

available at www.sciencedirect.comwww.compseconline.com/publications/prodclaw.htm

**Computer Law
&
Security Report**

Pacific Rim news

A snapshot of legal developments and industry issues relevant to information technology, media and telecommunications in key jurisdictions across the Asia Pacific – Co-ordinated by Lovells and contributed to by other leading law firms in the region

Gabriela Kennedy, Sarah Doyle

Lovells, Hong Kong

A B S T R A C T

This new column provides a country-by-country snapshot of the latest legal developments, cases and issues relevant to the IT, media and telecommunications industries in key jurisdictions across the Asia Pacific region. The articles appearing in this column are intended to serve as 'alerts' and are not submitted as detailed analyses of cases or legal developments.

© 2007 Lovells. Published by Elsevier Ltd. All rights reserved.

1. Hong Kong

1.1. *Leaked data scandal causes Hong Kong to rethink its data protection laws*

The scope of the powers conferred on Hong Kong's Privacy Commissioner for Personal Data ("Commissioner") under the Personal Data (Privacy) Ordinance ("Ordinance") have become the subject of public debate following the widely publicized 'leak' of personal data relating to approximately 20,000 individuals from the from the Independent Police Complaints Council ("IPCC"). The personal data, which made its way onto the Internet after falling into the hands of an independent contractor, related to persons who had made complaints to the police, including crime victims.

The Commissioner, in exercising the powers conferred upon him under the Ordinance, initiated an investigation of the IPCC which revealed serious deficiencies in the IPCC's

data security and protection policies, procedures and safeguards. The Commissioner's findings were that, in allowing the personal information of complainants to be accessed by an independent contractor without either taking measures to ensure the integrity of the contractor or imposing any positive obligations on the contractor to safeguard such data, the IPCC had contravened the requirements of Data Protection Principle 4, which imposes an obligation on data users to take all reasonably practicable steps to ensure that personal data held by it is protected against unauthorized or accidental access, processing, erasure or other use.

Based on this finding, the Commissioner exercised the only enforcement power conferred upon him under the Ordinance for the Contravention of a Data Protection Principle, namely the issuance of an Enforcement Notice under Section 50 of the Ordinance. Under the Ordinance, an Enforcement Notice serves merely as a formal direction to a contravening data user to take any steps specified in the notice to remedy the

contravention. Provided that such steps are taken, then no penalty or further recourse is available against the contravening data controller in respect of the contravention under the Ordinance. It is only the subsequent contravention by the data user of the Enforcement Order that gives rise to any prosecution or 'actual' penalty as such.

This framework effectively gives data users 'carte blanche' to contravene the Personal Data Principles which underpin the Ordinance and provide protection against the misuse of personal data.

The justification for the lack of real powers conferred upon the Commissioner under the Ordinance is based on the original intent and purpose of the introduction behind the Ordinance, which was to promote awareness of privacy and protection of personal data amongst the Hong Kong population and not to detect or punish misuse of such data as such.

However, with the advent of the Internet and technological measures which permit the electronic storage and instantaneous transmission and dissemination of information all over the world, there are calls for the Ordinance, which was introduced more than 10 years ago, to be amended to reflect the current technological climate and to address what is now, thanks to the well publicized IPCC scandal, widely considered amongst the Hong Kong population to be a serious issue worthy of closer scrutiny and tougher measures.

As privacy and personal data protection receive increasing attention internationally, the failure of Hong Kong to introduce in its laws enforcement measures equally robust to the data protection laws in place in other jurisdictions carries with it the risk of restricting the free flow of personal data into Hong Kong which may, in turn, have serious consequences for Hong Kong's economic well-being.

Sarah Doyle (Australian qualified lawyer), Lovells, Hong Kong, sarah.doyle@lovells.com; and *Gabriela Kennedy* (Partner), Lovells, Hong Kong, gabriela.kennedy@lovells.com.

1.2. ISP liability for copyright infringement under review

There are no reported cases in Hong Kong to date in which an ISP has been sued or held liable in the context of copyright infringement by one of its Internet account subscribers. It is, however, well established in Hong Kong that an ISP may be subject to *Norwich Pharmacal* order under which it is required to disclose all relevant details of any such Internet account subscriber suspected to have engaged in copyright infringing activities on or using the Internet.

