Conquering Spam in Concert: Anti-Spam Legislative Efforts in the Asia Pacific Region

Natasha Herbert, Mallesons Stephen Jaques

Natasha Herbert is a solicitor at Mallesons Stephen Jaques in Sydney, specialising in intellectual property and information technology law.

There is little doubt that the enactment of anti-spam legislation, as an isolated measure, is not capable of addressing the scourge of spam. But coupled with technical, educational and industry-led initiatives, anti-spam legislation plays an important role in defining prohibited conduct and establishing norms that denounce spamming.

In the last nine months, legislators around the Asia Pacific region have been deliberating over what form anti-spam legislation should take. Detailed legislative proposals have been promulgated and made available for public comment in Hong Kong and Singapore, while New Zealand's Unsolicited Electronic Messages Bill is under review by a Select Committee. And in Australia, the Department of Communications, Information Technology and the Arts is currently reviewing the three year operation of the Australian anti-spam legislation.

This article summarises the key features of the proposed anti-spam regimes in Hong Kong, New Zealand and Singapore, as well as that enacted in Australia. It then considers the importance of harmonising these legislative efforts if anti-spam legislation is to fulfil the important role afforded to it in any multi-faceted approach to overcoming spam.

Hong Kong – Unsolicited Electronic Messages Bill

The Commerce, Industry and Technology Bureau released detailed proposals for Hong Kong's Unsolicited Electronic Messages Bill ("HK UEM Bill") in January 2006.[1] The HK UEM Bill proposes an 'opt-out' regime of broad application to all forms of electronic communication except for person-to-person voice and video calls. The proposed extra-territorial reach of the HK UEM Bill is also expansive: a commercial electronic message will fall within the proposed Hong Kong regime if it has a nexus with Hong Kong, including where a message is merely transmitted through Hong Kong to another jurisdiction.

The HK UEM Bill's basic rules about sending commercial electronic messages mandate that all commercial electronic messages contain an unsubscribe facility, unless that requirement is inconsistent with a private arrangement between the sender and the recipient. And in a proposal that appears to be without precedent in the Asia Pacific region, the HK UEM Bill obliges senders to retain unsubscribe messages for at least 7 years after receipt.

Senders must refrain from sending commercial electronic messages to persons who have submitted an unsubscribe request in accordance with the HK UEM Bill, as well as those listed on 'do-not-call' registers established by Hong Kong's Telecommunications Authority. At this stage, the Hong Kong Government envisages that the Telecommunications Authority will establish "do-not-call" registers for opting out of promotional (i) pre-recorded voice, sound, video or image-based messages, (ii) SMS/MMS messages and (iii) fax messages.

The HK UEM Bill also proposes to enact a range of offences that apply to address harvesting, dictionary attacks and the transmission of multiple commercial electronic messages in connection with fraud-related activities. These latter offences are analogous to those prohibitions enacted by section 4(a) of the United States' CAN-SPAM Act of 2003.

The proposed enforcement regime for Hong Kong's anti-spam regime is government-led and graduated to reflect the gravity of the harm caused by specific types of contravention. For contraventions of the HK UEM Bill's basic rules about sending commercial electronic messages, the Telecommunications Authority is empowered to issue enforcement notices. An enforcement notice specifies the necessary steps to remedy the alleged contravention; failure to comply with an enforcement notice is an offence punishable by a fine of up to HKD$100,000 (approximately AUD$17,000), unless the person charged can prove that he or she exercised all due diligence to comply with the relevant enforcement notice. The address harvesting and dictionary attack offences proposed in the HK UEM Bill are punishable by fines of up to HKD$1,000,000 (approximately AUD$170,000) and imprisonment for up to 5 years, while the most serious fraud-related offences in the HK UEM Bill can attract uncapped fines and imprisonment for up to 10 years.

Finally, the HK UEM Bill contemplates a broad private right for persons who sustain pecuniary loss as a result of another's contravention of the HK UEM Bill.

New Zealand – Unsolicited Electronic Messages Bill

New Zealand's Unsolicited Electronic Messages Bill ("NZ UEM Bill")[2] proposes an anti-spam regime that adopts an 'opt-in' approach in respect of unsolicited commercial electronic messages, and an 'opt-out' approach in respect of unsolicited promotional electronic messages – non-commercial electronic messages that promote or market an organisation or its aims or ideals. This separate regulation of non-commercial electronic messages appears to be unprecedented in the Asia Pacific region.

