MORRISON | FOERSTER

Legal Updates & News

Bulletins

The New Hong Kong Unsolicited Electronic Messages Ordinance

June 2007
by Jeffrey S. Huang, Gordon Milner

Privacy Update, June 20, 2007

PDF Version

On June 1, following almost two years of public consultations and legislative contemplation, Hong Kong's telecommunications industry regulator, the Office of the Telecommunications Authority (OFTA) brought into force the Unsolicited Electronic Messages Ordinance (the Ordinance). As its name implies, the Ordinance is aimed at addressing the ever increasing volume of unsolicited commercial messages received every day by e-mail accounts, phones and fax machines in Hong Kong.

Scope

The Ordinance seeks to regulate the sending of commercial electronic messages with a Hong Kong Link (CEMHKLs). This core concept has three distinct elements which must all be present in order for the Ordinance to apply:

- **There must be an ''electronic message.''** This is defined in a very broad, technology neutral manner as a message sent in any form to an electronic address via any public telecommunications service. An ''electronic address'' is also very widely defined and includes telephone numbers as well as e-mail addresses, etc. Thus an ''electronic message'' will include e-mails, faxes, text (SMS) and multimedia (MMS) cellular messages and also pre-recorded telephone messages.
- **The message must be for a commercial purpose and for the furtherance of a business.** This would include messages with a purpose of advertising, promoting, or offering any goods, services or business opportunities. The commercial purpose need not be the sole purpose of the message, but it must exist—a message about an amateur sports event with no commercial purpose would not be covered by the Ordinance.
- **There must be a ''Hong Kong Link.''** Broadly, this means that the message must either (a) originate or be received in Hong Kong; (b) be sent by a Hong Kong business or company; or (c) be sent to a Hong Kong assigned electronic address (such as a Hong Kong telephone number or .hk e-mail address).

Schedule 1 sets out certain forms of communication that are expressly excluded from the operation of the Ordinance. These include automated voice telephone enquiry systems, faxes-on-demand, television and sound broadcast services, and (perhaps most notably) non-recorded live person-to-person telephone calls—thus the Ordinance does not cover live telemarketing calls even if they are commercial in nature.

CEMHKLs that recipients have affirmatively requested or have otherwise consented to are also exempt from the Ordinance. In addition, the Ordinance includes an express presumption that telecommunications service providers (such as Internet service providers) are not senders of CEMHKLs where they are merely acting as carriers of such traffic. The Ordinance will be brought into effect in two distinct stages:

Phase I

Phase I came into force with immediate effect June 1. It is comprised of a number of key prohibitions, the contravention of which will constitute a direct criminal offense in Hong Kong, in most cases punishable by heavy fines and up to five to 10 years imprisonment:

Creation and Use of Botnets
The unauthorized accessing of telecoms devices or networks (commonly referred to as ‘‘zombie PCs’’ or ‘‘botnets’’) to send multiple CEMHKLs;

Falsifying Header Information
The material falsification of header information in multiple CEMHKLs in such a way as to obfuscate the identity of the sender;

Use of False Identities
Registering for electronic addresses or domain names that falsely represent the source of prohibited CEMHKLs, or falsely representing to be the registrant of an electronic address or domain name for the purposes of sending CEMHKLs.

Address Harvesting and Use
The supply, acquisition or use of software, the main purpose of which is electronic address collection, or the supply, acquisition or use of lists of electronic addresses generated by such software, in each case in connection with the sending of CEMHKLs;

Automated Generation of Electronic Addresses
Generating electronic addresses by automated processes to send CEMHKLs, or the use of scripts or other automated means to register for five or more e-mail addresses to send multiple CEMHKLs.

Misuse of Open Relays and Proxies
The use of any telecommunications device, service or network to relay or retransmit multiple CEMHKLs, with the intent to deceive or mislead recipients, or any telecommunications service provider, as to the sender.

Phase II

Phase II regulates the content and nature of CEMHKLs themselves and provides for the establishment of ‘‘do-not-call’’ registers in relation to certain classes of electronic addresses (notably this is likely to be limited to telephone and fax numbers).