While this has proven to be an effective means for copyright owners to identify potential infringers against whom they may have legal recourse, it is also time-consuming and the expenses incurred in obtaining an order often exceed any compensation recovered in subsequent legal proceedings against the persons identified.

The Copyright Ordinance is currently under review and the introduction of a more time and cost efficient mechanism for compelling the disclosure by ISPs of the identity of customers suspected of engaging in infringing activities on or using the Internet is being considered. Also under consideration is the introduction of new provisions which, if introduced, will go one step further and expose ISPs to liability for the copyright

infringing activities of their customers on the Internet. The proposals currently on the table are:

- (a) encouraging online service providers to develop, together with copyright owners, appropriate guidelines on good industry practices or codes of practice binding on all operators to combat online piracy activities (which may include tightening up service contracts with subscribers to put in place measures against repeated infringers);
- (b) imposing liability on online service providers in circumstances where an online service provider fails to take steps to remove or disable access to infringing materials identified on their service platforms; and
- (c) introducing factors to determine whether an online service provider has, in providing the relevant online services, 'authorised' infringing conduct undertaken by its customers utilizing the services offered (thereby themselves attracting liability for indirect copyright infringement).

The introduction of these amendments will greatly benefit copyright owners by allowing them direct recourse against ISPs, which are likely to have much deeper pockets than the customers responsible for direct copyright infringement, while potentially reshaping the role of ISPs in Hong Kong by requiring them to monitor and accept some level of responsibility for the activities of, and content posted or uploaded by, customers on the Internet.

Sarah Doyle (Australian qualified lawyer), Lovells, Hong Kong, sarah.doyle@lovells.com; *Gabriela Kennedy* (Partner), Lovells, Hong Kong, gabriela.kennedy@lovells.com; and *Christine Li* (Trainee), Lovells, Hong Kong.

2. People's Republic of China

2.1. New rules may improve anti-piracy measures for audiovisual products

The Ministry of Culture ("MOC") has recently issued *The Measure on Management of Wholesale, Retail and Rental of Audiovisual Products* (the "Measure"). The Measure came into effect on 1 December 2006 and replaces an identically named regulation first issued by the MOC on 5 March 2002, and subsequently amended on 2 June 2004. At least three key amendments brought in by the Measure could have a positive impact on anti-piracy efforts for audiovisual ("AV") products:

1. The Measure stipulates that dealers in AV products are not allowed to make, sell or rent any AV products that were unlawfully produced by any entity. This should be welcome news for overseas copyright holders, who typically suffer at the hands of their Chinese licensees who regularly manufacture AV products in excess of the orders placed by the overseas rights owners. Entities which deal in unlawfully produced AV products can be liable to a fine between one to five times their illegal revenue. A "serious case" will arise where 100 pieces of discs or more are involved, following which the MOC can suspend, rectify or even withdraw the violator's business license. This penalty may force traders

and retailers to tighten their screening criteria for lawfully produced and duplicated AV products, as well as for qualified distributors.

2. The Measure requires wholesalers and chain store proprietors to provide to the MOC the postal addresses of their warehouses or distribution centres, their managers' contact details, and to report any changes to such information. This provision aims to strengthen information management and assist anti-piracy investigations. However, the Measure does not set penalties for delayed recordation; nor does it set penalties for the willful modification of information or for providing false information.
3. The Measure also provides that the MOC will either issue a warning or impose a fine of RMB 10,000 (approximately US\$1270) on publishers or importers if they fail to place authentication labels on genuine AV products as mandated. Entities which deal with AV products over the Internet shall also identify their business qualifications and authentication marks. The Measure should help consumers distinguish between genuine and counterfeit AV products and assist anti-piracy efforts.

Other provisions in the Measure have received mixed comments.

For example, the Measure allows the MOC to reduce or waive the penalties imposed on an infringer if the infringer discloses the source of the illegal products (provided that such source can be later verified). Although the information obtained would help the MOC investigate piracy networks and strike at supply chains, the relevant provision could enable distributors to shift liability for copyright infringement onto their suppliers and thereby continue to sell illegal AV products with impunity.

