets the young person (a person under the age of 16), (ii) travels with the intention of meeting the young person or (iii) arranges for the young person to travel to meet him or her. The groomer must take the steps mentioned above with the intention that he or she, or the young person concerned, will take action that would amount to a sexual offence pursuant to the Crimes Act. Offenders are liable to imprisonment for up to seven years; a groomer can avail him or herself of a statutory defence where he or she can demonstrate that he or she (i) took reasonable steps to find out whether the young person was at least 16 years old or (ii) believed on reasonable grounds that the young person was at least 16 years old.

It is also an offence punishable by up to seven years imprisonment to organise or promote child sex tours outside New Zealand.

2.8 ONLINE CHILD SAFETY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

At the date of writing, there are no upcoming legislative developments that relate to online child safety.

9. New Zealand

Part 3 – Benchmark Comparison

Key: Favourable alignment | Moderate alignment | Weak alignment

(E) Enacted
(P) Pending
(Title [x]) Title [x] of the Council of Europe Convention on Cybercrime

Area	Legislative regime to be compared with benchmark	Benchmark legislation	Overall alignment	Areas of strong alignment	Areas of moderate alignment	Areas of weak alignment
Computer Security Laws	Crimes Act 1961 (E)	Council of Europe Convention on Cybercrime (Titles 1, 2 and 5)		• Data and system interference offences • Computer-related forgery offence • Ancillary liability for attempting, aiding or abetting cybercrimes	• Illegal access, illegal interception and misuse of devices offences • Computer-related fraud offence • No express provision for corporate criminal liability but case law supports corporate criminal liability	
Privacy Laws	Privacy Act 1993 (E)	Model Privacy Bill (drafted by Microsoft)		• Transparency matters that must be notified to data subject (e.g. the identity of the entity that collects data and the purposes of use of the personal information) • Obligation to keep personal information free from loss or unauthorised disclosure or destruction • Data subject's right to access and correct personal information • No restrictions on transborder data flows	• Definition of personal information • Distinction between primary and secondary purposes of use and disclosure • Mode of enforcement (enforcement by individual or Commissioner cf. enforcement by Commissioner) • Consequence of infringement (civil liability cf. statutory and civil liability)	• 'Opt-in' regime to use or disclose personal information for a secondary purpose • Exemptions for some entities e.g. news agencies in respect of their news functions, courts and tribunals in respect of their judicial functions • No additional obligations in respect of sensitive information • No protected disclosures to affiliates with common privacy practices • No breach notification provisions
Spam Laws	Unsolicited Electronic Messages Act 2007 (E)	Anti-spam legislation checklist (drafted by Microsoft)		• Transparency requirements (sender identification, functional unsubscribe facility) • Address harvesting measures • Exclusion of pre-existing business relationship messages from the definition of commercial electronic message	• Capped statutory fines (pursued by enforcement department) in addition to civil liability in damages • ISP safe harbour for transmitting infringing messages but no express exclusion of obligation on ISPs to carry or block certain electronic messages	• 'Opt-in' regime for unsolicited commercial electronic messages (but note that transactional or relationship messages are excluded) • Private right of action for all persons affected by spam (and not just ISPs/email service providers)
Online Child Safety Laws	Films, Videos, and Publications Classification Act 1993 (E)	Council of Europe Convention on Cybercrime (Title 3 COE)/ICMEC principles			• General prohibitions on distribution and possession (including mere possession) of objectionable publications • Child sex abuse images are an aggravating factor in sentencing	• No definition of child pornography • No general or computer-facilitated child pornography offences • No scope for ISP reporting of dealing in child pornography

10. The Philippines

Part 1 – Snapshot of Legislative Status

Key: (E) Enacted
(P) Pending
(Title [x] COE) Title [x] of the Council of Europe Convention on Cybercrime (COE)

Area	Topic	Enacted legislation	Pending legislation	Relevant instruments/Comments
Computer Security Laws	**Core offences (Title 1 COE):** illegal access, illegal interception, data interference, system interference, misuse of devices	✓	✓	Electronic Commerce Act (E) Anti-Wire Tapping Act (E) Cybercrime Prevention Act of 2007 (P)* Anti-Computer Fraud and Abuses Act of 2007 (P)
	Computer-related offences (Title 2 COE): computer-related forgery, computer-related fraud	✓	✓	Revised Penal Code (E) Cybercrime Prevention Act of 2007 (P)* Anti-Computer Fraud and Abuses Act of 2007 (P)
	Ancillary liability (Title 5 COE): attempt; aiding/abetting, corporate liability	✗	✓	Cybercrime Prevention Act of 2007 (P)*
Privacy Laws	**Data protection**	✗	✗	Constitutional right of privacy. No comprehensive data protection regulation, however the Department of Trade and Industry has promulgated an administrative order that contains voluntary guidelines for the protection of personal data held by private sector organisations.
	Surveillance (see illegal interception under computer security)	✓	✗	Anti-Wire Tapping Act (E)
	Sensitive information	✓	✗	Secrecy of Bank Deposits Act (E)
Spam Laws	**Anti-spam regulation**	Partial	✓	No general legislation but see implementing rules on sending spam messages by SMS and MMS under the Telecommunications Policy Act (E) Cybercrime Prevention Act of 2007 (P)*
Online Child Safety Laws	**General child pornography offences**	✗	✗	No general child pornography regulation but use of children in production of pornography is prohibited under the Special Protection of Children Against Abuse, Exploitation and Discrimination (E)
	Computer-facilitated child pornography offences (Title 3 COE)	✗	✓	Cybercrime Prevention Act of 2007 (P)* Internet Indecency Act (P)

*It is understood that the proposed Cybercrime Prevention Act of 2007 (HB 190) is closely based on the proposed Cybercrime Prevention Act of 2005 (HB 3777), which was introduced (but not passed) by the previous congress, the 13th Congress of the Republic of the Philippines. The analysis that follows is based on the Cybercrime Prevention Act of 2005 (HB 3777) since a translation of the Cybercrime Prevention Act of 2007 (HB 190) was not available at the time of writing.

Part 2 – Legal and Regulatory Position

2.1 COMPUTER SECURITY LAWS – CURRENT LEGISLATIVE FRAMEWORK

Key: (RA) Republic Act
(HB) House Bill

Core offences (Title 1 COE): Illegal access, illegal interception, data interference, system interference, misuse of devices

The Electronic Commerce Act (RA 8792) is the key source of enacted computer security regulation in the Philippines. Its broad provisions define "hacking" or "cracking" as:

- unauthorized access into or interference with an information system; or
- any access in order to corrupt, alter, steal or destroy electronic data or electronic documents using a computer or other similar information and communication devices. Such access must be without the knowledge and consent of the owner of the information system.

The first type of hacking or cracking is understood to cover denial of service attacks and simple hacking to test the security vulnerability

of an information system. The second variety of hacking or cracking is intended to cover the introduction of viruses into a computer system and is broadly equivalent to the data interference offence under the Convention on Cybercrime. Criminal liability attaches to offences under the Electronic Commerce Act and penalties include fines (minimum PhP100,000 (approximately USD$2,250)) and mandatory imprisonment (for between six months and three years). Civil remedies can also be pursued and may include compensatory and punitive damages.

The Anti-Wire Tapping Act (RA 4200) prohibits any person from using a device to secretly overhear, intercept or record private communications without the authorisation of the parties to that communication. A peace officer may apply for a written court order to secretly overhear or intercept private communications in cases involving national security. Despite the fact that evidence gathered from unauthorized tapping is inadmissible in court, it has been reported that unauthorised tapping is not uncommon in the Philippines.

Computer-related offences (Title 2 COE): computer-related forgery, computer-related fraud

The Revised Penal Code (Act No 3815) makes it an offence for a person to defraud or damage another by deceit. This offence is likely to cover impersonation of another through a computer where such impersonation is intended for a deceitful or fraudulent purpose.

Ancillary liability (Title 5 COE): Attempt and aiding/abetting, corporate liability

There are no pre-emptive legal provisions in the Philippines that address situations where an offence has not yet been committed. Corporate liability is not expressly addressed in the Electronic Commerce Act.

2.2 COMPUTER SECURITY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

Core offences (Title 1 COE): Illegal access, illegal interception, data interference, system interference, misuse of devices

In July 2007, the draft Cybercrime Prevention Act of 2007 (HB 190) was filed in the Philippines Congress and referred to the Committee on Justice for discussion and debate. It is understood that the proposed Cybercrime Prevention Act of 2007 (HB 190) is a further iteration of the proposed Cybercrime Prevention Act of 2005 (HB 3777), which was introduced (but not passed) by the previous congress, the 13th Congress of the Republic of the Philippines. It is expected that the latest iteration of the Cybercrime Prevention Act will be enacted in late 2007. Since a translation of the Cybercrime Prevention Act of 2007 (HB 190) was not available at the time of writing, the analysis that follows is based on the Cybercrime Prevention Act of 2005 (HB 3777).

The proposed Cybercrime Prevention Act of 2005 is closely modelled on the Council of Europe's Convention on Cybercrime. In fact, the proposed Act almost identically reproduces the Convention's provisions relating to illegal access, illegal interception, data interference, system interference and misuse of devices. However, these offences are included as part of an inclusive list of offences. Proposed section 4A of the Cybercrime Prevention Act of 2005 criminalises any act committed through an electronic operation that targets the security of a computer or communications system or network or the data processed by them, and specifically includes the Convention's illegal access, illegal interception and misuse of devices offences. Similarly, proposed section 4B criminalises the input, alteration, erasure or suppression of computer or communication data or interference with a computer or communication system or network with intent to hinder the functioning of the system or network, and specifically includes the Convention's data interference and system interference offences.

Important departures from the Convention framework include (i) that interception of communications is not illegal unless there is a "reasonable expectation of privacy"; (ii) it is not unlawful for an officer, employee or agent of a service provider to intercept, disclose or use a communication while engaged in an activity necessary to perform the particular service, or when protecting the service provider's rights or property; (iii) that system interference can involve reckless interference and can result in damage to computer programs and electronic documents and messages in addition to computer data; (iv) that use of a device to facilitate the commission of a core offence described above is prohibited; (v) the proposed misuse of devices offence doesn't extend to dealings in, or possession of, devices used to commit the Convention's data interference and system interference offences; and (vi) it is not an element of the proposed misuse of devices offence that dealings with devices must be with intent to commit the proposed illegal access and illegal interception offences. The proposed Cybercrime Prevention Act makes the core offences discussed above punishable with a fine of at least PhP100,000 (approximately USD$2,250) and mandatory imprisonment.

The proposed Anti-Computer Fraud and Abuses Act of 2007 is currently being considered by the Committee on Science and Technology. It is uncertain when the Act is expected to be passed. The proposed Act addresses each of the these core offences (except misuse of devices) in accordance with the Convention framework. It also seeks to establish a number of computer security offences in relation to unauthorised access, interception and damage to information held on computer systems belonging to the Government, and in some cases, financial institutions operating in the Philippines. The penalties for committing core offences under the proposed Anti-Computer Fraud and Abuses Act are noticeably

stricter than those imposed by the Cybercrime Prevention Act: imprisonment is for a term of between eight and 20 years; fines can extend up to PhP1,000,000 (approximately USD$22,550).

Computer-related offences (Title 2 COE): computer-related forgery, computer-related fraud

The proposed Cybercrime Prevention Act of 2005 implements the Convention's computer-related fraud offence (manipulation of data or system interference with intent to gain an economic benefit). The proposed Act also contains an offence that is similar to the Convention's computer-related forgery offence: it is an offence to input, alter, erase or suppress (i) any computer or communication data or program, electronic document or data message, or (ii) interfere with a computer and electronic communication system or network, in a manner that would constitute the offence of forgery under the Revised Penal Code. The computer-related forgery offence in the Cybercrime Convention contains the requirement that the offender commit the prohibited acts intending that the data is considered or acted upon for legal purposes as if it was authentic; it is unclear whether a similar requirement exists in the Revised Penal Code's offence of forgery. The proposed computer-related fraud and forgery offences in the Cybercrime Prevention Act are punishable by a fine of at least PhP100,000 (approximately USD$2,250) and mandatory imprisonment.

The proposed Anti-Computer Fraud and Abuses Act of 2007 defines both computer forgery and fraud in a manner similar to the proposed Cybercrime Prevention Act. In addition, the proposed Anti-Computer Fraud and Abuses Act creates special offences in relation to computers belonging to certain private financial institutions/agencies and the Filipino government. These offences are punishable by imprisonment for a term of between eight and 20 years and fines of up to PhP1,000,000 (approximately USD$22,550). Finally, the Anti-Computer Fraud and Abuses Act authorises the National Security Council to investigate computer-related crimes in contravention of the proposed Act, particularly where the violation affects national security.

Ancillary liability (Title 5 COE): Attempt and aiding/abetting, corporate liability

The aiding and abetting provision in the Cybercrime Prevention Act of 2005 directly mirrors that found in the Convention on Cybercrime: liability accrues when a person willfully aids or abets a person in the commission of an offence under the proposed Act. This, however, is not the case for the proposed Act's attempt and corporate liability provisions. Instead of requiring simple attempt, the proposed Act requires a conspiracy (an agreement to commit an illegal act) plus steps to carry out the conspiracy; corporate liability is imposed on the corporation's high-ranking officers and employees rather than on the corporation itself.

The proposed Anti-Computer Fraud and Abuses Act of 2007 does not expressly consider attempt, aiding/abetting or corporate liability.

2.3 PRIVACY LAWS – CURRENT LEGISLATIVE FRAMEWORK

Data protection

The Philippines does not have any specific data protection legislation. However, Filipinos enjoy a right to privacy under the Constitution's Bill of Rights.

In 2006, the Department of Trade and Industry released an administrative order that applies in respect of personal data held by private sector organisations in information and communications systems. The order contains a number of principles to guide private sector organisations in the development of their personal data protection policies; some of the order's principles bear a resemblance to those found in the APEC Privacy Framework. The order also contemplates the establishment of Data Protection Certifiers – independent third parties accredited by the Department of Trade and Industry to certify, monitor and oversee an organisation's privacy program, and the publication of a list of private sector organisations that have had their privacy programs accredited by a Data Protection Certifier. Compliance with this administrative order is entirely voluntary; its aim is to encourage private sector organisations to adopt privacy policies rather than to penalise them for not doing so.

Surveillance

See the discussion regarding the Anti-Wire Tapping Act in section 2.1 earlier.