The commencement date for Phase II has yet to be determined, in large part to provide businesses with an opportunity to adapt, and to provide the recipients of unsolicited messages time to join ‘‘do-not-call’’ registers. However, OFTA has indicated that it anticipates Phase II will become effective toward the end of 2007. Phase II sets out certain requirements for CEMHKLs:

Identification
Each CEMHKL must contain clear and accurate information identifying the sender which will be reasonably likely to be valid for 30 days;

Unsubscribe Mechanism
Each CEMHKL must contain a clear ‘‘unsubscribe’’ mechanism that complies with certain technical criteria and which will be reasonably likely to be valid for 30 days. Where a recipient sends an unsubscribe request to a sender of CEMHKL, the sender will have 10 working days to cease sending further CEMHKLs to the recipient in question;

Misleading Headings
CEMHKLs must not be sent with subject headings which would be likely to mislead the recipient about a material fact regarding the content or subject matter of the message; and

Blocked CLI
Telephone or fax CEMHKLs must not be sent with the calling line identification data (CLI) concealed.

In general, these requirements will not apply if the sender did not know, and could not with reasonable diligence have ascertained, that the message had a Hong Kong Link.

Phase II also provides for the establishment by OFTA of codes of practice in addition to the do-not-call register. CEMHKLs must not be sent to recipients listed in the do-not-call register (although a grace period of 10 working days is permitted for senders to update their databases).

Unlike the prohibitions in Phase I, the contravention of most of the requirements in Phase II will not automatically constitute a criminal offense, but may result in an enforcement notice from OFTA. Any further contravention of such a notice will be a criminal offense that may result in a fine of up to HK$100,000 ($12,806). It will also be a direct criminal offense to harvest electronic addresses from the do-not-call list or that are provided under unsubscribe notices.

Enforcement

OFTA is the threshold agency responsible for enforcing the Ordinance. The onus for identifying violations, however, effectively rests with the recipients of CEMHKLs. As an initial matter, recipients are encouraged to contact and request the sender to cease sending electronic messages to them, though senders are not obligated to honor such requests until Phase II becomes effective. Recipients are also encouraged to add their phone, fax and mobile telephone numbers to do-not-call registers.

OFTA has published a prescribed form for the submission of complaints regarding CEMHKLs. Such forms will be ''collated and analyzed'' to identify potential spammers. If such analysis identifies a Phase I violation, OFTA may refer the matter to the Hong Kong Police for further investigation and potential prosecution.

It should be noted that where a company has engaged in any conduct constituting an offense under the Ordinance, any director of that company who has responsibility for its internal management shall be presumed to have committed the offense in question unless he can prove that he did not authorize the acts in question.

In addition to criminal sanctions, the Ordinance provides a private right of action to recipients who have suffered loss or damage as a result of a violation of the Ordinance irrespective of whether the violator has been convicted for such violation.

Anticipated Effectiveness

It remains to be seen how effective the Ordinance will be at controlling unsolicited commercial electronic messages in Hong Kong. Although the Legislative Council expressed a hope that the new law would help reduce spam by up to 80 percent, the measures may be severely limited by territorial jurisdiction issues as the vast majority of such certain key categories of messages (such as e-mail) come from overseas.

However, there are sound reasons to believe that the Ordinance will have a substantial impact upon unsolicited SMS or MMS messages sent to mobile phones; as such messages commonly originate from within Hong Kong. At present, many who have received such messages while overseas have complained of hefty roaming charges and other fees from simply reviewing and deleting such messages. Because the senders of such messages are more readily identifiable, investigating and taking legal action against them ought to be relatively straightforward.

Conclusion

The Ordinance attempts to establish a comprehensive mechanism to regulate unsolicited commercial electronic messages in Hong Kong. Similar regimes have been implemented in jurisdictions around the world (most notably the U.S. CAN-SPAM Act). The limited success of such endeavors in reducing the sheer volume of spam is perhaps a testament to the substantial profits to be made from such activities and the ease with which those responsible can relocate their activities to less well regulated jurisdictions. Ultimately, time will tell whether a piecemeal patchwork of national legislation such as the Ordinance can be effective or whether a supra-national approach may be required.

Reproduced with permission from *Privacy & Security Law Report*, Vol. 6, No. 23, 06/04/2007, pp. 891-893.