The NZ UEM Bill has the same jurisdictional reach as the Australian legislation and does not apply to voice calls or faxes. An important aspect of the Bill's definition of 'commercial electronic message' is that it excludes a specified list of transactional or relationship messages sent in furtherance of a pre-existing business relationship. In this respect, the NZ UEM Bill is similar the United States' CAN-SPAM Act of 2003.

Overall, the 'opt-in' regime proposed by the New Zealand Government for the regulation of unsolicited commercial electronic messages is comparable to that enacted in Australia. To avoid the prohibition on sending unsolicited commercial electronic messages, senders must be able to demonstrate that they obtained a recipient's express, inferred or deemed consent to the receipt of a commercial electronic message. Furthermore, all commercial electronic messages must contain a functional unsubscribe facility and accurate sender information.

To implement the 'opt-out' regime for unsolicited promotional electronic messages, the NZ UEM Bill provides that promotional electronic messages must not be sent to a recipient who opts out of receipt of the same. Like commercial electronic messages, promotional messages must contain a functional unsubscribe facility and accurate sender information.

The NZ UEM Bill also prohibits the supply, acquisition and use of address-harvesting software and harvested-address lists to send unsolicited commercial electronic messages and promotional electronic messages in contravention of the NZ UEM Bill.

The enforcement regime contemplated by the NZ UEM Bill contemplates a significant role for ISPs. Persons affected by contraventions of the NZ UEM Bill's key prohibitions can complain to their ISP or seek an injunction from the High Court. ISPs are obliged to consider any complaints made to them and can refer these on to the enforcement department, which is likely to be New Zealand's Department of Internal Affairs.

The enforcement department is only obliged to consider complaints that it receives from ISPs, although it is empowered to take enforcement action of its own initiative. As with the Australian regime, the enforcement department can respond to contraventions of the NZ UEM Bill in a number of ways, including by issuing formal warnings and contravention notices, seeking enforceable undertakings or bringing proceedings in the High Court. The pecuniary penalties recoverable by the enforcement department in the High Court are capped at NZD$200,000 (approximately AUD$167,000) where the perpetrator is an individual, or NZD$500,000 (approximately AUD$419,000) in the case of an organisation. Contraventions of the proposed 'opt-out' regime for promotional electronic messages attract the lesser penalty of NZD$50,000 (approximately AUD$42,000) irrespective of whether the perpetrator is an individual or an organisation.

Finally, the NZ UEM Bill contemplates a broad private right of action for persons who sustain direct or consequential loss or damage as a result of another's contravention of the NZ UEM Bill.

Singapore – Spam Control Bill

In September 2005, the Infocomm Development Authority and the Attorney-General's Chambers released the proposed Spam Control Bill.[3] The Spam Control Bill contemplates an 'opt-out' regime that applies to 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, voice telephone calls or instant messaging tools do not. Singapore's proposed bulk transmission requirement is the same as that enacted in the United States, and the concept of a 'Singapore link' is taken from the Australian legislation.

The key prohibitions in the Spam Control Bill are against:

1. sending unsolicited commercial electronic messages in bulk without a functional unsubscribe facility;
2. sending unsolicited commercial electronic messages in bulk other than in accordance with the Spam Control Bill's transparency requirements; and
3. sending an electronic message (whether solicited or unsolicited) to an electronic address through use of a dictionary attack or address harvesting software.

The Spam Control Bill's transparency requirements include the usual prohibitions on sending an unsolicited commercial electronic message with false or misleading header information, or with a misleading subject title. In addition, the Spam Control Bill mandates that all unsolicited commercial electronic messages contain the letters '<ADV>' in the subject line. This labelling requirement is not a feature of the regimes proposed in Hong Kong and New Zealand, or that enacted in Australia.

The Spam Control Bill does not contemplate enforcement by a government agency; enforcement of the Spam Control Bill is at the suit of those that suffer loss or damage as a result of unlawful spam activity. When pursued, spammers can be liable to either ordinary civil damages or statutory damages of up to SGD$25 (approximately AUD$21) per contravention (capped at SGD$1 million [approximately AUD$836,000] in the ordinary case).