Sensitive information

Other than the Secrecy of Bank Deposits Act (RA 1405), the Philippines does not have any legislation that specifically addresses sensitive information. The Secrecy of Bank Deposits Act prohibits banks from disclosing any information relating to bank deposits or investment in government bonds of its customers without the customer's written consent, except in certain limited circumstances.

Miscellaneous

The implementing rules under the Electronic Commerce Act require online businesses to make available to consumers and business users (where appropriate) the means to exercise choice with respect to privacy, confidentiality, content control and anonymity (where appropriate).

10. The Philippines

2.4 PRIVACY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

Miscellaneous

The proposed National Identification Card System Act (HB 0217) seeks to establish an identification card system in the Philippines. The current draft of the bill does not appear to contemplate the associated privacy risks and proposes to incorporate the following personal information on an identity card: full name, residential address, date of birth, gender, height and weight, nationality and signature.

2.5 SPAM LAWS – CURRENT LEGISLATIVE FRAMEWORK

Although the Philippines has not enacted comprehensive spam regulation to date, the National Telecommunications Commission (NTC) has issued implementing rules on broadcast messaging services pursuant to the Public Telecommunications Policy Act of the Philippines (RA 7925). These rules establish an opt-in regime (with scope for prior consent) for receiving unsolicited commercial messages and subscription messages sent by SMS or MMS. All such messages must identify the sender and provide sender contact details. Those who send unsolicited commercial messages or subscription messages without (i) the recipient's prior consent or (ii) the recipient having opted-in are liable for "appropriate administrative and penal sanctions, in accordance with law". No further guidance is given as to what these sanctions may involve.

2.6 Spam Laws – Upcoming legislative developments

The proposed Cybercrime Prevention Act of 2005 (HB 3777) establishes an opt-out regime in respect of commercial electronic communications. Such communications must contain an unsubscribe facility, not intentionally disguise the source of the electronic message or include misleading information in order to induce a recipient to read the message. The term "commercial electronic communication" is not defined, but it appears to embrace electronic messages which seek to advertise, sell or offer for sale products and services. Persons acting in contravention of this section could face imprisonment and/or fines of between PhP100,000 (approximately USD$2,270) and PhP600,000 (approximately USD$13,600).

2.7 ONLINE CHILD SAFETY LAWS – CURRENT LEGISLATIVE FRAMEWORK

General child pornography offences

The age of consent in the Philippines is 12 for boys and girls alike.

The Philippines' Revised Penal Code (Act No 3815) does not draw a distinction between adult and child pornography. The Code contains a general ban on obscene material and prohibits the selling, giving away and exhibition of obscene material. The mere possession or receiving of obscene material is not illegal.

The Special Protection of Children Against Child Abuse, Exploitation and Discrimination Act (RA 7610) contains specific prohibitions on the use of children in pornographic productions and shows. A child is defined as a person under 18 years or a person older than 18 years who is unable to care for him or herself. Parents and other caregivers who cause or allow their children to be used in obscene productions are liable to the same punishment (which includes imprisonment) as the principal. The Act also makes it an offence to promote or facilitate child prostitution and to engage in trading or dealing with children.

Computer-facilitated child pornography offences (Title 3 COE)

Although the Revised Penal Code contains a general ban on obscene material, currently there is a gap with regard to internet pornography. This is because much of the pornographic material distributed over the internet cannot be said to be sold, given away or exhibited contrary to the provisions of the Penal Code. No other Filipino legislation appears to address this gap left by the Penal Code.

Miscellaneous

In 2003, the Philippines became the first country in South East Asia to enact a comprehensive anti-trafficking in persons law. The Anti-Trafficking in Persons Act of 2003 (RA 9208) makes it unlawful to engage in acts of trafficking that lead to prostitution, pornography, forced labor and other forms of exploitation. Acts that promote trafficking, such as allowing a house to be used to promote trafficking, are similarly prohibited. While the law does not specifically apply to online crimes, it does take the anti-mail order bride law a step further and makes it illegal to introduce or match any Filipino woman to a foreign national through a mail order marriage system for the purpose of acquiring, buying, offering, selling, or trading her to engage in prostitution, pornography, forced labor or other forms of exploitation. Sanctions and penalties for this offence and other acts of trafficking are stiffer as well, ranging from 6 years to life imprisonment and fines of up to PhP2,000,000 (approximately USD$45,330). Importantly, trafficking a child (a person below the age of 18 years or who is over 18 but unable to care for him or herself) is penalised more harshly: offenders face life imprisonment and a fine of between PhP2,000,000 (approximately USD$45,330) and PhP5,000,000 (approximately USD$113,320).

2.8 ONLINE CHILD SAFETY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

Computer-facilitated child pornography offences (Title 3 COE)

In addition to those security-related offences mentioned in section 2.2 earlier, the proposed Cybercrime Prevention Act of 2005 also introduces computer-facilitated child pornography offences punishable with a fine of between PhP200,000 (approximately USD$4,530) and PhP800,000 (approximately USD$18,150) and mandatory imprisonment. Once again, these offences closely reflect the equivalent provisions in the Convention on Cybercrime. The definition of child pornography in the proposed Act covers visual depictions of minors and persons appearing to be minors, but does not embrace "realistic images representing a minor". However, this does not result in any inconsistency with the Convention requirements; parties may opt not to include "realistic images representing a minor" in the definition of child pornography. It is prohibited to possess, produce, offer, make available or distribute child pornography using a computer. Procuring child pornography remains outside the scope of the proposed Act, but, again, this is not a mandatory requirement of the Convention. However, the proposed Act does state that prosecution under it is without prejudice to prosecution under the Anti-Trafficking in Persons Act of 2003 (RA 9208) and the Special Protection of Children Against Abuse, Exploitation and Discrimination Act (RA 7610).

In 2005, the Internet Indecency Act (HB 4386) was introduced into the House of Representatives to prohibit persons from engaging in any form of pornographic exploitation using information technology. It is unclear whether the proposed Act will be re-introduced in the current session of the Philippines Congress. Cybersex – one form of pornographic exploitation mentioned in the proposed Act – was broadly defined to include viewing and/or downloading pornography, reading and writing sexually explicit letters, visiting sexually-oriented chat rooms and engaging in interactive online sexual affairs for a fee. Offenders are liable to imprisonment for five years or a fine not exceeding PhP1,000,000 (approximately USD$22,550) or both. It is a separate offence to solicit persons to engage in pornographic exploitation and the severity of the penalty for this offence depends on whether the victim has reached the age of majority (18) or not. Proposed section 8 obliges "establishments that provide Internet services" to block access to pornographic sites and to prevent minors from engaging in any interactive sexual online affairs and conversation. It specifically prohibits such establishments from having a "private room" where sexual predators can engage in pornographic exploitation.

10. The Philippines

Part 3 – Benchmark Comparison

Key: Favourable alignment | Moderate alignment | Weak alignment

(E) Enacted
(P) Pending
(Title [x]) Title [x] of the Council of Europe Convention on Cybercrime

Area	Legislative regime to be compared with benchmark	Benchmark legislation	Overall alignment	Areas of strong alignment	Areas of moderate alignment	Areas of weak alignment
Computer Security Laws	Electronic Commerce Act (E) Anti-Wire Tapping Act (E) Revised Penal Code (E)	Council of Europe Convention on Cybercrime (Titles 1, 2 and 5)		• Illegal access, data interference and system interference offences	• Illegal interception offence	• No misuse of devices, computer-related forgery and computer-related fraud offences • No attempt, aiding or abetting or corporate liability provisions
	Cybercrime Prevention Act of 2005 (P)	Council of Europe Convention on Cybercrime (Titles 1, 2 and 5)		• Illegal access, data interference, system interference, misuse of devices and computer-related fraud offences • Aiding and abetting provisions	• Attempt and corporate liability provisions • Illegal interception and computer-related forgery offences	
	Anti-Computer Fraud and Abuses Act of 2007 (P)	Council of Europe Convention on Cybercrime (Titles 1, 2 and 5)		• Illegal access and data interference offences	• Illegal interception, system interference, computer-related fraud and forgery offences	• No attempt, aiding or abetting or corporate liability provisions • No misuse of devices offence (although trafficking in passwords prohibited)
Privacy Laws	There is no enacted or pending data protection legislation in the Philippines upon which a benchmarking analysis can be conducted.					
Spam Laws	Implementing rules under the Telecommunications Policy Act (E)	Anti-spam legislation checklist (drafted by Microsoft)			• Requirement for unsubscribe facility • Mandatory identification of the sender	• No coverage of spam email messages • "Opt-in" regime • No private right of action • Sanctions for infringing implementing rules not specified • No consideration of ISP liability for transmission • No labelling requirements
	Cybercrime Prevention Act of 2007 (P)	Anti-spam legislation checklist (drafted by Microsoft)		• "Opt-out" regime • Prohibitions on falsification of transmission information and misleading content • Requirement for unsubscribe facility • No 'ADV' or other labelling requirements		• No private right of action for ISPs/email service providers; criminal sanctions only • No consideration of pre-existing business relationships • No consideration of ISP liability for transmission • No anti-address harvesting measures

Area	Legislative regime to be compared with benchmark	Benchmark legislation	Overall alignment	Areas of strong alignment	Areas of moderate alignment	Areas of weak alignment
Online Child Safety Laws	Revised Penal Code (E) The Special Protection of Children Against Child Abuse, Exploitation and Discrimination Act (E)	Council of Europe Convention on Cybercrime (Title 3 COE)/ICMEC principles			• Criminal sanctions for selling, distributing and exhibiting obscene material	• No legislation specific to child pornography • No definition of child pornography • No specific computer-facilitated child pornography offences • Possession irrespective of intent to distribute is not prohibited • No scope for ISP reporting of dealing in child pornography
	Cybercrime Prevention Act of 2007 (P)	Council of Europe Convention on Cybercrime (Title 3 COE)/ICMEC principles		• Definition of child pornography • Criminal sanctions for possessing, producing, offering for sale, making available or distributing child pornography using a computer		• No scope for ISP reporting of dealing in child pornography

Last Updated: 15 October 2007

11. Singapore

Part 1 – Snapshot of Legislative Status

Key: (E) Enacted
(P) Pending
(Title [x] COE) Title [x] of the Council of Europe Convention on Cybercrime (COE)

Area	Topic	Enacted legislation	Pending legislation	Relevant instruments/Comments
Computer Security Laws	**Core offences (Title 1 COE):** illegal access, illegal interception, data interference, system interference, misuse of devices	✓	✗	Computer Misuse Act (Cap. 50A) (E)
	Computer-related offences (Title 2 COE): computer-related forgery, computer-related fraud	✓	✗	Computer Misuse Act (Cap. 50A) (E)
	Ancillary-liability (Title 5 COE): attempt and aiding/abetting, corporate liability	✓	✗	Computer Misuse Act (Cap. 50A) (E)
Privacy Laws	**Data protection**	✗	✗	No specific data protection legislation, but NIAC's Model Data Protection Code has gained some support.
	Surveillance (see illegal interception under computer security)	✓	✗	Telecommunications Act (Cap. 323) (E); Internal Security Act (Cap. 143) (E); Undesirable Publications Act (Cap. 338) (E); National Registration Act (Cap. 201) (E)
	Sensitive information	✓	✗	Banking Act (Cap. 19) (E); Official Secrets Act (Cap. 213) (E)
Spam Laws	**Anti-spam regulation**	✓	✗	Spam Control Act (E)
Online Child Safety Laws	**General child pornography offences**	✗	✗	No general child pornography legislation, but it is an offence to distribute (and possess with intent to distribute) obscene material (Penal Code (Cap. 224) (E); Undesirable Publications Act (Cap. 338)). It is also an offence to commit or procure an indecent act with a child or young person (Children and Young Persons Act (Cap. 38)). Trafficking and prostitution of women and children is also punishable (Women's Charter (Cap. 353) (E)). Singapore is not considering enacting general child pornography offences, but Singapore is considering the enactment of a sexual grooming offence that applies in respect of minors.
	Computer-facilitated child pornography offences (Title 3 COE)	✗	✗	

Part 2 – Legal and Regulatory Position

2.1 COMPUTER SECURITY LAWS – CURRENT LEGISLATIVE FRAMEWORK

Core offences (Title 1 COE): Illegal access, illegal interception, data interference, system interference, misuse of devices

The Computer Misuse Act (Cap. 50A) includes a basic hacking offence – causing a computer to secure access to a program or data without authority – which is punishable by a fine not exceeding S$5,000 (approximately USD$3,320) or by imprisonment for a term not exceeding two years or by both. If the unauthorised access causes damage, this penalty can be increased to a fine not exceeding S$50,000 (approximately USD$33,160) or to imprisonment for a term not exceeding seven years or to both.

A separate offence exists in relation to securing unauthorised access to a program or data for the purpose of facilitating the commission of further offences involving property, fraud or dishonesty. Offenders who engage in this extended type of hacking may be fined up to S$50,000 (approximately USD$33,160) or face imprisonment for a term not exceeding 10 years or both.

The Computer Misuse Act also creates offences in respect of unauthorised interference with data, illegal interception of a

computer service and system interference. Each of these offences is punishable by a fine not exceeding S$10,000 (approximately USD$6,630) or by imprisonment for a term not exceeding three years or both. Once again, stiffer penalties accrue if damage results from the offending conduct.

The Act's unauthorised disclosure of password offence only partially implements the Convention's misuse of devices offence.

Singapore's Evidence Act (Cap. 97) specifically addresses the admissibility of electronic evidence which assists in the prosecution of cybercrime offences. Computer output is admissible if it is relevant or otherwise admissible under the Evidence Act and it is:

- expressly agreed between the parties to the proceedings that the computer output's authenticity or accuracy is not disputed;
- produced in an approved process; or
- shown by the party tendering the computer output that (i) there is no reason to suspect that the output is inaccurate due to improper use of the computer or any other reason and (ii) there is reasonable ground to believe that the computer was operating properly at all material times, or if not, that the accuracy of the output was not affected by the malfunction.

Computer-related offences (Title 2 COE): Computer-related forgery, computer-related fraud

The Convention's computer-related forgery and fraud offences have no direct counterpart in the Computer Misuse Act. However, the Computer Misuse Act's extended hacking offence – securing unauthorised access to a program or data for the purpose of facilitating the commission of a further offence – is understood to cover largely the same ground when the further offence involves forgery or fraud.