While the supervision of authentication labels has been tightened, the Measure also relieves the MOC of its duty to authenticate AV products. The Measure provides that the MOC "may" (but does not have to) accept applications for authentication from copyright owners. This could potentially lead to delays during enforcement action as there may be no effective support from the MOC.

Benjamin Qiu (Solicitor), Lovells, Beijing, benjamin.qiu@lovells.com; and **Lester Pei** (Solicitor), Lovells, Beijing, lester.pei@lovells.com.

2.2. Beijing court issues decision on peer-to-peer file-sharing technology

On 19 December 2006, Beijing No. 2 Intermediate People's Court issued its decision on China's first copyright infringement case relating to peer-to-peer (P2P) file-sharing technology. The Defendant (a network service provider) was ordered to cease the infringement and pay RMB 200,000 in damages to the plaintiff.

The Plaintiff was the copyright owner of a large number of music files. The Plaintiff discovered that the Defendant was providing services to subscribers, which included searching for, sharing, and downloading musical works in which the Plaintiff has copyright, via the Defendant's P2P software and

network. Accordingly, the Plaintiff instituted legal proceedings against the Defendant for copyright infringement.

The Court found that the Defendant should have known that the musical recordings in question were protected by copyright and should not have been uploaded without the Plaintiff's consent. Based on this knowledge which the Defendant ought to have had, the Defendant failed to take steps to prevent users using its software to upload the musical recordings in question. The Court was basically placed an affirmative duty on service providers to prevent copyright infringement when they provide P2P file-sharing technology.

The Court also held that the Defendant had contributed to copyright infringement for the following reasons: the Defendant's P2P software only permitted the transmission of digital music files; the Defendant's website provided a multi-layer and systematic classification of music files, various ways to search for and download music files, music sampling, disc recording, and disc burning; the Defendant advertised its music downloading services to attract customers; and the Defendant derived its income from registration fees.

Benjamin Qiu (Solicitor), Lovells, Beijing, benjamin.qiu@lovells.com.

2.3. Chinese court rejects infringement claim brought by seven leading record labels

The International Federation of the Phonographic Industry ("IFPI") sued Baidu.com for copyright infringement on behalf of seven leading record labels including EMI, Universal, Warner, Sony and BMG. The claim stemmed from Baidu's MP3 file search service. On 17 November 2006, Beijing No. 1 Intermediate People's Court cleared Baidu.com of liability for copyright infringement.

The Court held that search engines help Internet users quickly locate information. Baidu had no intention to infringe copyright when it provided a service to search for MP3 files and measures for dealing with the alleged copyright infringement. The Court held that there were no legal grounds to impose liability on an online search service provider based on search results beyond its control or prediction. In addition, where an information network transmission right is infringed, the relevant right holder must, as a first step, present a notice to the Internet service provider, identifying the URL of the infringing website(s) and request that the website(s) be taken down. The Plaintiff, however, failed to give the Defendant this notice prior to the lawsuit.

Lester Pei (Solicitor), Lovells, Beijing, lester.pei@lovells.com; and **Stacy Yuan** (Trainee), Lovells, Beijing, stacy.yuan@lovells.com.

2.4. The state administration of radio, film and television promulgates industrial standard for mobile phone television

On 24th October 2006, the State Administration of Radio, Film and Television (SARFT) announced the industrial standard in China for mobile multimedia broadcasting ("mobile phone television"), namely, STiMi, a mobile phone television standard independently developed in China. The standard was adopted on 1 November 2006.

The standard, named GY/T220.1-2006, was issued by SARFT's Academy of Broadcasting Planning, and has been granted independent intellectual property rights.

Statistics show that China has over 500,000 mobile phone television users at present. It has been predicted that in the next 5 years, the Compound Annual Growth Rate for mobile phone television users in China will exceed 315%. Thus, by 2008, the number of mobile phone television users will reach 52.2 million, with a market value of up to RMB 1.3 billion. By 2010, there will be 97.5 million mobile phone television users, with a market value of up to RMB 2.4 billion.

