INTERNATIONAL NEWSLETTER

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

# Comprehensive US federal privacy legislation: "This is the conversation we need to have"

**Eugene Oscapella** reports

Late to join the party, but enthusiastic once it did, Microsoft has added its voice to the call for comprehensive federal privacy legislation in the United States. And singing the same tune is Commissioner Pamela Jones Harbour of the US Federal Trade Commission.

Speaking at an IAPP conference held in early March in Washington, DC, Brad Smith, Senior Vice President and General Counsel at Microsoft, acknowledged that developing such legislation would be a complicated task, but that the time for action had arrived. Mr Smith's words were not random musings. He had already issued a "white paper" on behalf of Microsoft in November 2005, outlining the company's support for federal legislation. And, he noted, companies like Intel and HP had been calling for such legislation for some time.

The Microsoft white paper noted that much of the privacy regulation in the United States occurs at the state level, and that laws are inconsistent. A set of business practices that is legal and commonplace in one state may be prohibited just across the state line. In addition, said the paper, the number of state privacy laws is increasing quickly. Between January 2004 and November 2005, more than 20 states enacted financial privacy laws. At the same time, continued the paper, Congress has enacted federal privacy provisions in legislation specific to certain industries:

- The Gramm-Leach-Bliley Act for financial institutions;
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) for health care providers;
- The Cable Act for cable operators;
- The Communications Act for telecommunications carriers.

Added to this mix of laws, pointed out the white paper, are specific laws to address children's online privacy, spam, telemarketing and junk faxes. Concerns over spyware and identity theft are prompting a further array of federal legislative proposals.

Concludes the white paper, "this has led to an overlapping, inconsistent and incomplete patchwork of state and federal laws that creates compliance chaos for businesses and uncertainty for consumers." Mr Smith drew an analogy to the confusion over multiple mandatory nutritional labeling requirements in the United States that eventually led to a common labeling standard.

Mr Smith identified several reasons, beyond the inconsistencies caused by the patchwork of legislation, for moving to comprehensive federal data protection legislation:

- Consumer confidence about privacy on the Internet and privacy in general was declining. Some people were losing confidence in buying on the Internet. Mr Smith referred to the findings of a recent Consumers Union survey that 25 per cent of Internet users have stopped making

*Continued on p.3*

Issue 82 **May 2006**

## NEWS



## LEGISLATION & REGULATION



## MANAGEMENT & STRATEGY



## TECHNOLOGY

INTERNATIONAL newsletter

ISSUE NO 82 MAY 2006

**EDITORIAL DIRECTOR & PUBLISHER**
**Stewart H Dresner**
stewart@privacylaws.com

**EDITOR**
**Lucy Fisher**
lucy.fisher@privacylaws.com

**ASSOCIATE EDITOR**
**Laura Linkomies**
laura@privacylaws.com

**NEWSLETTER SUBSCRIPTIONS**
**Glenn Daif-Burns**
glenn@privacylaws.com

**ISSUE 82 CONTRIBUTORS**

**Alisa Bergman**
DLA Piper Rudnick Gray Cary US LLP

**Professor Graham Greenleaf**
Asia-Pacific Editor, Privacy Laws & Business

**James Michael**
Insitute of Advanced Legal Studies, London University

**Robin McLeish**
Barrister

**Eugene Oscapella**
Associate, Privacy Laws & Business

**Professor Whon-il Park**
Asst. Prof. of Law at Kyung Hee University, South Korea

**Dugie Standeford**
Freelance journalist

**PUBLISHED BY**
Privacy Laws & Business,
5th Floor, Raebarn House,
100 Northolt Road, Harrow, Middlesex,
HA2 0BX, United Kingdom
Tel: +44 (0)20 8423 1300,
Fax: +44 (0)20 8423 4536
Website: www.privacylaws.com
The *Privacy Laws & Business* International Newsletter is produced five times a year and is available on an annual subscription basis only. Subscription details are at the back of the newsletter. Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given. No part of this publication in whole or in part may be reproduced or transmitted in any form without the prior permission of the publishers.
Design by ProCreative +44 (0)20 8429 2400
Printed by Direct Image +44 (0)20 7336 7300
ISSN 0953-6795


# "comment"

## Legislation struggles to keep up

Privacy crises occur in all countries. Management must respond in the short term, while legislation, reflecting national culture, struggles to keep up.