Ancillary liability (Title 5 COE): Attempt and aiding/abetting, corporate liability

Attempting, abetting and otherwise furthering the commission of an offence under the Computer Misuse Act is punishable in exactly the same way as the principal offence. The Act does not appear to address corporate liability expressly.

2.2 COMPUTER SECURITY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

At the date of writing, there are no upcoming legislative developments that relate to computer security.

2.3 PRIVACY LAWS – CURRENT LEGISLATIVE FRAMEWORK

Data protection

Singapore does not have any specific data protection legislation. However, a private-led initiative of the National Internet Advisory Committee (NIAC) has attempted to fill this vacuum to a degree. Its Model Data Protection Code (released in 2002) is a voluntary code for private sector organisations that collect personal data in electronic form. The Code sets forth a set of data protection principles that are loosely based on the OECD's privacy guidelines. Although enforcement of the Code remains unclear, the National Trust Council has adopted the Model Data Protection Code and requires all TrustSg-accredited businesses to adhere to the Code.

Surveillance

In addition to the illegal interception offence in the Computer Misuse Act, the unauthorised interception of telecommunications may amount to a criminal offence under section 46 of the Telecommunications Act (Cap. 323). This section is likely to embrace interception of emails, while section 41 of the same Act is thought to cover wiretapping. Both of these offences under the Telecommunications Act (Cap. 323) are punishable by a fine not exceeding S$10,000 (approximately USD$6,630) or to imprisonment for a term not exceeding 3 years or to both.

Despite these prohibitions on interception, the Internal Security Act (Cap. 143), the Telecommunications Act and the Undesirable Publications Act (Cap. 338) vest officers and other authorised persons with wide powers of search, seizure and interception in the name of national security, public safety and public interest. These powers are typically exercisable without a warrant but defendants have the right to request judicial review of such searches.

Closed circuit television surveillance is also common in Singapore.

Every person lawfully resident within Singapore must register under the National Registration Act (Cap. 201) and is provided with an identity card.

Sensitive information

Like most other South East Asian jurisdictions, Singapore has banking laws that prohibit disclosure of financial information without the consent of the customer. The Official Secrets Act (Cap. 213) and the Public Service Code of Official Conduct protect some government information from unauthorised use and disclosure.

2.4 PRIVACY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

It is understood that privacy regulation was one of the measures called for in the National Trust Framework (NTF) that Singapore's Infocomm Development Authority released in 2006. We understand that the NTF is intended to develop infrastructure, manpower, education and regulation that will enhance Singapore's image as a trusted hub.

11. Singapore

2.5 SPAM LAWS – CURRENT LEGISLATIVE FRAMEWORK

The Spam Control Act came into force in June 2007 and establishes an 'opt-out' regime in respect of bulk unsolicited commercial electronic messages with a Singapore link. Email, SMS and MMS messages fall within the ambit of the regime; messages sent by fax to a fixed telephone number, voice telephone calls and messages sent using instant messaging tools (such as Windows Live Messenger) do not.

The definition of commercial electronic message includes electronic messages that have the primary purpose of (i) offering to supply, advertising or promoting goods or services, or (ii) assisting a person to obtain by dishonesty or deception property or a financial advantage from another person. A commercial electronic message is unsolicited if the recipient did not (i) request to receive the message or (ii) consent to the receipt of the message. The Act only applies to electronic messages that have a Singapore link. A Singapore link can be established if an electronic message originates in Singapore, or if an electronic message originates overseas and is accessed in Singapore.

Electronic messages are deemed to be sent in bulk where the same sender (defined as the person who sends the message, causes it to be sent or authorises its sending) sends:

(a) more than 100 electronic messages containing the same or similar subject-matter during a 24-hour period;

(b) more than 1,000 electronic messages containing the same or similar subject-matter during a 30-day period; or

(c) more than 10,000 electronic messages containing the same or similar subject-matter during a one-year period.

Persons sending unsolicited commercial electronic messages in bulk must comply with the Spam Control Act's transparency requirements. These requirements include that unsolicited commercial electronic messages must (i) contain an unsubscribe facility, (ii) be labelled '<ADV>', (iii) contain a subject title that does not mislead the consumer as to the content of the message, (iv) have header information that is not false or misleading, and (v) contains a phone number or email address by which the sender can be readily contacted.

The Spam Control Act's prohibition on sending electronic messages to an electronic address generated or obtained through the use of a dictionary attack or address harvesting software applies irrespective of whether the message is solicited or of a commercial nature. Thus, indiscriminate spamming by means of a dictionary attack will be caught even if the electronic message so transmitted is of a purely factual nature.

The Spam Control Act contains safe harbour provisions for ISPs and other intermediaries that provide online services, network access services, or services relating to the transmission or routing of data. These intermediaries will not be taken to have contravened the Act merely because they provide facilities by which spam may be transmitted.

The Spam Control Act gives a statutory right of action to ISPs, email providers and individuals that have suffered loss or damage as a direct or an indirect result of a contravention of the proposed legislation. These individuals or entities will be entitled to bring civil proceedings against (i) the person that sent or caused or authorised the sending of the electronic message or (ii) any person who aided, abetted or otherwise assisted with the contravention of the proposed legislation. Courts can grant ordinary damages, statutory damages and injunctions for contraventions of the Act. Litigants must elect between ordinary damages and statutory damages; they cannot recover both. Statutory damages are limited to an amount not exceeding S$25 (approximately USD$17) for each unlawful electronic message up to a maximum of S$1 million (approximately USD$666,600) (unless the litigant proves that their actual loss from the unlawful activity exceeds S$1 million). The Act does not expressly allow for enforcement by a government agency.

2.6 SPAM LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

At the date of writing, there are no upcoming legislative developments that relate to spam.

2.7 ONLINE CHILD SAFETY LAWS – CURRENT LEGISLATIVE FRAMEWORK

General child pornography offences

The age of majority in Singapore is 21 years; the age of consent to sexual relations for females is generally 14 years.

Singapore does not have any specific child pornography legislation. However, there are general obscenity prohibitions in both the Penal Code (Cap. 224) and the Undesirable Publications Act (Cap. 338). Both statutes prohibit the sale, distribution or circulation of obscene and objectionable objects. However, production and possession of obscene or objectionable material only amounts to an offence when the purpose of such production or possession is distribution. The Penal Code's definition of obscene objects is wide as is the Undesirable Publications Act's definition of obscene and objectionable publications. Accordingly, most forms of child pornography, including that which is distributed in digital format, should fall within the ambit of both statutes. Under the Undesirable Publications Act (which provides the highest penalties), offenders are liable to a fine of up to S$10,000 (approximately USD $6,630) or up to two years imprisonment or both. Offenders who distribute obscene objects to persons under the age of 20 face stricter penalties than usual under the Penal Code.

The Children and Young Persons Act (Cap. 38) also makes it an offence for a person to commit, attempt, abet or procure the commission by any person of an obscene or indecent act with any child (a person under the age of 14) or young person (a person between the ages of 14 and 16). If convicted, an offender is liable to imprisonment for a term not exceeding two years or a maximum fine of S$5,000 (approximately USD$3,320) or to both. Repeat offending is punished more severely.

Trafficking and prostitution of women and children is addressed by the Women's Charter (Cap. 353). Maximum penalties for offences contained therein range between three and 10 years imprisonment and fines of S$2,000 (approximately USD$1,330) and S$15,000 (approximately USD$9,950).

Computer-facilitated child pornography offences (Title 3 COE)

Singapore does not have any legislation that creates computer-facilitated child pornography offences.

Miscellaneous

Another method by which Singapore restricts activities related to child pornography is by regulating Internet traffic. Internet service and content providers targeting Singaporean viewers must, under Singapore's Class License system (established pursuant to the Broadcasting Act (Cap. 28), use their best efforts to ensure that they are not offering material that offends good taste or decency.

2.8 Online Child Safety Laws – Upcoming legislative developments

Singapore's Penal Code (Amendment) Bill (38/2007) proposes to enact a new offence in the Penal Code that appears to criminalise both online and offline sexual grooming of minors. The elements of the offence under proposed section 367E are as follows:

- the offender (who must be at least 21 years of age) must have met or communicated with the victim (either within or outside Singapore) on two or more occasions;
- the victim must be under the age of 16 and the offender must not reasonably believe that the victim is 16 years of age or older; and
- the offender must travel to meet, or intentionally meet, the victim in Singapore with the intent to commit a sexual offence involving the minor during or after the meeting.

Offenders will be liable to imprisonment for up to three years and/or a fine, the amount of which is unspecified.

The Penal Code (Amendment) Bill was read for the first time in September 2007. In accordance with usual Singaporean parliamentary procedure, it is expected that the bill will be passed into law without amendment after it has been read three times.

11. Singapore

Part 3 – Benchmark Comparison

Key: Favourable alignment Moderate alignment Weak alignment

(E) Enacted
(P) Pending
(Title [x]) Title [x] of the Council of Europe Convention on Cybercrime

Area	Legislation to be compared with benchmark	Benchmark legislation	Overall alignment	Areas of strong alignment	Areas of moderate alignment	Areas of weak alignment
Computer Security Laws	Computer Misuse Act (Cap. 50A) (E)	Council of Europe Convention on Cybercrime (Titles 1, 2 and 5)		• Data interference, illegal interception and system interference offences • Liability for aiding, abetting and attempting cybercrimes	• Illegal access offence • Computer-related fraud and forgery offences • Unauthorised distribution of password offence (partial implementation of the Convention's misuse of devices offence)	• Corporate liability not addressed
Privacy Laws	There is no comprehensive enacted or pending data protection legislation in Singapore upon which a benchmarking analysis can be conducted.					
Spam Laws	Spam Control Act (E)	Anti-spam legislation checklist (drafted by Microsoft)		• 'Opt-out' regime • Address harvesting measures • Safe harbour provisions for ISPs • Transparency requirements (functional unsubscribe facility, sender identification, prohibitions on false/ misleading header information or subject lines)	• Definition of commercial electronic message	• 'ADV' labelling requirements for commercial electronic messages • Little scope for pre-existing business relationships • "Bulk" requirement • No adjustment of statutory damages regime for wilful conduct and implementation of best practice procedures • Opting-out on a business-unit or product-line basis is not facilitated • Private right of action for all persons affected by spam (and not just ISPs/email service providers)
Online Child Safety Laws	Penal Code (Cap. 224) (E) Children and Young Persons Act (Cap. 38) (E) Women's Charter (Cap. 353) (E)	Council of Europe Convention on Cybercrime (Title 3)/ICMEC principles			• Criminal sanctions for distributing, transmitting, making available and possessing with intent to distribute obscene/ objectionable material	• No legislation specific to child pornography • No definition of child pornography • No specific computer-facilitated child pornography offences • Possession irrespective of intent to distribute is not prohibited • No scope for ISP reporting of dealing in child pornography

12. South Korea

Part 1 – Snapshot of Legislative Status

Key: (E) Enacted
(P) Pending
(Title [x] COE) Title [x] of the Council of Europe Convention on Cybercrime (COE)

Area	Topic	Enacted legislation	Pending legislation	Relevant instruments/Comments
Computer Security Laws	**Core offences (Title 1 COE):** illegal access, illegal interception, data interference, system interference, misuse of devices	✓	✗	Act on Promotion of Information and Communication Network Use and Information Protection (E)
	Computer-related offences (Title 2 COE): computer-related forgery, computer-related fraud	✓	✗	Criminal Code (E); Act on Promotion of Information and Communication Network Use and Information Protection (E)
	Ancillary liability (Title 5 COE): attempt; aiding/abetting, corporate liability	✓	✗	Act on Promotion of Information and Communication Network Use and Information Protection (E); Criminal Code (E)
	Miscellaneous	✓	✗	The Act on Information Communication Infrastructure Protection (E) establishes a general framework for critical infrastructure protection.
Privacy Laws	**Data protection**	✓	✓	No data protection legislation of general application, but see sectoral regulation: Act on Promotion of Information and Communication Network Use and Information Protection (E); and Act on the Protection of Personal Information Maintained by Public Agencies (E) Basic Act on the Protection of Personal Information (P); Act on the Protection of Personal Information Maintained in the Private Sector (P); Amendment to the Act on the Protection of Personal Information Maintained by Public Agencies (P); Grand National Party Bill (P); Terrorism Prevention Bill (P)
	Surveillance (see illegal interception under computer security)	✓	✗	Protection of Communications Secrets Act (E); National Security Law (E); Social Surveillance Law (E)
	Sensitive information	✓	✗	Various legislation including Act on the Use and Protection of Credit Information (E), Telecommunications Business Act (E), Medical Service Act (E), Real Name Financial Trade and Secrecy Act (E) and Digital Signatures Act (E).
	Miscellaneous	✗	✓	Act on Real Name Use on the Internet (P); Amendment to the Act on Promotion of Information and Communication Network Use and Information Protection (P)
Spam Laws	**Anti-spam regulation**	✓	✗	Act on Promotion of Information and Communication Network Use and Information Protection (E)
Online Child Safety Laws	**General child pornography offences**	✓	✗	Juvenile Sex Protection Act (E); Juvenile Protection Act (E); Criminal Code (E)
	Computer-facilitated child pornography offences (Title 3 COE)	✗	✗	No computer-facilitated child pornography offences, but see the Ministry of Information and Communication's obligations in the Act on Promotion of Information and Communication Network Use and Information Protection (E).

12. South Korea

Part 2 – Legal and Regulatory Position

2.1 COMPUTER SECURITY LAWS – CURRENT LEGISLATIVE FRAMEWORK

Core offences (Title 1 COE): Illegal access, illegal interception, data interference, system interference, misuse of devices

The Act on Promotion of Information and Communication Network Use and Information Protection (Information and Communication Network Act) establishes the framework for computer security regulation in South Korea. The Act creates offences in respect of illegal access, data interference and system interference. Each of these offences is punishable by a maximum term of imprisonment of between three and five years, and a maximum fine of between KRW30 million (approximately USD$32,490) and KRW50 million (approximately USD$54,110). The Information and Communication Network Act does not appear to criminalise the illegal interception of non-public transmissions of data or the misuse of devices in the commission of cybersecurity offences.