According to Gartner Shanghai, China Mobile, China Netcom and other domestic telecommunication operators will benefit from reduced intellectual property royalties under this standard. Moreover, industry professionals believe that the establishment and implementation of STiMi will contribute to and form the basis for the large scale entry of mobile phone television into the Chinese market. By taking advantage of this opportunity, China can accelerate the convergence of the telecommunications, Internet, and cable television industries.

According to the PRC Standards Law, national and industrial standards are classified into compulsory standards and recommended standards. STiMi is a recommended industrial standard and therefore it may be enforced by administrative authorities which oversee industrial rules. However, the standard will not be legally enforceable.

The Ministry of Information Industry has not indicated whether the STiMi standard is the sole standard permitted for use in China. At present, STiMi is not the technology standard used by all mobile phone television operators. Nearly 40 institutions and enterprises in the broadcasting, television, and telecommunication fields (including China Mobile and China Unicom) have participated in the development of other mobile phone television standards. It is still questionable whether the STiMi standard can obtain enough support, both from the technology and consumer market sectors.

Lester Pei (Solicitor), Lovells, Beijing, lester.pei@lovells.com.

2.5. Domain name notices – a scam!

Brand owners from all over the world, and in particular those having a business presence in the PRC, are being inundated with notices from 'accredited PRC based domain name registrars' urging them to register certain <.cn> domain names and/or Internet keywords to prevent the 'imminent' registration of their key brands as domain names and Internet keywords by identified third parties.

Under pressure to meet sales quotas issued by the China Internet Network Information Center ("CNNIC"), it has become commonplace for domain name registrars accredited by CNNIC to approach brand owners directly to invite them to register domain names reflecting their brands cloaked under the guise of wanting to protect the brand owner's interests against the ever increasing number of domain name and brand hijackers in the PRC by allowing brand owners the right to 'get in first'.

These notifications follow the same basic formula:

- (i) the sender identifies him or herself as an accredited CNNIC domain name registrar;
- (ii) the sender identifies a third party which is claimed to have applied for the registration of domain names and/or Internet keywords incorporating the recipient's brands;
- (iii) the sender issues a gentle warning that it will allow the domain name and/or Internet keyword applications to progress to registration if the recipient does not itself apply to register them.

More often than not the third party identified in the notification in fact does not exist and the domain names and/or Internet keywords claimed to be the subject of a hijack turn out to be already registered (usually by the recipient of the notifications), placed on the registrar's domain name 'reserved list', or simply remain available notwithstanding the notification.

This is not to say that in all cases there will be no objective merit in registering <.cn> domain names identified in notices. There are obvious commercial benefits in registering domain names which reflect a brand owner's major brands. In addition to providing links to a brand owner's website, the registration of domain names is also an important way to protect brands against hijacking and infringement by third parties. If a decision is made to register a domain name identified in a notice, then a different and more reputable CNNIC accredited registrar should be used.

Sarah Doyle (Australian qualified lawyer), Lovells, Hong Kong, sarah.doyle@lovells.com; and Gabriela Kennedy (Partner), Lovells, Hong Kong, gabriela.kennedy@lovells.com.

3. Taiwan

3.1. First criminal convictions for browser hijacking

The Taipei District Court issued a landmark ruling on 12 September 2006. The Court ruled the first convictions under Articles 359 and 360 of Criminal Code. These two Articles fall within Chapter 36 – Offences Relating to the Use of Computers. Chapter 36 had been added to the Criminal Code in June 2003 but there had been no convictions under the two Articles until this past year.

The defendants had been charged with the "unauthorized acquisition, deletion, or alteration of the electromagnetic records of another's computer or related equipment resulting in damage to the public interest or the interest of an individual" (Article 359) and with the "unauthorized use of a computer program or other electromagnetic means to interfere with another's computer or related equipment thereby resulting in losses to either the public interest or the interest of an individual" (Article 360).

The Court found that the two defendants, Defendant A and Defendant B, worked for a company that provided online chat services to its users. Defendant A served as the company's Responsible Person. He instructed Defendant B, the company's IT manager, to develop a software program that would hijack users' browsers and redirect them back to the company's website when users attempted to visit a predefined list of websites offering competing or similar services. The Company placed

the software on its site as a free download for visitors disguising the Malware within an Internet content filter.