Australia - Spam Act 2003

Australia's federal Spam Act 2003 ("Spam Act")[4] establishes an 'opt-in' regime in respect of unsolicited commercial electronic messages that have an 'Australian link', that is, messages that originate from, or are accessed in, Australia. The Spam Act regulates all manner of commercial messages, apart from spam faxes.[5] To avoid contravening the Spam Act, senders of commercial electronic messages must (i) obtain a 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. In some limited circumstances, a recipient's consent to the receipt of

certain messages is deemed from the conspicuous publication of their electronic address(es). Consent offered under the Spam Act can also 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 that sender, then consent will be taken to have been withdrawn within 5 business days of receipt of the 'opt-out' request.

In the recent case of *Australian Communications and Media Authority v Clarity1 Pty Limited*[6] - the first case under the Spam Act - the Federal Court of Australia took a pragmatic approach to the Spam Act's consent provisions. The Court held that the Spam Act requirement to include a functional unsubscribe facility in all commercial electronic messages is directed at senders, and that requirement cannot ordinarily be relied upon to argue that a recipient's failure to use an unsubscribe facility implies that the recipient has consented to the receipt of future commercial electronic messages.[7] The Court also considered the nature of a 'business relationship' from which a recipient's consent may be inferred and held that, on the face of it, the conclusion of an email contract for the purchase of goods or services constitutes a 'business relationship' between the vendor and purchaser from which it is reasonable to infer the purchaser's consent to the receipt of future commercial electronic messages about the vendor's business, unless the vendor has received an indication to the contrary.[8] This decision is likely to be welcomed by persons regulated by the Spam Act for its commercially realistic approach to the way in which senders infer consent from their business dealings with recipients.

Returning to the key features of the Australian anti-spam regime, the Spam Act also prohibits the supply, acquisition or use of address-harvesting software or harvested-address lists to send commercial electronic messages in contravention of the Spam Act.

The Australian Communications and Media Authority ("ACMA") is the sole enforcer of the Spam Act. ACMA 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. In practice, one of ACMA's key enforcement powers is its ability to levy pecuniary penalties: for individuals, these fines can extend up to AUD$44,000 per day for a first contravention and up to AUD$220,000 for repeat contraventions; corporations can face up to AUD$220,000 per day for a first contravention and up to AUD$1.1 million per day for repeat contraventions.

Pursuant to the co-regulatory model contemplated by the federal Telecommunications Act 1997, ACMA registered the Australian eMarketing Code of Practice[9] in March 2005 and the Internet Industry Spam Code of Practice[10] in March 2006. These industry codes supplement the Spam Act regime by providing detailed guidance to those that interact closely with the spam problem: the eMarketing Code of Practice regulates the conduct of persons who send commercial electronic messages as part of their e-marketing activities, while the Internet Industry Spam Code of Practice considers how internet service providers and email service providers can address sources of spam within their own networks. Both of these codes are enforceable by the ACMA, and the Telecommunications Act penalties for breaching these codes are in addition to those remedies provided under the Spam Act.

The need for further harmonisation of anti-spam regimes in the Asia Pacific region

It is clear from the above discussion that although there are some common elements among the proposed and enacted anti-spam regimes in Australia, Hong Kong, New Zealand and Singapore, there are also significant areas of divergence. Consider, for example, the anomalies that would result if the proposed anti-spam regimes in Hong Kong, New Zealand and Singapore were enacted in their current form. In Australia and New Zealand, it would not be permissible for an e-marketer to send an unsolicited commercial electronic message, whereas e-marketers in Hong Kong and Singapore would be free to do so. A commercial email from an Australian company to a Singaporean-based customer would need to be labelled '<ADV>', but it would be unnecessary (and potentially damaging from a filtering perspective) for that same company to use '<ADV>' labelling when communicating with its Hong Kong and New Zealand-based customers. Finally, an ISP based in Hong Kong may suffer considerable loss from a barrage of spam originating in Australia, but since that ISP would not be entitled to pursue that spammer in Australia in its own right, the Hong Kong ISP would need to rely on complex reciprocal enforcement of judgment laws to have recourse against the spammer and his or her assets in Australia.

This lack of regional harmonisation is particularly troubling in the spam context. The borderless nature of electronic communications means that spam presents a cross-jurisdictional problem that cannot effectively be addressed by localised legislative efforts. Inconsistencies among the world's spam laws impose unnecessary compliance costs on multi-national businesses and cause frustration for customers who are left without redress in situations where overseas spammers prove to be beyond the reach of the arm of the law.