Unlike the Convention on Cybercrime, the formulation of the illegal access and data interference offences in the Information and Communication Network Act requires that the offences be committed in respect of an information and communications network; protection is not afforded to standalone computers (although network connectivity is likely to be a reality where the internet is involved). In addition, the South Korean Act tends to focus on specific applications of the Convention's broadly-drafted offences. For example, one permutation of the system interference offence is predicated on the offender sending "a large volume of signals or data for the purpose of hindering the stable operation of [an] information and communications network". Similarly, the transmission and distribution of malicious programs, as a means of causing data interference, is hardwired into the legislation. This focus on current techniques for the commission of cybercrimes may compromise the ability of the Information and Communication Network Act to regulate new cybercrime techniques as they evolve.

Computer-related offences (Title 2 COE): Computer-related forgery, computer-related fraud

The Convention's computer-related forgery and fraud offences have no direct counterpart in the Information and Communication Network Act. However, the malicious program offence mentioned above does envisage the situation where a malicious program operates to forge data.

The Criminal Code contains a computer-related fraud offence that is punishable by imprisonment for up to 10 years or a fine of up to KRW20 million (approximately USD$21,640). The Criminal Code also contains an offence that may have some application to computer-related forgery: article 314(2) of the Code criminalises damage to computers or electromagnetic records by inputting false information, improper order or otherwise causing an impediment to data processing. This Criminal Code offence is punishable by imprisonment for up to five years or by a fine not exceeding KRW15 million (approximately USD$16,230).

Ancillary liability (Title 5 COE): Attempt and aiding/abetting, corporate liability

Although the Information and Communication Network Act does not explicitly address ancillary liability for attempting, aiding or abetting the commission of an offence, it is understood that the equivalent provisions in the Korean Criminal Code will apply. As for corporate liability for cybercrimes, the Information and Communication Network Act provides that if a representative, agent or employee of a corporation commits an offence punishable by a penal sanction, then the corporation will be liable for the applicable fine in addition to the punishment that the principal offender receives.

Miscellaneous

The Act on Information Communication Infrastructure Protection has been in force since July, 2001, and provides a general policy framework for critical infrastructure protection. It established a cross-agency Committee on Critical Information Infrastructure, and sets out (i) the criteria for the designation of critical infrastructures and (ii) security guidelines to be followed.

2.2 COMPUTER SECURITY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

At the date of writing, there are no upcoming legislative developments that relate to computer security laws.

2.3 PRIVACY LAWS – CURRENT LEGISLATIVE FRAMEWORK

Data protection

There is no data protection legislation of general application in South Korea. However, certain sectors of the economy are regulated in their dealings with personal information.

Telecommunications service providers, ISPs, content providers and other offline information intermediaries (including travel agencies and educational institutes) are obliged to comply with the data protection provisions of the Information and Communication Network Act. Based on the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, this Act requires data users to obtain consent from data subjects to the collection, use and disclosure of personal information, except in certain circumstances. These circumstances include where the information provided has been de-identified, or where collection, use or disclosure is necessary to give effect to a contract. Data users should collect as little personal data as is necessary and are obliged to notify the data subject of certain matters prior to collection, including the type of personal information that will be collected, the duration of storage and use of the collected personal information

and the identity of any third parties that the personal information will be provided to. The Act allows the data subject to withdraw consent for the collection, use and disclosure of personal information at any time; such requests must be complied with by the data user unless it is obliged to preserve the personal information under another statute. Further, every data subject has a right to access and correct his or her personal information. There are also special provisions that relate to how data users can obtain and deal with the personal information of children under the age of 14, and the Act's transborder data protection provisions require (i) the data user to enter into an international contract with the foreign transferee that is consistent with the Act and (ii) the data subject's consent be obtained prior to transmission of their personal information abroad.

The Act on the Protection of Personal Information Maintained by Public Agencies applies to the automated (and not manual) processing of personal data in the public sector. It obliges public agencies to maintain records of personal information databases they administer and to report these databases to the Ministry of Government Administration and Home Affairs. In turn, the Ministry is typically obliged to notify the public of the existence of these databases. The Ministry can request information about the data user's practices and is empowered to issue opinions on the adequacy of these. Data subjects have a right of access to, and correction of, personal information held by a public agency.

Surveillance

The Protection of Communications Secrets Act prohibits certain forms of surveillance – censoring mail, wiretapping telecommunications, and recording or listening in on private conversations – except in cases of national security or where a criminal investigation is being undertaken. Government officials who rely on their powers under the Act must obtain judicial approval before placing wiretaps, or in the event of an emergency, soon after placing them. There have been several inquiries into illegal wiretapping during the late 1990s all of which have condemned the frequency with which this activity occurs in South Korea.

The National Security Law and the Social Surveillance Law also contain provisions that relate to surveillance.

Sensitive information

South Korea has a range of legislation that protects sensitive information including the Act on the Use and Protection of Credit Information, the Telecommunications Business Act, the Medical Service Act, the Real Name Financial Trade and Secrecy Act, and the Digital Signatures Act.

Miscellaneous

South Koreans enjoy rights to the protection of secrecy and the liberty of private life under the Constitution of the Republic of Korea.

2.4 PRIVACY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

Data protection

There are several pending data protection bills in South Korea:

- **Act on the Protection of Personal Information.** The bill contemplates the establishment of a data protection regime that applies to both the private and public sectors with some exceptions (for example, use of private information by the press, religious institutions and political parties). The bill contains general provisions that apply to both sectors, as well as sector-specific provisions. By and large, the bill is more prescriptive than the APEC Privacy Framework and often sets a higher standard than that contemplated by the APEC principles. For example, regulated entities must obtain a data subject's consent to the collection of their private information unless collection is permitted by law. Further, a regulated entity may only use or disclose collected private information for purposes that are notified to the public, with the data subject's consent or as permitted by law. On the enforcement front, contraventions of the bill can attract criminal sanctions and the Private Information Committee – an independent committee established by the Prime Minister – can issue regulated entities with corrective orders requiring recipients to take certain steps in circumstances where the Committee has reasonable cause to believe that private information has been infringed. The bill does appear to contemplate a co-regulatory model, but the interaction between industry codes and the bill is not clear from the bill itself.
- **Act on the Protection of Personal Information Maintained in the Private Sector.** This bill proposes to separate the data protection provisions found in the existing Information and Communication Network Act and expand on them. Its provisions would apply to all those who (i) collect personal information for commercial reasons and (ii) process and use personal information using telecommunications networks, computers and data processors. The bill envisages the creation of a Personal Information Protection Commission and the introduction of a personal information impact evaluation system. The Ministry of Information and Communication is currently reviewing this bill.
- **Amendment to the Act on the Protection of Personal Information Maintained by Public Agencies.** This bill proposes to enhance the current public sector legislation (see further section 2.3 previous). In particular, the Amendment would require the head of the collecting agency to post a notice regarding the collection of data on the relevant agency's website. It is expected that restrictions would also be imposed on the sharing of personal information among different public sector agencies. Maintenance of personal information files on individuals would be conditional upon the Minister of Government Administration and Home Affairs' prior approval of such conduct

(at a global level) and there would be an obligation to destroy these personal information files when they are no longer necessary. This bill was submitted to the National Assembly in June 2004, and has since been presented to a Standing Committee of the National Assembly.

The Hannara Party (the Grand National Party) has proposed another data protection bill that applies to both the private and public sectors. In some respects, this bill appears to be less onerous for regulated entities than other proposed data protection bills. For example, the Grand National Party Bill permits businesses to undertake cost/benefit analyses in determining whether to provide notice to data subjects prior to the collection of personal information, and class actions against regulated entities are not permissible. However, the Grand National Party Bill does require regulated entities to register their privacy policy with a privacy committee who may direct the regulated entity to adopt a standard position in certain areas where the risk of infringement is high.

In May 2006, there were proposals by the Government Administration and Local Autonomy Committee of the National Assembly to combine the following three bills into a single piece of legislation:

- the Basic Act on the Protection of Personal Information;
- the Act on the Protection of Personal Information Maintained in the Private Sector; and
- the privacy bill proposed by the Hannara Party.

Miscellaneous

A revised version of the Terrorism Prevention Bill was introduced into the National Assembly in November 2003. This bill proposes to expand the National Intelligence Service's (NIS) power to enact anti-terrorism measures and provides for the establishment of a Counter-Terrorism Center under the command of the NIS. Some of the bill's provisions are under scrutiny from the human rights community.

In August 2006, two bills with a privacy dimension were under consideration. The first was the Act on Real Name Use on the Internet, which reportedly requires all persons to use their real names when posting comments online using portals or news media websites. It is understood that the purpose of the bill was to reduce the incidence of defamatory postings on the internet.

The second, related legislative proposal was an amendment to the Information and Communication Network Act to allow service providers to take temporary action to protect the interests of persons who are the subject of defamatory postings or disclosure of private facts.

2.5 SPAM LAWS – CURRENT LEGISLATIVE FRAMEWORK

The anti-spam regime established by the Information and Communication Network Act differs according to the medium by which the advertising information is transmitted – emails and other forms of media prescribed by Presidential Decree are regulated on an 'opt-out' basis, while telephone and fax messages are regulated on an 'opt-in' basis. In terms of transparency requirements, article 50(4) of the Information and Communication Network Act requires that a person who transmits advertising information by email (or other media prescribed by Presidential Decree) and for the purposes of profit must explicitly indicate the:

- type of the information transmitted (by labelling the spam message with [ADV] or [ADLT] (as appropriate) and including an "@" symbol at the end of the subject field);
- content of the message (in the subject line);
- sender's name and contact information (in the body of the email); and
- methods by which receivers may easily 'opt-out' of receiving spam emails.

Only the latter two pieces of information need to be included in advertising information that is transmitted by telephone or fax. In addition, special consent must be obtained to transmit advertising information by phone or fax between the hours of 9pm and 8am.

It is an infringement of the Act to send advertising information that does not comply with the above transparency requirements. It is a separate infringement of the Act to send advertising information where an addressee has explicitly rejected (i.e. opted-out of receiving) such communications. Both these infringements are punishable by an administrative fine of up to KRW30 million (approximately USD$32,490) imposed by the Ministry of Information and Communication.

Failure to obtain prior consent from recipients of advertising information transmitted by telephone or fax also attracts an administrative fine of up to KRW30 million (approximately USD$32,490). Note that there is no need to obtain prior consent where (i) the recipient's contact information is collected directly from the recipient in connection with a transaction for goods and services, and the advertising information relates to those goods and services, or (ii) the advertisement is of the kind provided for in article 13(1) of the Act on the Consumer Protection in the Electronic Commerce Transactions or article 6(3) of the Door to Door Sales Act.

The Information and Communication Network Act also prohibits the use of technical measures that (i) interfere with a recipient's refusal to receive unsolicited messages, (ii) automatically identify a recipient's contact information or (iii) automatically register email addresses to enable for-profit transmission of advertising information. Harvesting

email addresses from internet webpages without the prior consent of the operator of the homepage and the sale of lists compiled by this means is also prohibited. Each of these activities is a criminal offence and attracts liability of up to KRW10 million (approximately USD$10,830).

Further, the provisions of the Act entitle ISPs and webmail service providers to deny service to spammers in the following circumstances:

- Where transmission or receipt of advertising information causes or is feared to cause an impediment to the provision of services; or
- Where spam recipients do not want to receive advertising information.

This entitlement to deny service is conditioned upon the ISP or web-mail service provider (i) outlining its denial of service policy in its contract with the spammer and (ii) notifying the spammer and other interested persons of its intention to cease providing service.

Korean law enforcement agencies have been known to enforce the spam-related provisions of the Information and Communication Network Act where there has been a suspected breach.

2.6 SPAM LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

There is some suggestion that KISA is considering revising its anti-spam regime to be 'opt-in' instead of 'opt-out'. At the date of writing, the details of this proposal are not known.

2.7 ONLINE CHILD SAFETY LAWS – CURRENT LEGISLATIVE FRAMEWORK

General child pornography offences

The age of majority in South Korea is 20 years; the age of consent to sexual relations is 13 years (although pursuant to the Juvenile Sex Protection Act, it is a crime to pay for sexual relations with a person under the age of 19).

The Juvenile Sex Protection Act defines child pornography as obscene material that depicts a juvenile (a person under the age of 19) performing a range of specified sexual acts. This definition is understood to cover altered child pornography material only where an actual minor (as opposed to a depiction thereof) is used as a basis for the altered material. Although animated child pornography is considered to be outside the scope of the Juvenile Sex Protection Act, this form of child pornography is likely to fall under the general ban on obscene material in the Criminal Code.

Under the Juvenile Sex Protection Act, for-profit possession and distribution of child pornography material is punishable by imprisonment for up to seven years; mere possession of child pornography material is not prohibited. Furthermore, producing, importing or exporting child pornography material is punishable by a minimum term of imprisonment of five years, and introducing juvenile to someone who produces child pornography material is punishable by imprisonment for a term of between one and 10 years.

In addition to regulating animated child pornography, the Criminal Code's general ban on obscene material is relevant to the extent that distribution of child pornography material (other than importing or exporting) is not-for-profit. Under the Code, such distribution is punishable by imprisonment for up to one year or by a fine of up to KRW5 million (approximately USD$5,410).

It is a separate offence under the Juvenile Sex Protection Act to induce someone to purchase sex with a juvenile or to solicit a minor to have sex for money as part of a "business". Conversely, personal, not-for-profit solicitation of juveniles for sex is not a crime.

The Juvenile Sex Protection Act obliges computer-aided communication service providers to implement functionality that restricts juveniles from gaining access to harmful advertisements by way of their communication services (Article 20(1)3).

Computer-facilitated child pornography offences (Title 3 COE)

South Korea does not have any legislation that creates computer-facilitated child pornography offences. However, pursuant to the Information and Communication Network Act, the Ministry of Information and Communication is obliged to take measures to protect juveniles from "harmful information, including lascivious and violent information" that is distributed via an information and communications network. These measures involve:

- The development and dissemination of content screening software and other technologies to protect juveniles;
- Education and publicity for the protection of juveniles; and
- Other matters prescribed by Presidential Decree for the protection of juveniles.

Further, persons who make available, by means of a telecommunications service, media materials that are deemed to be harmful to juveniles under the Juvenile Protection Act must label them as such. It is also prohibited to use an information and communications network to transmit advertising information without taking measures to restrict access to juveniles where the material so transmitted is considered to be harmful to juveniles. Finally, some providers of information and communications services are obliged to appoint an authority to protect juveniles from harmful information.

2.8 ONLINE CHILD SAFETY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

At the date of writing, there are no upcoming legislative developments that relate to online child safety.