The Court ruled that the Defendants had redirected users back to their site through the unauthorized alteration of users' computers through a computer program and that the alteration had been made without due cause. The Defendants had argued that the software's primary intent had been to filter Internet content containing pornography, advertising, and counterfeit/infringing content. They had argued that users had voluntarily installed the software after the Company had disclosed the 'secondary' function to the users and that the Company had provided users with software to uninstall the program. The Court found, however, that while the Defendants had disclosed to users that the software would hijack browsers and had provided software to uninstall the program, the Defendants did not do so until after the authorities had questioned them as part of the criminal investigation into the software. The uninstaller also did not lend itself to the easy removal of the Malware. The Court found that the main purpose of the software had been to increase traffic to its website and to prevent users from accessing websites providing similar content and services. This purpose had not been disclosed to users when the software had been first posted to the Company's website.

Offences under Articles 359 and 360 require that the Court find that damages occurred as a result of the Defendants' actions in order for an offence to have taken place. The concept of damages under the Criminal Code is capable of a broad interpretation. The Court found that the Malware had interfered with users' ability to freely access and connect to Internet content. This interference constituted an injury both to the public interest and to the interests of individual users. The Court also concluded that at least one user had suffered further injury by the fact that the user had to reinstall the computer's operating system to effectively remove the program.

The Defendants faced a maximum sentence of five years' imprisonment and/or a fine of up to approximately US\$6000 under Article 359 and three years' imprisonment and/or a fine of up to approximately US\$3000 under Article 360. The Court sentenced each Defendant to five months' imprisonment or a fine of approximately US\$4000 in lieu of serving the sentence.

The decision marks the first convictions under Articles 359 and 360 and, significantly, the Court chose to adopt a broad interpretation of damage when assessing the elements of the offences.

Marcus S. Clinch (lawyer), *Winkler Partners, Taiwan*, mclinch@winklerpartners.com; and **Chih Shan Lee** (lawyer), *Winkler Partners, Taiwan*, cleo@winklerpartners.com.

3.2. *Taiwanese courts divided on legality of file-sharing business*

Kuro and ezPeer, once popular Taiwanese peer-to-peer (P2P) fee-based services with combined memberships of over 700,000, were the subjects of landmark criminal copyright infringement cases in 2005. In the first of the two cases, the court found ezPeer not guilty of criminal copyright infringement. Two months later, however, a separate court found Kuro guilty on similar charges. Both decisions were appealed.

The International Federation of the Phonographic Industry (IFPI), which initiated the legal action against Kuro and ezPeer in 2002, welcomed the Kuro conviction. The courts in both cases made it clear that unauthorized downloading of copyrighted material from sites like Kuro and ezPeer violated Taiwan's Copyright Act. The conflicting outcomes, however, led to a degree of ambiguity on the legality of P2P services in Taiwan and gave rights owner cause for concern.

Kuro and ezPeer continued to operate their sites unchanged while appeals were before the courts. Both companies, however, recently reached separate settlements with the IFPI and media groups. The settlement agreements saw Kuro and ezPeer shut down their previous P2P operations and switch to the licensed distribution of copyrighted material on new platforms.

The court in the ezPeer case found P2P technology in essence neutral and that ezPeer itself did not transmit or reproduce copyrighted files. The court concluded that while ezPeer might be aware that its users would share copyrighted material, the company could not be held criminally liable for direct copyright infringement as it failed to meet the "joint-offender" test under Taiwan's Criminal Code.

The court in the Kuro decision took a slightly broader view of joint offences. The court found Kuro guilty of contributory infringement on the basis that Kuro encouraged users to commit criminal acts. This was, however, supported by the fact that Kuro advertised the large volume of music available for sharing on its site. The court also found Kuro guilty of vicarious infringement as the company did not employ filtering technology to prevent illegal copying. The ezPeer court addressed this latter issue but questioned the effectiveness of existing filtering technologies to police P2P technology and whether the company had any legal obligation to employ such technology.

Kuro was found guilty of criminal copyright infringement and was fined approximately US\$90,000. Three Kuro executives were sentenced to prison terms up to three years and a fine of approximately US\$90,000 each. The judge also found one Kuro user guilty of infringement but issued a shorter sentence commutable to a fine. The Kuro case was the first criminal conviction in a P2P case.