In their background paper for the 2005 ITU WSIS Thematic Meeting on Cybersecurity, Bambauer et al consider the possibility of developing a model spam law as a means of overcoming the disadvantages associated with inconsistent anti-spam regulation.[11] They conclude that "[a] model spam law is possible to develop, despite differences among the world's spam laws".[12] In reaching this conclusion, Bambauer et al analysed existing anti-spam laws to identify the areas in which those laws strongly converge and diverge. They found that enacted anti-spam laws strongly converge in the following areas:[13]

- a focus on commercial content;

- the mandatory disclosure of sender and transmission information;
- prohibitions on fraudulent or misleading content;
- prohibitions on address harvesting and dictionary attacks;
- the ability to contact a recipient where there is a pre-existing business relationship between the sender and the recipient;
- the requirement to include an opt-out mechanism; and
- a mix of graduated civil and criminal liability.

Not surprisingly, a prior consent requirement – or more colloquially, whether a particular regime is 'opt-in' or 'opt-out' – is at the top of the list of areas where enacted anti-spam laws diverge. Other areas of contention include enforcement responsibility, labelling requirements, the application of anti-spam laws to electronic communications generally (and not just e-mail) and the extra-territorial operation of anti-spam legislation.[14]

This analytical groundwork appears to be a useful first step toward harmonising proposed and enacted anti-spam laws. It provides a yardstick by which legislative efforts can be compared, and helps to focus legislators' attention on the more difficult aspects of anti-spam legislation.

Yet even with the benefit of analyses such as that prepared by Bambauer et al, there is no doubt that harmonisation of anti-spam laws – particularly those already enacted – will be a difficult task. Even among jurisdictions with a common legal heritage – as is the case with Australia, Hong Kong, New Zealand and Singapore – legislators struggle to find a coherent fit between anti-spam laws and existing regulation, and the economic imperatives informing their approach to electronic communications.

In the final analysis, harmonisation of anti-spam laws is not merely desirable, but essential to the effective regulation of the cross-jurisdictional problem that spam presents. Legislators in AustrFalia, Hong Kong, New Zealand and Singapore should be mindful of this as they make their contributions to the regulation of spam in the Asia Pacific region.

---

[1] Commerce, Industry and Technology Bureau, *Consultation Paper on Legislative Proposals to Contain the Problem of Unsolicited Electronic Messages* (January 2006) Available at: http://www.citb.gov.hk/ctb/eng/paper/pdf/UEM(Eng)-final.pdf (29 May 2006)

[2] Available at: http://www.knowledge-basket.co.nz/gpprint/docs/bills/20052811.txt (29 May 2006)

[3] Infocomm Development Authority of Singapore and the Attorney-General's Chambers of Singapore, *Proposed Spam Control Bill: Joint IDA-AGC Consultation Paper* (September 2005) Available at: http://www.ida.gov.sg/idaweb/pnr/infopage.jsp?infopagecategory=infoecon:pnr&versionid=1&infopageid=I2883 (29 May 2006)

[4] Available at: http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/current/bytitle/7C84FF3ED0D0FC13CA256FE70083B9A1?OpenDocument&mostrecent=1 (29 May 2006)

[5] *Spam Regulations 2004* (Cth) Available at: http://www.comlaw.gov.au/ComLaw/Legislation/LegislativeInstrumentCompilation1.nsf/0/ED5984D617843AB1CA256F7100590CEB/$file/2004No56.pdf (29 May 2006)

[6] *Australian Communications and Media Authority v Clarity1 Pty Limited* [2006] FCA 410 (13 April 2006) Available at: http://www.austlii.edu.au/au/cases/cth/federal_ct/2006/410.html (29 May 2006)

[7] Above note 6, paragraph 74.

[8] Above note 6, paragraph 97.

[9] Available at: http://www.acma.gov.au/ACMAINTER.65646:STANDARD:398315724:pc=PC_2887 (29 May 2006)

[10] Available at: http://www.acma.gov.au/acmainterwr/telcomm/industry_codes/codes/iia%20spam%20code%20dec%202005.pdf (29 May 2006)

[11] David E Bambauer, John G Palfrey Jr and David E Abrams "A Comparative Analysis of Spam Laws: The Quest for a Model Law" Background Paper for the ITU WSIS Thematic Meeting on Cybersecurity (Switzerland, 28 June - 1 July 2005) Available at: http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_of_Spam_Laws.pdf (29 May 2006)

[12] Above note 11, page v.

[13] Above note 11, pages 26 - 27.

[14] Above note 11, page 27.