12. South Korea

Part 3 – Benchmark Comparison

Key: Favourable alignment | Moderate alignment | Weak alignment

(E) Enacted
(P) Pending
(Title [x]) Title [x] of the Council of Europe Convention on Cybercrime

Area	Legislative regime to be compared with benchmark	Benchmark legislation	Overall alignment	Areas of strong alignment	Areas of moderate alignment	Areas of weak alignment
Computer Security Laws	Act on Promotion of Information and Telecommunication Network Use and Information Protection (E) Criminal Code (E) Protection of Communications Secrets Act (E)	Council of Europe Convention on Cybercrime (Titles 1, 2 and 5)		• Illegal access offence • Corporate liability provision	• Data interference and system interference offences • Ancillary liability for attempt, aiding or abetting under the Criminal Code • Computer-related fraud and forgery offences	• No misuse of devices offence
Privacy Laws	Act on Promotion of Information and Telecommunication Network Use and Information Protection (E)	Model Privacy Bill (drafted by Microsoft)		• Protective measures to secure personal information from loss or theft • Liability of data user where third party deals with personal information on its behalf • Data subject's right to access and correct personal information • Use and disclosure in accordance with notified purposes does not require consent	• Definition of personal information • Matters that must be contained in the privacy notice provided prior to collection • Finality principle (use of personal information only as notified to user or with user's consent) • Limitations on third party use of personal information	• Not applicable to public sector entities • Collection of personal information must be with consent • No distinction between primary and secondary purposes of use or disclosure • Mode of enforcement (mediation, prosecution or enforcement by the MIC cf. enforcement by Commissioner) • Consequence of infringement (civil liability, criminal offence or administrative fine cf. statutory and civil liability) • Data subject's consent required for transborder data flows within the corporate group • No linkage between withdrawal of consent and cancellation of service • No breach notification provisions

Area	Legislative regime to be compared with benchmark	Benchmark legislation	Overall alignment	Areas of strong alignment	Areas of moderate alignment	Areas of weak alignment
Privacy Laws (continued)	Act on the Protection of Personal Information Maintained by Public Agencies (E)	Model Privacy Bill (drafted by Microsoft)		• Protective measures to secure personal information from loss, theft • Data subject's right to access and correct personal information	• Definition of personal information • Limitations on third party use of personal information	• Not applicable to private sector entities • Restrictions on the type of personal information that can be collected • No distinction between primary and secondary purposes of use • Collection of personal information requires advance notification to the applicable Ministry and public notification thereof • Mode of enforcement (prosecution or administrative appeal cf. enforcement by Commissioner) • Consequence of infringement (criminal offence or administrative fine cf. statutory and civil liability) • No breach notification provisions
Spam Laws	Act on Promotion of Information and Telecommunication Network Use and Information Protection (E)	US State Spam Bill (drafted by Microsoft)		• 'Opt-out' regime for most forms of unsolicited communications including emails • Transparency requirements (sender identification, functional unsubscribe facility) • No private right of action for individuals	• Address harvesting measures	• 'Opt-in' regime for unsolicited communications to telephones and facsimiles • Not-for-profit spamming not regulated • No recognition of pre-existing business relationships • Labelling requirements for commercial emails • Limited criminal sanctions; mostly administrative fines only • No consideration of ISP liability for transmission • No private right of action for ISPs/email service providers
Online Child Safety Laws	Juvenile Sex Protection Act (E) Criminal Code (E)	Council of Europe Convention on Cybercrime (Title 3 COE)/ICMEC principles		• General child pornography offences	• Definition of child pornography	• No specific computer-facilitated child pornography offences • Mere possession of child pornography is not prohibited • No scope for ISP reporting of dealing in child pornography • Distinction between for-profit and not-for-profit dealing in child pornography

13. Taiwan

Part 1 – Snapshot of Legislative Status

Key: (E) Enacted
(P) Pending
(Title [x] COE) Title [x] of the Council of Europe Convention on Cybercrime (COE)

Area	Topic	Enacted legislation	Pending legislation	Relevant instruments/Comments
Computer Security Laws	**Core offences (Title 1 COE):** illegal access, illegal interception, data interference, system interference, misuse of devices	✓	✗	Criminal Code (E); Telecommunications Act (E); Communications Protection and Monitoring Act (E)
	Computer-related offences (Title 2 COE): computer-related forgery, computer-related fraud	✓	✗	Criminal Code (E)
	Ancillary liability (Title 5 COE): attempt; aiding/abetting, corporate liability	Partial	✗	Criminal Code (E)
Privacy Laws	**Data protection**	✓	✓	Computer-Processed Personal Data Protection Law (E) The Legislative Yuan is currently considering an amendment to the Computer-Processed Personal Data Protection Law.
	Surveillance (see illegal interception under computer security)	✓	✗	Criminal Code (E), Telecommunications Act (E); Communications Protection and Monitoring Act (E)
	Sensitive information	✓	✓	Criminal Code (E); Computer-Processed Personal Data Protection Law (E) The Legislative Yuan is currently considering an amendment to the Computer-Processed Personal Data Protection Law that makes provision for sensitive personal data.
Spam Laws	**Anti-spam regulation**	✗	✓	Draft Commercial Spam Statute (P)
Online Child Safety Laws	**General child pornography offences**	✓	✗	Criminal Code (E); The Law to Suppress Sexual Transactions involving Children and Juveniles (E)
	Computer-facilitated child pornography offences (Title 3 COE)	✓	✗	Criminal Code (E); The Law to Suppress Sexual Transactions involving Children and Juveniles (E)
	Miscellaneous	✓	✗	Internet content rating regulations (E); Cybercafe regulations (E)

Part 2 – Legal and Regulatory Position

2.1 COMPUTER SECURITY LAWS – CURRENT LEGISLATIVE FRAMEWORK

Core offences (Title 1 COE): Illegal access, illegal interception, data interference, system interference, misuse of devices

In 2003, Taiwan enacted a new chapter of the Criminal Code to address computer crimes. Article 358 of the Code contains a broad illegal access offence that is punishable by imprisonment for up to three years, detention and/or a fine of up to TWD$300,000 (approximately USD$9,000). The Code's data interference offence is similarly broad: it is a crime to unlawfully possess, delete or alter the electromagnetic records on another's computer or related equipment if this interference results in injury to others. Offenders are liable to imprisonment for up to five years, detention and/or a fine of up to TWD$600,000 (approximately USD$18,100).

As for system interference, the Criminal Code punishes those who use computer programs or other electromagnetic techniques to obstruct the functioning of a person's computer or related equipment if this interference results in injury. This offence is punishable by imprisonment for up to three years, detention and/or a fine of up to TWD$300,000 (approximately USD$9,000).

Prohibitions on illegal interception can be found in a number of statutes. Article 315 bis of the Criminal Code makes it an

offence to unlawfully use electromagnetic records to record the private activities of another person. Offenders are liable to imprisonment for up to three years, detention or a fine of up to TWD$90,000 (approximately USD$2,720). It is also an offence under the Telecommunications Law to receive, record or use telecommunications messages without authorisation; this offence is punishable by imprisonment for up to five years and a fine of up to TWD$1.5 million (approximately USD$45,200). Finally, the Communications Protection and Monitoring Act criminalises the monitoring of communications unless (i) the person conducting the monitoring is a party to the communication, (ii) the parties to the communication have consented to the monitoring and such monitoring is not conducted for an illegal purpose, or (iii) the monitoring is conducted in accordance with laws that permit monitoring (for example, in the law enforcement context), and it has been approved by the relevant authorities. Those who monitor communications in contravention of the Communications Protection and Monitoring Act face imprisonment for up to five years; higher penalties follow if a violation is committed with intent to profit.

The Criminal Code also contains a limited misuse of devices offence insofar as it criminalises the production of viruses for the purpose of committing the Code's computer-related offences. This misuse of devices offence is punishable by imprisonment for up to five years, detention and/or a fine of up to TWD$600,000 (approximately USD$18,100).

Computer-related offences (Title 2 COE): Computer-related forgery, computer-related fraud

Article 339 quarter of the Criminal Code establishes a computer-facilitated fraud offence that is broadly equivalent to that found in the Convention on Cybercrime. Offenders are liable to imprisonment for up to seven years.

Although the Criminal Code does not contain a specific computer-related forgery offence, "electromagnetic records" are deemed as "quasi documents" under Article 220 of the Criminal Code, and the forgery offences for tangible documents set forth in Chapter 15 of the Criminal Code will also apply to quasi documents. This offence is punishable by imprisonment for up to five years for forgery of private documents, and up to seven years for forgery of official documents.

Ancillary liability (Title 5 COE): Attempt and aiding/abetting, corporate liability

Articles 29 and 30 of the Criminal Code establish ancillary liability for abetting and aiding the commission of all criminal offences. No criminal liability will apply to an attempt to commit an offence unless Taiwan's laws expressly provide otherwise. It is also a general principle that criminal liability applies only to the commission of crimes by individuals and does not extend to the commission of crimes by legal persons, such as corporations, except where the law expressly provides otherwise, for example, corporations can face criminal liability for copyright infringement under Taiwan's Copyright Law. There is neither ancillary liability for attempting to commit the computer crimes discussed above nor corporate liability for committing the same.

2.2 COMPUTER SECURITY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

At the date of writing, there are no upcoming developments that relate to computer security laws.

2.3 PRIVACY LAWS – CURRENT LEGISLATIVE FRAMEWORK

Data protection

Taiwan's Computer-Processed Personal Data Protection Law applies to local and central government agencies, and to a limited range of private sector industries including credit investigators, telecommunications providers, financial services institutions and those whose business it is to collect and process personal data. Furthermore, as its name suggests, the Computer-Processed Personal Data Protection Law only applies to personally identifiable information that is processed by computers.

Under the Law, regulated businesses may only collect and process personal data for a specific purpose, and if the regulated business has obtained the written consent of the data subject, entered into a contractual or similar relationship with the data subject, or another of the circumstances specified in Article 18 of the Law applies. A regulated business' use of personal data is generally restricted to the purpose for which it was collected unless the data subject has consented to the proposed use. Data subjects are entitled to access and correct their personal data, and in certain circumstances, may even request that their personal data is deleted, or no longer used or processed. Further, in order to be entitled to collect, use or disclose personal data using a computer, regulated businesses must hold a licence issued by the government authority in charge of their industry sector.

The Law contemplates restrictions on transborder flows of personal data where the destination jurisdiction does not have adequate data protection laws.

Contraventions of the Computer-Processed Personal Data Protection Law can lead to criminal, administrative and civil liability. Criminal liability can involve imprisonment for up to two years and/or a fine of up to TWD$40,000 (approximately USD$1,210), while administrative fines of up to TWD$100,000 (approximately USD$3,020) can be imposed by the government authority in charge of the particular industry sector. Regulated businesses can also face civil liability in damages at the suit of a data subject unless the business can show that any damage caused was not as a result of its willful conduct or negligence.

13. Taiwan

Surveillance

See further the discussion of Taiwan's interception laws in section 2.1 earlier.

Sensitive information

There is no special definition or treatment of sensitive information under current laws. However, sensitive information may fall within the definition of "personal data" and be protected by the Computer-Processed Personal Data Protection Law if it is personal data to be collected or processed by a computer. In addition, sensitive information may also be protected by Criminal Code if it qualifies as a secret.

Customers' banking records are classified as personal data by the Computer-Processed Personal Data Protection Law, and can be protected by the same law as long as it is collected or processed by a computer. Please refer to the previous section on data protection laws for the consequences of contravention of the Computer-Processed Personal Data Protection Law. Customers' banking records can be deemed to be a secret and thereby protected by the Criminal Code. A bank has an obligation to keep such banking records confidential, and those who violate this obligation will be subject to imprisonment for up to one year, detention or a fine of up to TWD$3,000 (approximately USD$90).

Miscellaneous

Pursuant to Taiwan's Household Registration Law, Taiwanese citizens over the age of 14 must hold a citizen's identification card. To obtain this card, citizens must provide their information about the household in which they reside and other personal information. Previously, citizens were required to provide their fingerprints to obtain a citizen identification card, but on 28 September 2005, the Grand Justice declared this requirement to be a violation of Taiwan's Constitutional Law and it is now invalid.

2.4 PRIVACY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

Data protection

In 2005, amendments to the Computer-Processed Personal Data Protection Law were passed by the Executive Yuan. Since then, those amendments have been awaiting passage by the Legislative Yuan, and it is thought that the bill is unlikely to have its second reading in the Legislative Yuan before June 2008.

The proposed amendments extend the application of the Personal Data Protection Law to all industries and to all forms of personal data – the requirement for personal data to be collected or processed by a computer will no longer exist. The draft of the amending legislation also affords additional protection to sensitive personal data such as medical records, generic data, sexual life, health check records, and criminal records.

2.5 SPAM LAWS – CURRENT LEGISLATIVE FRAMEWORK

There is no specific anti-spam legislation in Taiwan. However, some spamming techniques might constitute the offence of system interference discussed in section 2.1 previously. This Criminal Code offence is punishable by imprisonment for up to three years, detention and/or a fine of up to TWD$300,000 (approximately USD$9,070).

2.6 SPAM LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

In January 2005, the Executive Yuan adopted the Draft Commercial Spam Statute which proposed an 'opt-out' regime in respect of commercial electronic mail. The details of this regime are set out below. As at September 2007, this bill appears to be awaiting passage by the Legislative Yuan.

The definition of commercial electronic mail includes emails that have as their primary purpose the marketing of products or commercial services, but excludes emails that provide "relevant information" in the context of an existing transactional relationship. A transactional email contains "relevant information" in the following circumstances:

- where the email is necessary for entering into a contract that has been mutually agreed to by the sender and the recipient;
- where the email contains product or service warranty, recall or safety information;
- where the email contains vital transaction information for the recipient such as transaction deadlines, changes of rights and obligations, or the status of ongoing contractual relationships; or
- where the email contains goods or services, or updates thereto, pursuant to the terms of the transaction that have been mutually agreed by the sender and the recipient.

The general position under the proposed legislation is that all commercial electronic mails must contain an unsubscribe facility and be labelled "commercial", "advertisement", "ADV" or with any other designation that has been approved by the National Communications Commission. Note, however, that solicited commercial electronic mails do not need to be labelled.

It is an infringement of the Draft Commercial Spam Statute to transmit a commercial email that the sender knows or should have known that the recipient has opted-out of receiving. It is also an infringement to transmit commercial emails which the sender knows or should have known to contain false or misleading representations in the subject line or header information.