The courts in both cases also considered whether either platform had substantive non-infringing uses that could to some degree offset their infringing uses. The court found that the ezPeer service offered redeeming uses. The Kuro court, in clear reference to the *Grokster* decision by the US Supreme Court, took the position that Kuro's non-infringing uses did not mitigate its infringing ones. The court found that Kuro's entire business model had been based on encouraging the illegal copying of copyrighted materials by its users.

The ezPeer decision alarmed rights holders and prompted the Taiwan Intellectual Property Office to undertake damage control. Taiwan's commitment to the protection of intellectual property rights was reasserted and the public was warned over unauthorized sharing of copyrighted materials online. The court in the ezPeer decision, however, lacked significant precedent to address the issues presented by P2P.

Taiwan is a civil law jurisdiction. Judges must clearly establish grounds under the laws of Taiwan to support the application of imported legal principles such as contributory and

vicarious infringement. The court found the grounds lacking in the ezPeer case and there was little outside precedent at the time within the context of P2P to consider when seeking those grounds. The courts are also generally adverse to broadly interpret the law to allow the imposition of criminal sanctions for the protection of purely commercial interests – the prevailing opinion is that the civil courts should be used in such cases. The court in the Kuro case, however, had the benefit of the Grokster decision from the United States and also considered the Kazaa decision from Australia and the Soribada settlement from Korea.

The IFPI and ezPeer reached a settlement in late June 2006. ezPeer shut down its unauthorized file-sharing site and services and agreed to pay the IFPI an undisclosed monthly royalty to provide copyrighted material legally on a new site under the name of ezPeer+. The new platform employs digital rights management technology to prevent unlicensed sharing. The IFPI took a harder line with Kuro. In September 2006, Kuro agreed to close its unauthorized operation within one month and pay IFPI damages of over US\$11 million. It should be noted that both Taiwanese courts will render decisions on the appeals though settlements have been reached.

Following the court's decision, Kuro lobbied for an amendment to the Copyright Act which would permit the competent authority to determine the remuneration online music service providers should pay rights owners to distribute copyrighted material. The proposed bill has not made any headway and still awaits first reading.

The IFPI backed a separate bill that would make it a specific criminal offence to provide software or technology that facilitates the unauthorized public transmission or reproduction of copyrighted material online and then obtaining benefit from that. The amendment also provides that the use of advertisements or other inducements to induce the public to infringe through the use of software or technology would constitute sufficient intent under the law. Violator's of the proposed amendment would be subject to imprisonment of no more than two years, detention and/or a fine of up to approximately US\$15,000. The proposed bill has completed first reading and has been approved for inter-party negotiations.

Marcus S. Clinch (lawyer), Winkler Partners, Taiwan, mclinch@winklerpartners.com; and **Chih Shan Lee** (lawyer), Winkler Partners, Taiwan, clew@winklerpartners.com.

4. Australia

4.1. Do Not Call Register Regulations

Following the introduction of the *Do Not Call Register Act 2006* (Cth) (the Act) and the *Do Not Call Register (Consequential Amendments) Act 2006* (Cth) (together, the Legislation), the *Do Not Call Register Regulations 2006* (Cth) (the Regulations) have now been gazetted. The Legislation was discussed in the August 2006 edition of the *Privacy Update* available at www.bdw.com under Publications.

The Regulations provide some clarification to the Legislation, and will be of assistance to organisations which make telemarketing calls.

4.1.1. Background to the Legislation

The Legislation allows people to choose not to receive unsolicited telemarketing calls by registering their telephone number on a Do Not Call Register (the Register). A telemarketing call is essentially a voice telephone call where a purpose of that call is to offer to supply, or to promote or advertise, goods or services.

Once a number is registered, an organisation cannot make a telemarketing call to that number unless the call is a “designated telemarketing call” or an exception applies. “Designated telemarketing calls” are calls made by exempt bodies such as charities, registered political parties and religious organisations, while exceptions to the prohibition include where there is consent to the call by the account-holder of a registered telephone number or their nominee.