Enforcement of the proposed legislation is at the suit of those affected by the infringing conduct. These individuals or organisations can receive statutory damages of between TWD$500 and TWD$2,000 (approximately USD$15 to USD$60) per infringing commercial email up to a maximum of TWD$20

million (approximately USD$604,760). However, the statutory caps on the amount of damages recoverable will not apply if (i) the damage incurred by the recipient exceeds the per email cap or (ii) the sender's profit from sending the infringing emails exceeds the overall cap of TWD$20 million (approximately USD$604,760). The proposed legislation does not accommodate reductions in statutory damages where the sender has acted in accordance with industry best practice. Advertising agencies involved in the transmission of infringing commercial emails may be jointly liable with the sender of the message; recipients must bring their action under the proposed legislation within two years of their becoming aware of (i) the damage caused by the infringing spam activity and (ii) the identity of the responsible party. The Draft Statute also contains provision for class actions led by foundations or public-interest associations.

The competent authority – the National Communications Commission – is not responsible for enforcing the proposed legislation; its role is to urge email service providers to take measures to prevent commercial spamming and to engage in international cooperation to reduce spam volumes.

2.7 ONLINE CHILD SAFETY LAWS – CURRENT LEGISLATIVE FRAMEWORK

General child pornography offences

The age of majority in Taiwan is 20 years. The age of consent to sexual relations is 16 years unless there is a sexual transaction, in which case the age of consent is 18 years.

The Law to Suppress Sexual Transactions involving Children and Juveniles criminalizes the production, distribution and sale of paintings, video tapes, films, CDs or other products that show indecency or sexual interaction involving a person under the age of 18. Penalties associated with the production of child pornography range from imprisonment for six months and a fine of up to TWD$500,000 (approximately USD$15,100), to imprisonment for a minimum of seven years and a fine of TWD$10 million (approximately USD$301,550) depending on which section the offender is charged under.

The distribution and sale of child pornography does not attract penalties of the same magnitude as the production offences discussed above: offenders are liable to imprisonment for a maximum term of three years and a fine of not more than TWD$5 million (approximately USD$150,770).

Computer-facilitated child pornography offences (Title 3 COE)

The Law to Suppress Sexual Transactions involving Children and Juveniles was amended in 2005 to criminalize the production, distribution and sale of "electronic signals" that show indecency or sexual interaction involving a person under the age of 18.

This amendment means that criminal liability will attach to the distribution and sale of child pornography over the internet. The penalties associated with the production, distribution, and sale of child pornography over the internet are the same as those for paintings, video tapes, films and CDs discussed earlier.

Miscellaneous

Internet content rating regulations

In April 2004, the government promulgated internet content rating regulations under the Children and Youth Welfare Act, which came into force on 25 October 2005. The regulations were further amended in October 2005. Under this rating system, content hosts are required to classify and label internet content hosted in Taiwan based on a two-level classification system:

- **Restricted:** content that can only be accessed by persons 18 years or older.
- **Unrestricted:** content that may be accessed by children, but may require supervision by a parent, guardian or other persons taking care of children depending on the content.

In addition, the regulations require ISPs to restrict access to content that is not appropriately labelled or to remove the offending content. If the platform provider does not restrict access or cannot effectively restrict access to restricted content by children, it must provide supplemental measures for rating assistance, but the nature of these measures is not specified in the regulations.

Cybercafe regulations

The Taiwanese government has also introduced internet café regulations that prevent cybercafes from being established within a certain distance (set by the relevant local government authority) of schools and oblige operators to restrict the hours during which children under the age of 15 can enter their premises. The regulations do not oblige internet café operators to directly monitor the internet use of their patrons, but it is understood that most operators have agreed to prevent their patrons accessing "questionable" material.

2.8 ONLINE CHILD SAFETY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

Miscellaneous

Computer software rating regulations

In 2005, it was understood that the Taiwanese government was contemplating new content rating regulations that would apply to computer software. At that time, the draft regulations did not apply to online games.

13. Taiwan

Part 3 – Benchmark Comparison

Key: Favourable alignment | Moderate alignment | Weak alignment

(E) Enacted
(P) Pending
(Title [x]) Title [x] of the Council of Europe Convention on Cybercrime

Area	Legislative regime to be compared with benchmark	Benchmark legislation	Overall alignment	Areas of strong alignment	Areas of moderate alignment	Areas of weak alignment
Computer Security Laws	Criminal Code (E); Telecommunications Act (E); Communications Protection and Monitoring Act (E)	Council of Europe Convention on Cybercrime (Titles 1, 2 and 5)		• Illegal access, data interference and illegal interception offences • Computer-related forgery offence	• System interference offence • Partial implementation of misuse of devices offence • No computer-related fraud offence, but conduct may fall within general fraud offence • Ancillary liability for aiding and abetting cybercrimes	• No ancillary liability for attempting the commission of computer-related offences, and no corporate criminal liability
Privacy Laws	Computer-Processed Data Protection Law (E)	Model Privacy Bill (drafted by Microsoft)		• Definition of personal data • Data subject's right to access and correct personal data	• Mode of enforcement (enforcement by state and individuals cf. enforcement by Commissioner) • Consequence of infringement (criminal, administrative and civil liability cf. statutory and civil liability)	• Limited application of the regime in the private sector • Regime only applies to personal data that is collected or processed by computer • Restrictions on transborder data flows • Licensing regime operated by industry-specific government authorities • Transparency notifications made to government authority not data subject • No breach notification provisions
	Amendment to the Computer-Processed Data Protection Law (P)	An English translation of this amending legislation was not readily available to enable a benchmark analysis to be conducted.				

Area	Legislative regime to be compared with benchmark	Benchmark legislation	Overall alignment	Areas of strong alignment	Areas of moderate alignment	Areas of weak alignment
Spam Laws	Draft Commercial Spam Statute (P)	Anti-spam legislation checklist (drafted by Microsoft)		• 'Opt-out' regime • Recovery of capped statutory damages • Transparency requirements (sender identification, functional unsubscribe facility)	• Some recognition of pre-existing business relationships	• Labelling requirements for unsolicited commercial emails • Private right of action for all persons affected by spam (and not just ISPs/email service providers) • No ISP safe harbour for transmitting infringing messages or express exclusion of obligation on ISPs to carry or block certain electronic messages • Provision for class actions led by public-interest associations
Online Child Safety Laws	The Law to Suppress Sexual Transactions involving Children and Juveniles (E)	Council of Europe Convention on Cybercrime (Title 3 COE)/ICMEC principles		• General prohibitions on the production, distribution and sale of child pornography • Criminalisation of internet-facilitated distribution of child pornography		• Mere possession of child pornography not criminalised • No scope for ISP reporting of dealing in child pornography

14. Thailand

Part 1 – Snapshot of Legislative Status

Key: (E) Enacted
(P) Pending
(Title [x] COE) Title [x] of the Council of Europe Convention on Cybercrime (COE)

Area	Topic	Enacted legislation	Pending legislation	Relevant instruments/Comments
Computer Security Laws	**Core offences (Title 1 COE):** illegal access, illegal interception, data interference, system interference, misuse of devices	✓	✗	Computer Crime Act (E); Penal Code (E)
	Computer-related offences (Title 2 COE): computer-related forgery, computer-related fraud	✓	✗	Computer Crime Act (E); Penal Code (E)
	Ancillary liability (Title 5 COE): attempt and aiding/abetting, corporate liability	Partial	✗	Computer Crime Act (E); Penal Code (E)
Privacy Laws	**Data protection**	Partial	✓	Official Information Act of 1997 (E) Personal Data Protection Bill (P)
	Surveillance (see illegal interception under computer security)	✓	✓	Telegraph and Telephone Act of 1934 (E); Anti-Money Laundering Law of 1999 (E) National Identity Card Bill (P) The Anti-Money Laundering Office announced in July 2005 that it is seeking an amendment to the Anti-Money Laundering Law of 1999 (E).
	Sensitive information	✓	✗	Credit Information Business Act of 2002 (E)
Spam Laws	**Anti-spam regulation**	✗	✗	Computer Crime Act (E)
Online Child Safety Laws	**General child pornography offences**	✓	✗	Computer Crime Act (E); Penal Code (E) In 2005 a bill was tabled in the House of Representatives to address child pornography. It is not known if or when these legislative proposals will proceed to enactment.
	Computer-facilitated child pornography offences (Title 3 COE)	✗	✗	

Part 2 – Legal and Regulatory Position

2.1 COMPUTER SECURITY LAWS – CURRENT LEGISLATIVE FRAMEWORK

The Computer Crime Act 2007 came into force on 10 July 2007. It creates a number of criminal offences relating to the integrity of computer systems and data, and has clearly been influenced by the Council of Europe's Convention on Cybercrime.

In addition, provisions of the Penal Code may apply to some of the acts criminalised by the Council of Europe's Convention on Cybercrime.

Core offences (Title 1 COE): Illegal access, illegal interception, data interference, system interference, misuse of devices

Computer Crime Act

The Computer Crime Act has two illegal access offences: one in respect of a computer system that is secured with an access protection measure that is not meant for the offender's use; and another in respect of computer data that is secured in the same way. Contrastingly, the Convention has a single illegal access offence that applies in relation to the whole or any part of a computer system. The Act's illegal access offence in respect of a computer system is punishable by up to six months imprisonment and/or a fine of THB10,000 (approximately USD$310). The same offence committed in respect of computer data is punishable by up to two years imprisonment and/or a THB40,000 fine (approximately USD$1,240).

The Computer Crime Act also contains illegal interception and data interference offences that appear to be broadly aligned with the

equivalent offences in the Convention. However, the Act's data interference offence does not appear to extend to the suppression of computer data without right and the illegal interception offence only appears to apply to transmissions of data within a computer system as opposed to also applying to transmissions between computer systems which is how it is dealt with in the Cybercrime Convention. The Act's illegal interception offence is punishable by up to three years imprisonment and/or a THB60,000 fine (approximately USD$1,860), whereas the data interference offence is punishable by up to five years imprisonment and/or a THB100,000 fine (approximately USD$3,100), unless damage is caused to the general public or to computer data or a computer system relating to national security, public safety, economic stability or public utilities, in which case higher penalties apply.

Illegally causing a third party's computer system to be "suspended, delayed, hindered or disrupted" so that the computer system fails to operate normally is also an offence under the Computer Crime Act (maximum penalty: five years imprisonment and/or a THB100,000 fine (approximately USD$3,100)). As with the Act's data interference offence, higher penalties apply if the system interference causes damage to the general public or to computer data or a computer system relating to national security, public safety, economic stability or public utilities. In practical terms, the Act's system interference offence is likely to apply more broadly than its Convention counterpart since there is no requirement under the Act that the system interference must seriously hinder the functioning of a computer system – it is enough that the interference affects the computer system's normal operations.

The Computer Crime Act does not criminalise the misuse of devices to the extent that is contemplated in the Convention on Cybercrime. However, the Act does criminalise the sale or dissemination of programs designed to commit the offences mentioned above, as well as the illegal disclosure of access security measures in a manner that is likely to cause damage to the person who created those access security measures. Both of these offences are punishable by imprisonment for up to one year and/or a THB20,000 fine (approximately USD$615).

It is also worth noting that the Computer Crime Act contains additional offences that do not have direct counterparts in the Convention on Cybercrime. These include:

- the offence of sending emails or computer data with concealed information as to their source in such a way that interferes with the normal operation of the recipient's computer system; and
- offences concerning the input or dissemination of computer data in connection with an offence under Thailand's Penal Code.

Computer-related offences (Title 2 COE): Computer-related forgery, computer-related fraud

Computer Crime Act

It is an offence to input or disseminate forged data into a computer system in a manner that is likely to (i) cause damage to a third party or to the public, or (ii) undermine national security or cause public unrest (maximum penalty: five years imprisonment and/or a THB100,000 fine (approximately USD$3,100)). Services providers (ISPs and those that provide computer data storage services) face the same fine as the primary offender if they intentionally support or give their consent to someone undertaking this prohibited conduct. Under the Convention's computer-related forgery offence, it is enough that the data is altered or suppressed with the intention that it may be acted upon for legal purposes as if it was authentic; whether or not the conduct caused, or is likely to cause, damage is irrelevant. Contrastingly, under the Thai Act, the likelihood of damage is a key element of the offence.

There is no offence in the Computer Crime Act that deals with computer-related fraud (i.e. the act of causing a loss of property to a person by (i) inputting, altering, deleting or suppressing computer data, or (ii) interfering with the functioning of a computer system, with the intention of deriving an economic benefit or profit).

Other laws

Computer-related forgery and fraud may also be covered by the Penal Code's general forgery and fraud offences, although this is yet to be tested in the courts. The Penal Code offence of obtaining property by impersonating another may be relevant; this offence is punishable by a fine of up to THB10,000 (approximately USD$310), imprisonment for up to five years, or both.

Ancillary liability (Title 5 COE): Attempt and aiding/abetting, corporate liability

Computer Crime Act

The Computer Crime Act does not contain any provision that directly deals with aiding, abetting or attempting to commit the offences contained in the Act, or provisions that address corporate criminal liability generally. However there is a separate provision that makes internet and content service providers liable if they intentionally support or consent to another person using their service to (i) forge computer data, (ii) falsify computer data in a manner likely to damage national security of cause a public panic, (iii) import computer data related to an offence against the King of Thailand's security, or (iv) import any pornography.

14. Thailand

Other laws

Thailand's Penal Code provides for ancillary liability for attempting the commission of an offence, and aiding and abetting the same. However, it is not certain whether this ancillary liability would extend to computer-related offences. Corporations may be charged for some criminal acts of their officers or employees if the officers or employees are deemed to be acting on behalf of the company.

2.2 COMPUTER SECURITY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

At the date of writing, there are no upcoming legislative developments that relate to computer security.