4.1.2. Concerns about the Legislation

The Regulations cover two key areas of concern arising out of the Legislation:

- (a) that certain calls of a primarily “non-commercial” purpose may come within the scope of the telemarketing prohibition; and
- (b) that the telemarketing prohibition may frustrate the ability of business to call individuals who are not the account-holder of a telephone number or their nominee appointed in writing (which will be the case in many households).

4.1.3. The regulations

Regulation 4 addresses the first concern by clarifying the definition of a telemarketing call. It specifies that certain “customer service” calls are not telemarketing calls, even where such calls may also involve an organisation giving a consumer information about related goods and services of the organisation. These calls include calls relating to product recalls, fault rectification, appointment rescheduling, appointment reminders, payments for goods and services, other solicited calls and include calls not answered by the person to whom such calls are made.

In relation to the second concern, under section 39 of the Act, a “nominee” is a person who has been nominated in writing by a telephone account-holder whose number is included in the Register. Nominees, along with account-holders, can consent to telemarketing calls even if the account-holder's number is included in the Register. However, many individuals using telephone numbers will not be the account-holder or a nominee. Regulation 5 addresses this concern by deeming that persons who have provided a telephone number to an individual or organisation in certain circumstances are a nominee for the purposes of providing consent to telemarketing calls from that individual or organisation.

4.1.4. What is the result?

The result of the Regulations is twofold.

First, organisations will be able to give consumers information about related goods and services when that information is requested as part of a customer service call or a call that a consumer has requested. The Regulations make clear that calls of a primarily non-commercial purpose do not come

within the scope of telemarketing calls and therefore need not comply with rules relating to such calls. An important result of the Regulations is that restrictions on calling hours will not apply to these calls, meaning that they can be made outside of permitted calling hours.

Second, the Regulations alter the circumstances in which a person will be a nominee of a telephone account-holder and thereby entitled to consent to the making of telemarketing calls to a number which has been listed on the Register. Under the Regulations, a person will be deemed to be a nominee where that person, or another person acting on their behalf, has given the number to a person or organisation for the purpose of being contacted. The result is that telemarketing calls can be made to a person who has provided their number for that purpose.

4.1.5. Implementation

The Regulations relating to nominees will commence on the same day as Part 2 of the Act (which sets out the rules relating to telemarketing calls), which will come into effect next year, on a date to be proclaimed, and by 1 July 2007 at the latest. The remainder of the Regulations commenced in December 2006.

Tim Brookes (Partner), Blake Dawson Waldron, Sydney, tim.brookes@bdw.com; **Marlia Saunders** (Lawyer), Blake Dawson Waldron, Sydney, marlia.saunders@bdw.com; and **Leah Jessup** (Summer) Clerk, Blake Dawson Waldron, Sydney

5. New Zealand

5.1. Telecommunications Amendment Bill 2006

The Telecommunications Amendment Bill 2006 (Bill) has been introduced as one of the Government's measures aimed at improving the performance of New Zealand's telecommunications sector.

Two key features of the Bill are:

- Introduction of local loop unbundling, which requires Telecom (New Zealand's incumbent telecommunications network owner and service provider) to provide other telecommunication service providers with greater access to the line running from end users' premises to Telecom's nearest local exchange.
- Amendments to certain regulated services including the Unbundled Bistream Service, being a wholesale service that provides access seekers with increased access to the high frequency spectrum of the local loop.

The Bill will remove the current restriction on access seekers from applying for determinations in relation to a regulated service if they already have a commercial arrangement for the supply of that service. The Bill also expands the current powers of the Commerce Commission (Commission) by:

- Enabling the Commission to set access terms and conditions for regulated services for multiple access seekers under a standard terms determination process as well as accepting

binding commitments from access providers to supply a potential regulated service as an alternative to regulation.

- Empowering the Commission to continuously monitor the performance and development of the telecommunications sector and/or specific telecommunications markets.
- Enabling the Commission to take direct enforcement action and providing the Commission with a wider range of enforcement tools.

Karen Ngan (Partner), Simpson Grierson, Auckland, New Zealand, karen.ngan@simpsongrierson.com; and **Marc Cropper** (Senior Associate), Simpson Grierson, Auckland, New Zealand, marc.cropper@simpsongrierson.com.