2.3 PRIVACY LAWS – CURRENT LEGISLATIVE FRAMEWORK

Data protection

There is no private sector data protection legislation in Thailand. However, the Official Information Act 1997 regulates state agencies in their dealings with personal information – information relating to the "personal particulars" of a person, such as education, financial status and health records, and which is capable of identifying that person. Echoing the OECD guidelines, the Official Information Act requires state agencies to:

- Ensure that their personal information system is relevant to, and necessary for, the achievement of their objectives;
- Make an effort to collect personal information directly from the data subject and where personal information is so collected, notify the data subject of certain matters prior to or upon collection, such as the likely uses of their personal information;
- Publish material about the personal information's use in the Government Gazette;
- Provide for an appropriate security system in respect of held personal information;
- Notify the data subject if personal information is collected about him or her from a third party;
- Not disclose personal information to other state agencies or other persons without the data subject's prior or immediate written consent, except where the personal information will be used in accordance with the powers of the relevant State agency, the disclosure is necessary to prevent criminal activity and in certain other limited circumstances;
- Notify the data subject if their personal information is dispatched to any place in which it may become known to the general public, unless this is carried out in conformity with the ordinary use of the personal information; and
- Provide the data subject with rights of access, correction and deletion in respect of held personal information.

Enforcement of the Official Information Act is time-consuming and the process depends on the nature of the alleged contravention. The Act establishes Information Disclosure Tribunals that consider (at the request of the data subject concerned) refusals by state agencies to alter, correct or delete a data subject's personal information. The Official Information Board appears to have a broader mandate to consider complaints about violations of the Act, although its powers to sanction state agencies that have contravened the Official Information Act are not clear. That said, a failure to comply with an order or summons by the Official Information Board to furnish information or evidence is a criminal offence that attracts a fine of up to THB5,000 (approximately USD$160), imprisonment for up to three months or both.

Surveillance

Phone tapping without a warrant is a criminal offence under Thailand's Telegraph and Telephone Act 1934; offenders can face up to five years imprisonment. The Anti-Money Laundering Law of 1999 entitles police officers and other officials to gain court-issued interception warrants where there is "probable cause to believe" that a device or equipment was used, or might be used, in the commission of a money laundering offence.

Pursuant to the Identification Card Act of 1983, Thai citizens must apply for a national ID card within 60 days of turning 15 years old. Those over the age of 70 do not need to hold an ID card. The data held on the card is currently limited to basic personal information, such as the holder's legal name and date of birth. Thai citizens must produce their ID cards whenever confirmation of identity is necessary.

Sensitive information

The Official Information Act does not oblige state agencies to take special measures to protect sensitive information such as an individual's ethnic or racial origin. The Credit Information Business Act affords some protection to personal financial information insofar as it seeks to protect the integrity of personal information collected and used in the course of financial transactions (whether these transactions are with financial or non-financial institutions).

Miscellaneous

Thailand's Constitution contains several privacy-related protections. Section 34 provides that a person's "family rights, dignity, reputation or the right of privacy" shall be protected by law, while section 37 prohibits the interception of lawful communications unless the interception is (i) pursuant to a statutory power and (ii) for the purpose of maintaining national security, peace and order, or good public morality. Finally, section 58 affords Thai citizens the right to gain access to public information held by state agencies, unless the disclosure of this information affects national security, public safety or the interests of other persons protected by law.

2.4 PRIVACY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

Data protection

The Thai government has considered two versions of private sector data protection legislation: one drafted by the National Electronics and Computer Technology Center (NECTEC); and another drafted by the Office of the Official Information Commission. After much debate and the intervention of the Prime Minister, it is understood that the version drafted by the Office of the Official Information Commission is more likely to be adopted and jointly implemented by the Office of the Official Information Commission and the Ministry of Information and Communication Technology. The draft legislation is now being reviewed to determine how it can be amended to better align with the APEC Privacy Framework and address private sector concerns with the current drafting of the bill. It is still uncertain when the bill is expected to be enacted.

In June 2004, the Thai government was considering a draft amendment to the Official Information Act designed to improve the efficiency and effectiveness with which the Official Information Act's provisions can be enforced.

Surveillance

The Thai Cabinet has approved, in principle, a draft of the National Identity Card Bill submitted by the Interior Ministry. This Bill would require newborns to apply for identity cards within 60 days of birth and children under 15 to apply for an identity card within one year. It is unclear when this bill is likely to be enacted.

2.5 SPAM LAWS – CURRENT LEGISLATIVE FRAMEWORK

There is no comprehensive anti-spam legislation in Thailand.

However, it is an offence under the Computer Crime Act to send emails with concealed information as to their source in such a way that interferes with the normal operation of the recipient's computer system (maximum penalty: THB100,000 fine (approximately USD$3,100)). This offence could apply to sending a spam message in some circumstances.

In addition, to the extent that a spam message contains:

- false data that is likely to undermine national security or cause public unrest; or
- forged data that is likely to cause damage to a third party or to the public,

It will be an offence under the Computer Crime Act to disseminate that message through a computer system.

Finally, if a spam message constitutes an offer to sell goods or services direct to the public:

- the spammer is required to register as a direct marketing business operator under the Direct Sales and Marketing Act;
- consumer protection laws that relate to advertising will apply to the content of the spam; and
- the offer must be in Thai and must contain information required by the Direct Sales and Marketing Act.

2.6 SPAM LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

At the time of writing, there are no upcoming legislative proposals to enact anti-spam legislation.

2.7 ONLINE CHILD SAFETY LAWS – CURRENT LEGISLATIVE FRAMEWORK

General child pornography offences

The age of majority in Thailand is 20 years; the age of consent to sexual relations is 15 years.

Thailand has not enacted specific laws prohibiting the dissemination of child pornography. Instead, the Penal Code prohibits the distribution, exhibition, production and possession of obscene material (which is likely to embrace most forms of child pornography). Offenders are liable to a fine of THB6,000 (approximately USD$185), imprisonment for up to three years or both.

The Computer Crime Act also prohibits the acts of inputting into a computer system or disseminating via a computer system any pornographic computer data that is accessible to the public (maximum penalty: five years imprisonment and/or a THB100,000 fine (approximately USD$3,100). This offence would apply to child pornography to the extent that the offending material is made publicly available using a computer system (e.g. by posting child pornography onto a website or otherwise making child pornography available online). Service providers (ISPs and those that provide computer data storage services) face the same liability as the principal offender if they intentionally support or consent to the input or dissemination of pornography using their services.

Computer-facilitated child pornography offences (Title 3 COE)

There are no Thai laws that specifically prohibit computer-facilitated dealings in child pornography.

14. Thailand

2.8 ONLINE CHILD SAFETY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

Computer-facilitated child pornography offences (Title 3 COE)

In 2005, it was understood that a separate child pornography bill had been tabled in the House of Representatives. This bill defined child pornography to include digital material, rendered possession of child pornography illegal and doubled the applicable penalties if the subject of the child pornography was under 18. Production of child pornography remained outside the scope of the bill.

Miscellaneous

In 2005, the Cabinet had approved a proposal by the Ministry of Information and Communication Technology to formulate regulations to (i) establish a licensing regime for internet café operators and (ii) restrict the way in which minors can use online games. Under the proposed licensing regime for internet cafes, there would be restrictions on the opening hours of internet cafes and minimum standards for the physical environment within internet cafes. In addition, students under the age of 18 would only be allowed to use internet cafes during certain hours and may only play online games at an internet cafe for a maximum of three hours per day.

Part 3 – Benchmark Comparison

Key: Favourable alignment | Moderate alignment | Weak alignment

(E) Enacted
(P) Pending
(Title [x]) Title [x] of the Council of Europe Convention on Cybercrime (COE)

Area	Legislation to be compared with benchmark	Benchmark legislation	Overall alignment	Areas of strong alignment	Areas of moderate alignment	Areas of weak alignment
Computer Security Laws	Computer Crime Act 2007 (E); Penal Code (E)	Council of Europe Convention on Cybercrime (Titles 1, 2 and 5)		• Illegal access, illegal interception, data interference and system interference offences	• Computer-related forgery and misuse of device offences	• No specific computer-related fraud offence • No specific ancillary liability provisions under the Computer Crime Act
Privacy Laws	Official Information Act of 1997 (E)	Model Privacy Bill (drafted by Microsoft)		• State agencies are required to publish information about their privacy practices • Obligation to keep personal information free from loss or misuse • Data subjects' right to access and correct personal information	• Definition of personal information • Mode of enforcement (enforcement initiated by individual complaint cf. enforcement by Commissioner or state official)	• Legislation only applies to state agencies • Privacy regime part of freedom of information legislation • Regime not premised on primary and secondary purposes of use or disclosure • Use of held personal information not regulated (only disclosure is) • Consequences of infringement are not clear
Spam Laws	There is no enacted or pending comprehensive spam legislation in Thailand upon which a benchmarking analysis can be conducted.					
Online Child Safety Laws	Computer Crime Act 2007 (E); Penal Code (E)	Council of Europe Convention on Cybercrime (Title 3 COE)/ICMEC principles			• General prohibitions on distribution, production and possession of obscene material • Prohibition on inputting or disseminating computer data of a pornographic nature that is publicly accessible	• No definition of child pornography • No general or computer-facilitated child pornography offences • No scope for ISP reporting of dealing in child pornography

Last Updated: 23 October 2007

15. Vietnam

Part 1 – Snapshot of Legislative Status

Key: (E) Enacted
(P) Pending
(Title [x] COE) Title [x] of the Council of Europe Convention on Cybercrime (COE)

Area	Topic	Enacted legislation	Pending legislation	Relevant instruments/Comments
Computer Security Laws	**Core offences (Title 1 COE):** illegal access, illegal interception, data interference, system interference, misuse of devices	✓	✗	Law on Information Technology 2006 (E); Law on E-Transactions 2005 (E); Decree No 55 on the Management, Provision and Use of Internet Services (E); Decree No 142 Specifying Administrative Penalties in the Field of Post, Telecommunications and Radio Frequency (E); Civil Code (E); Penal Code (E)
	Computer-related offences (Title 2 COE): computer-related forgery, computer-related fraud	✗	✗	
	Ancillary liability (Title 5 COE): attempt; aiding/abetting, corporate liability	Partial	✗	Law on Information Technology 2006 (E) (corporate criminal liability only)
Privacy Laws	**Data protection**	✓	✗	Law on Information Technology 2006 (E); Law on E-Transactions 2005 (E)
	Surveillance (see illegal interception under computer security)	✓	✗	Law on Information Technology 2006 (E); Law on E-Transactions 2005 (E); Law on National Security 2004 (E)
	Sensitive information	✓	✗	
	Miscellaneous	✓	✗	Civil Code (E); Decree No 55 on the Management, Provision and Use of Internet Services (E)
Spam Laws	**Anti-spam regulation**	Partial	✓	Law on Information Technology 2006 (E); Ministry of Post and Telematics' Circular 04 dated 29 November 2004 implementing Decree 142 (E) A decree on spam is currently being drafted by the Vietnamese government.
Online Child Safety Laws	**General child pornography offences**	Partial	✗	No general child pornography legislation, but it is an offence to distribute pornography and commit obscene acts against children (Penal Code (E))
	Computer-facilitated child pornography offences (Title 3 COE)	✗	✗	

Part 2 – Legal and Regulatory Position

2.1 COMPUTER SECURITY LAWS – CURRENT LEGISLATIVE FRAMEWORK

There is no single law that criminalises threats to computer security in Vietnam. Instead, there are a number of different laws that address the conduct prohibited by the Council of Europe's Convention on Cybercrime.

Core offences (Title 1 COE): Illegal access, illegal interception, data interference, system interference, misuse of devices

One general observation is that the provisions under Vietnamese law that address illegal access, illegal interception, data interference and system interference are not particularly well-aligned with the equivalent offences in the Cybercrime Convention. In part, this is due to the infrequency with which criminal liability appears to attach to the relevant provisions in Vietnamese law.

Illegal access and interception

Decree No 55 on the Management, Provision and Use of Internet Services (Decree No 55) prohibits unauthorised entry or illegal access to a telecommunications network or telecommunications line. Offenders could face fines of up to VND10 million (approximately USD$620). Article 72 of the Law on Information Technology 2006 (IT Law) prohibits (i) hacking in order to access information held by other organisations or individuals and (ii) deleting or de-activating data or system security software. The IT Law is discussed in greater detail on the next page.

The scope of the offence appears to be narrower than the illegal access offence in the Cybercrime Convention which applies to access without right to a computer system, not a telecommunications network or line. Another difference is that unlike the Convention offence the provision in Decree No 55 does not contain an express requirement for the illegal act to be committed intentionally.

"Stealing" or intercepting and illegally using the private information of an organisation or individual on the Internet is prohibited by Decree No 55, and Decree No 142 specifying Administrative Penalties in the Field of Post, Telecommunications and Radio Frequency prohibits eavesdropping, stealing, destroying, or using private information of other individuals or organisations without their permission. Offenders could be fined up to VND10 million (approximately US$620). These provisions can be contrasted with the illegal interception offence in the Cybercrime Convention which provides that a person cannot intentionally and without right intercept the non-public transmission of computer data between or within computer systems.

Data and system interference

There are a number of provisions in Vietnamese law that deal with instances of data or system interference and these are examined in the following sections.

Penal Code

Under Article 226 of the Penal Code, a person who illegally uses or enters information into a computer system and consequently causes serious damage to another person may face up to five years imprisonment and/or a fine of up to VND30 million (approximately USD$1,870). Further, those who disrupt the operation of a computer system or block, corrupt or destroy data on a computer system could face up to five years imprisonment and/or a fine of VND30 million (approximately USD$1,870).

Decree No 55 and related laws

Decree No 55 prohibits some acts that could constitute system or data interference under the Convention framework. For example, the use of technical devices or expertise to illegally access a telecommunications network and destroy database(s), software or hardware of the network may result in criminal prosecution or fines of up to VND50 million (approximately US$3,120) depending on the severity of the offence. Those that access the Internet without authorisation (though it is unclear when access to the Internet will be unauthorised) and disrupt the operation of the Internet or block the transmission of data could face a fine of up to VND20 million (approximately US$1,250) and may also be temporarily or permanently prohibited from using the Internet.

Decree No 55 also prohibits the acts of disrupting and destroying computer systems and holds offenders liable to fines of between VND5 million and 10 million (approximately USD$310 – USD$620).

IT Law

Unlike the approach used in many other countries and in Vietnam's own Penal Code, the IT Law does not set out specific penalties for a breach of each of its provisions. Rather, it contains a general provision which appears to provide that depending on the severity of the breach individuals can face disciplinary action, administrative sanctions, penal liability (e.g. imprisonment) or may have to pay compensation. Organisations that contravene the IT Law are liable to administrative sanctions, trading suspensions or may have to pay compensation for damage caused.