5.2. Gaining wrongful access to another's e-mail account is an offence

The offence of wrongfully accessing another person's e-mail account for the purposes of obtaining a benefit is not confined to where the offender obtains a financial or pecuniary benefit

In a recent High Court case, the judge found that the respondent committed a breach of section 249(1)(a) of the New Zealand Crimes Act 1961 (Act) when he accessed the victim's e-mail account without a claim of right.

Under section 249(1)(a) of the Act:

Everyone is liable to imprisonment for a term not exceeding 7 years who ... accesses any computer system and thereby, dishonestly or by deception, and without claim of right, obtains any property, privilege, service, pecuniary advantage, benefit, or valuable consideration.

The issue was whether the word 'benefit' in section 249(1) of the Act is confined to a benefit of a financial or pecuniary nature. The High Court found that, as the term is not qualified by any adjective description, it would include non-monetary benefits such as acquiring knowledge or information to which one is not otherwise entitled or that could be used to exploit another person, or wrongfully accessing the e-mail communications of another for the advantage of disclosure.

The Court also held that whether something is a 'benefit' is a question of fact to be determined, objectively, in the circumstances. The judge noted that, although a benefit requires the person to have used the information or material for his or her own end, there need not be any corresponding loss or injury to another person. The Court concluded that the purpose of the inclusion of the crime described in section 249(1)(a) is to prohibit the dishonest access of any computer system where such access provides advantages to the person wrongly accessing the system, which might benefit that person in a variety of ways, pecuniary and otherwise.

Karen Ngan (Partner), Simpson Grierson, Auckland, New Zealand, karen.ngan@simpsongrierson.com; and **Marc Cropper** (Senior Associate), Simpson Grierson, Auckland, New Zealand, marc.cropper@simpsongrierson.com.

6. Singapore

6.1. System infringes software patent by performing same essential function

The Singapore High Court has recently issued its first judgment in respect of infringement of a software patent.

The plaintiffs had filed Singapore Patent No. 86037 (W/O 01/04846) in respect of a Dynamic Currency Conversion For Card Payment Systems, with the principal claim being a data processing method for determining a preferred currency for association with a charge, debit or credit card transaction between a merchant and the cardholder, "comprising the steps of obtaining the card number of the card from the cardholder ... [and further] identifying an identifier code from the said card number, determining the operating currency for said identifier code, by comparing said identifier code with entries in a table, wherein each entry in the table contains an issuer code or range of issuer codes and a corresponding currency code, and setting the currency for association with the card transaction as the determined operating currency for the issuer code."

The plaintiffs commenced an action against the defendant bank alleging that its dynamic currency conversion payment services offered to its customers, which was based on software supplied by the second defendants, FCC, infringed the subject patent.

The defendants challenged the validity of the plaintiff's patent for lacking novelty and an inventive step. The Singapore High Court adopted the approach in the UK case of *Kavanagh Balloons Pty. Ltd. v. Cameron Balloons Ltd.* [2004] RPC 5 requiring clear and satisfactory evidence in assessing the

probative value of evidence of prior user, and found the plaintiff's system to be novel. On the issue of inventive step, the Court held that the solution of automatic currency recognition was not something that could be easily picked up from the alleged prior art or common general knowledge.

The Court also found FCC's system to be infringing because it performed the same essential function as the plaintiff's. It was immaterial that the FCC system used slightly different currency detection sequences or had an additional feature. In any case, the plaintiff's patent allowed currency detection to be implemented at different stages of the transaction.

The first defendant also failed in its defence of innocent infringement because it continued to use the FCC system after it was aware of the plaintiff's invention, relying on the second defendant's assurance and indemnity. The Court distinguished between an infringer who believed that a patent could be challenged and one who did not know about the patent, and found the first defendant to be liable.

This decision is significant as Singapore's first successful software patent infringement claim, and highlights the risks facing software developers developing IT solutions implementing functionality over which patent protection has been secured.

Main-Line Corporate Holdings Limited v. United Overseas Bank Limited and First Currency Choice Pte Ltd (First Currency Choice Pte Ltd, Third Party) [2006] SGHC 233.

Lam Chung Nian (Partner), Lee & Lee, Singapore, lamchungnian@leenlee.com.sg; and **Loraine S. Muthiah** (Trainee), Lee & Lee, Singapore.