Some acts of illegal interception, data interference and system interference are prohibited by articles 71 and 72 of the IT Law. Under article 71 organisations and individuals may not create, install or spread computer viruses or malware on digital equipment belonging to other people in order to (i) change the installation parameters of the equipment, (ii) collect other people's information, (iii) delete or de-activate data and system security software, (iv) prevent users from deleting or limiting the use of unnecessary software, (v) modify or delete data, and (vi) do other acts infringing a user's "legitimate rights and interests".

Article 72 prohibits (i) modifying or deleting information of other organisations or individuals, (ii) "obstructing the provision of services by [an] information system", and (iii) other acts which interfere with the security or confidential nature of information which is transmitted or stored over a network.

Article 12 prohibits two specific kinds of system interference – illegally obstructing the operation of national domain-name servers, or destroying the information infrastructure of Vietnam. Article 12 also addresses data interference, but only to the extent that it involves destroying information in a computer network.

E-Transactions Law

The E-Transactions Law appears to prohibit the acts of:

- illegally obstructing or preventing the process of transmitting, sending and receiving data messages;
- illegally modifying, deleting, cancelling, counterfeiting, copying disclosing, displaying or moving part or all of a data message; and
- creating or disseminating software programs that trouble, change or destroy operating systems or software underpinning e-transactions.

15. Vietnam

There is no express penalty or remedy provided under the E-Transactions Law for contraventions of its provisions. References to acting "illegally" in the English translation of the E-Transactions Law may be intended to refer to a concept similar to acting "without right" which is used in the Cybercrime Convention.

Civil Code

The Civil Code provides that no person is permitted to interfere with the transmission of communications of another person. It is understood that this provision would extend to interference with electronic communications.

Misuse of devices

Although Vietnamese law does not appear to contain offences equivalent to the misuse of devices offence in the Convention on Cybercrime, the Penal Code, Decree No 55 and Decision 71 on Providing Regulations on Ensuring Security and Safety in the Management, Supply and Use of Internet Activities prohibit the acts of producing and intentionally disseminating or propagating computer viruses on the Internet. Under the Penal Code offenders can face fines of up to VND50 million (approximately US$3,120). Decree No 55 also prohibits the acts of stealing or illegally using passwords. Offenders could face fines of between VND5 million and 10 million (approximately USD$310 – USD$620). Article 71 of the IT Law discussed above also addresses the misuse of devices. Decree No 142 prohibits using a device to illegally access and destroy a database, software, or hardware in a telecommunications network. These offences can be viewed as a partial implementation of the Convention's misuse of devices offence.

Computer-related offences (Title 2 COE): Computer-related forgery, computer-related fraud

Under Vietnamese law there are no provisions that specifically address computer-related fraud or forgery in the manner that those acts are dealt with in the Cybercrime Convention. That said, one specific instance of computer-related forgery appears to be prohibited by the E-Transactions Law – a person must not wrongfully or illegally use the electronic signatures of others. There does not appear to be any liability imposed on those who breach this provision.

Ancillary liability (Title 5 COE): Attempt and aiding/abetting, corporate liability

The Penal Code contains a provision imposing liability on those who are involved with preparing to commit a crime. However, it does not apply to any of the provisions discussed above. There are no terms in any other law discussed in this Section 2.1 that address attempting or aiding and abetting the breach of a computer security provision.

Only the IT Law has provisions addressing corporate liability. Corporations or other organisations that breach the IT Law may be liable to administrative sanctions, trading suspensions or may have to pay compensation for damage caused.

Miscellaneous

Circular 04 issued by the Ministry of Post and Telematics in November 2001 obliges Internet users in Vietnam to maintain the confidentiality of their passwords, codes, private information and to protect and secure their own Internet equipment and systems. It further obliges users to coordinate with, and assist, the relevant authorities to ensure the security of the Internet, network hardware and information available on the Internet, and to assist them in carrying out investigations and preventing Internet crimes. It is understood that the Circular was amended in August 2006 although the details of this amendment are uncertain.

2.2 COMPUTER SECURITY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

At the date of writing, there are no upcoming legislative developments that relate to computer security.

2.3 PRIVACY LAWS – CURRENT LEGISLATIVE FRAMEWORK

Data protection

There do not appear to be any data protection laws of general application in Vietnam.

However, the IT Law does address the use of personal information in a networked environment. Article 21(1) of the IT Law provides that organisations and individuals that collect, process and use personal information in the networked environment must obtain the consent of the data subject. Consent is not needed: (i) where another law specifies it is not needed, (ii) when signing, performing or modifying a contract relating to the use of information, products or services in the network environment, or (iii) when calculating the charges for use of information products or services in a networked environment.

Anyone that collects personal information from an individual is required to:

- inform the individual about the form, scope, place and purpose of collecting, processing and using that individual's personal information;
- use the personal information for the "proper purpose," which is an undefined concept that may mean the purpose for which it was collected;
- store the personal information only for the period of time set by law or as agreed between the parties;
- take the necessary managerial and technical measures to maintain the security and integrity of the personal information;

- inspect and correct personal information about an individual when they request it and not supply or use that personal information until it has been corrected; and
- not disclose that personal information to a third party without the consent of the individual.

The IT Law also provides that individuals have a right to claim compensation as a result of someone else supplying their personal information in contravention of the IT Law.

The E-Transactions Law also contains provisions that address how to handle personal information collected as part of an electronic transaction. Information about the private and/or personal affairs of an individual, agency or organisation accessible by, or under the control of, the other party in an electronic transaction cannot generally be disclosed without the consent of the individual, agency or organisation to whom the information relates.

Surveillance

Article 20 of the IT Law appears to impose a general and seemingly broad obligation on competent state agencies to monitor and supervise digital information and investigate violations committed in the course of transmitting or storing digital information. However, Article 20(2) appears to require an organisation or individual that provides information technology services to monitor or supervise the digital information of their users at the request of a competent state agency.

Article 60 of the IT Law provides that organisations and individuals must submit to the "management, inspection and examination" of a competent state agency and must meet that agency's requirements for ensuring the security of their information infrastructure. It is unclear exactly what an individual or organisation will be required to do in order to comply with any such request by a competent state agency pursuant to Article 60(2).

Article 49 of the Law on E-Transactions provides that competent state agencies have the right to (i) search and seize part or all of a computer system and messages in such a system, copy and store copies of data messages, and (ii) prevent access to a computer system. The Law does not specify who are the competent state agencies, in what circumstances they will have the right to do the things specified in Article 49 or what penalties exist for a breach of this provision.

Under the Law on National Security 2004, the state agency in charge of the protection of national security has the right to examine communication equipment, computers, computer networks and materials of individuals and organisations if it has a reasonable suspicion that there has been a breach of national security. This provision potentially gives the relevant state agency the right to access all electronic information held by an organisation or individual.

Sensitive information

There appears to be no provision under Vietnamese law that deals specifically with the handling of sensitive personal information.

Miscellaneous

Article 34 of the Civil Code provides that an individual's right to privacy "shall be protected by law". However, there is no law dedicated to specifying the ambit of this right. Article 34 also provides that the collection and publication of information and materials regarding the private life of an individual must only occur with that individual's consent or in accordance with a decision of a competent state authority made pursuant to Vietnamese law. The Civil Code does not define what constitutes information and material relating to the private life of an individual and so there is the potential for this phrase to be narrowly interpreted by state authorities, thereby reducing the scope of an individual's right to privacy.

Decree No 55 on the Management, Provision and Use of Internet Services provides that the confidentiality of private information of individuals and organisations on the Internet must be protected according to the Constitution and other Vietnamese laws. The detail of how this information is to be protected is not prescribed by the Decree.

2.4 PRIVACY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

At the date of writing, there are no upcoming legislative developments that relate to privacy.

2.5 SPAM LAWS – CURRENT LEGISLATIVE FRAMEWORK

There is no comprehensive anti-spam legislation in Vietnam. However, there are provisions in both the IT Law and in a Ministry of Post and Telematics Circular that purport to address spam.

Article 70 of the IT Law, entitled 'Prevention of spam', contains three provisions. The first is that when a person or organisation sends information over a network, that person or organisation may not hide their name or impersonate other organisations or individuals. While it is possible that the purpose of this paragraph is to ensure that those who send spam identify themselves properly, the prohibition in Article 70(1) is not limited to the spam context and it is capable of application to all information sent over a network, including emails, online posts and information submitted via an online form.

15. Vietnam

The second paragraph of Article 70 provides that where advertisement information is sent over a network it must contain an unsubscribe facility. Again there is no qualification on the scope of this requirement; it applies to all advertisement information (a term which does not appear to be defined), which could, in some circumstances, include transactional messages to the extent they include an advertisement for a product or service.

Finally, Article 70(3) provides that where an individual has informed a sender that they no longer wish to receive advertisement information, the sender must stop sending this information to that individual.

A breach of the IT Law could result in disciplinary action, an administrative sanction, penal liability or, if damage is caused, a requirement that the offender pay compensation for that damage.

Under Circular 04 issued by the Ministry of Post and Telematics in November 2004 (which provides guidance on the implementation of Decree No 142) sending unsolicited messages which have the effect of destroying a database, software or hardware in a telecommunications network could result in criminal prosecution or a fine of up to VND50 million (approximately USD$3,120) depending on the severity of the offence.

2.6 SPAM LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

The Vietnamese government is in the process of drafting a decree on spam. An inter-governmental group consisting of officials from the Ministry of Post and Telematics, the Government Office, the Ministry of Public Security, the Ministry of Trade, the Ministry of Justice and the Ministry of Culture and Information have been tasked with drafting the decree. It has been reported that a draft of the decree could be submitted to the government in late 2007 and issued by 2008.

The contents of the proposed decree are not known, though it is understood that the decree will apply to messages received via email, mobile phones, fax machines and telephones, and will contain measures that prohibit the use of address harvesting software and harvested address lists. It has been reported that the inter-governmental group drafting the decree is considering adopting an opt-out approach for unsolicited messages sent via email and an opt-in approach for unsolicited messages sent via post.

2.7 ONLINE CHILD SAFETY LAWS – CURRENT LEGISLATIVE FRAMEWORK

General child pornography offences

The age of majority in Vietnam is 18 years. The age of consent to sexual relations is also 18 years.

Vietnam has not enacted specific legislation that addresses child pornography. Instead, the Penal Code contains a general offence prohibiting the distribution of pornography and is punishable by a fine, reform without detention for up to three years or imprisonment from six months to 15 years. There is also an offence of "disseminating debauched cultural products", which involves duplicating, circulating, transporting, selling, purchasing or stockpiling "decadent" publications and objects, including books, film and photographs, for the purpose of dissemination. This offence is punishable by a fine of between VND 5 and 50 million (approximately USD$310 – $3,120), reform without detention for up to three years or imprisonment for six months to 15 years. The concept of a "decadent" publication is not defined. An increased term of up to three to 10 years imprisonment applies to offenders who commit this crime against juveniles.

Those who commit obscene acts against children (a child is a person under the age of 16 years) can also be held liable under the Penal Code for a term of imprisonment between six months and three years. The Penal Code does not appear to define what constitutes an obscene act, but this concept is likely to include the act of involving a child in the creation of child pornography. Offenders are liable to more severe penalties where they commit this crime more than once, against more than one child, against a child whom the offender has the responsibility of taking care of, educating or treating medically, or where the obscenity has "serious consequences". The maximum penalty for this offence is 12 years imprisonment.

Computer-facilitated child pornography offences (Title 3 COE)

Vietnam does not have any legislation that creates computer-facilitated child pornography offences.

Miscellaneous

Article 73 of the IT Law imposes an obligation on the State, society and schools to protect children against the negative impacts of information presented online and take measures to prevent and combat IT applications that incite violence or contain obscene content. The IT Law also requires (i) families to prevent children from accessing harmful information (a term which does not appear to be defined), (ii) service providers to take measurers to prevent children from accessing harmful information in a networked environment, and (iii) those who supply IT products and services to children to include a warning with those products and services that their contents could be harmful to children. A breach of the IT Law could result in disciplinary action, administrative sanctions, penal liability or a requirement to pay compensation.

2.8 ONLINE CHILD SAFETY LAWS – UPCOMING LEGISLATIVE DEVELOPMENTS

At the date of writing, there are no upcoming legislative developments that relate to online child safety.

Part 3 – Benchmark Comparison

Key: Favourable alignment | Moderate alignment | Weak alignment

(E) Enacted
(P) Pending
(Title [x]) Title [x] of the Council of Europe Convention on Cybercrime

Area	Legislative regime to be compared with benchmark	Benchmark legislation	Overall alignment	Areas of strong alignment	Areas of moderate alignment	Areas of weak alignment
Computer Security Laws	Law on Information Technology 2006 (E); Law on E-Transactions 2005 (E); Decree No 55 on the Management, Provision and Use of Internet Services (E); Decree No 142 Specifying Administrative Penalties in the Field of Post, Telecommunications and Radio Frequency (E); Civil Code (E); Penal Code (E)	Council of Europe Convention on Cybercrime (Titles 1, 2 and 5)			• Illegal access, illegal interception, data and system interference and misuse of devices offences	• No specific computer-related fraud and forgery offences • No specific ancillary liability provisions for attempting, aiding or abetting cybercrimes • No specific corporate criminal liability for cybercrimes
Privacy Laws	Law on Information Technology 2006 (E); Law on E Transactions 2005 (E)	Model Privacy Bill (drafted by Microsoft)		• Data subject's right to access and correct personal information • Obligation to maintain security of personal information	• No definition of personal information • Transparency matters that must be notified to data subject (e.g. the purposes of use of the personal information)	• Applies only to information stored in a networked environment • Consent is generally needed before personal information can be collected, used or disclosed • No explicit distinction between primary and secondary purposes of use and disclosure • No breach reporting provisions • No additional obligations in respect of sensitive information
Spam Laws	There is no comprehensive enacted or pending spam legislation in Vietnam upon which a benchmarking analysis can be conducted.					
Online Child Safety Laws	Penal Code (E)	Council of Europe Convention on Cybercrime (Title 3 COE)/ICMEC principles			• General prohibitions on distribution of pornography	• No general child pornography offences • No computer-facilitated child pornography offences • No definition for child pornography • No scope for ISP reporting of dealings in child pornography

Last Updated: 24 October 2007

Microsoft®

For further information, please contact:

Julie Inman Grant
Regional Director, Corporate Affairs
Internet Safety and Security
Microsoft Asia Pacific
juliei@microsoft.com

November 2007