South Africa has an eye on becoming a serious player in the global outsourcing market. Its proposed data protection bill incorporates certain specific features of Roman-Dutch and common law and would make its Information Commissioner responsible for both the Protection of Personal Information Act and the Promotion of Access to Information Act which directly affects companies (pp.16-17).

Singapore has decided to assess the efficacy of its existing laws covering aspects of privacy (p5). Singapore is at the centre of the 21 member APEC process, and is the only Asian country joining Australia, Canada and the USA in a study group on information sharing and cross-border cooperation.

Latin America is pulled in two directions, towards the APEC model, led by Chile, and towards the EU model, led by Argentina (pp.18-19). Culturally, Latin American countries differ from other regions with privacy associated with intimacy rights, the right to be left alone.

In the United States, partly stimulated by multiple and well publicised privacy breaches, the call for comprehensive federal privacy legislation grows louder with explicit support from a Federal Trade Commissioner, Pamela Jones Harbour and Brad Smith, Microsoft's General Counsel (pp.1-4 ).

Many of the headline-grabbing privacy incidents, occur online - as Hong Kong realised to its dismay when the personal data of an estimated 20,000 people were posted on the web. And as things stand, there are few remedies in the country's rather "toothless" privacy law (pp. 10-13).

EU Data Protection Commissioners express concerns about e-mail tracking (pp.21-22 ) and RFIDs (pp.26-27 ). And we continue with Portugal, in the next instalment in our series on employee monitoring (pp.25-26 ).

Google has won applause for taking a stand against the US government earlier this year, in defence of its customers' privacy rights (pp.8-9). Will other companies show the same concern? What steps will they take to avoid privacy crises? PL&B's 19th Annual International Conference in Cambridge July 3-5th provides the perfect opportunity to find out what leading companies and privacy regulators are doing. We hope that you will join us.

Lucy Fisher,
Editor
PRIVACY LAWS & BUSINESS

### Contribute to PL&B publications

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Stewart Dresner on Tel: +44 208 423 1300, or e-mail: stewart@privacylaws.com.

# South Korea fights spam with new laws

While South Korea legislators are tackling spam with a succession of legal amendments, they have not yet adopted a comprehensive privacy law. **Professor Whon-il Park** reports

It's like a war between a spear and a shield.

Recently Internet users in Korea have been perplexed to discover that the number of unsolicited e-mails is constantly on the increase. Mail server administrators are also complaining that new types of spam are too sophisticated to block. They say that more than 90 percent of incoming mail is spam.

Recently the Korean government declared an all-out war against spam by amending the Act on the Promotion of Information and Communications Network Utilization and Data Protection, etc. (the "Act", visit: www.worldlii.org/int/special/privacy/for reference).

Spammers never sleep, while lawmakers are involved in numerous political affairs other than preparing a comprehensive data protection act that public opinion is longing for in Korea. Government officials and specialists worry that Internet users' e-mail boxes are increasingly occupied by messages which are harmful to youngsters, and that spammers are extending their targets to include mobile phones.

As a result, lawmakers agreed to add strict anti-spam provisions to the existing act rather than discussing the proposed comprehensive acts on data protection, which seem to be full of controversies.

## Existing anti-spam regulations

So far, South Korea has implemented specific but not so effective anti-spam regulations. The current act enables Internet users to refuse unsolicited e-mails.

No one is allowed to send direct marketing (DM) mails for profit contrary to an addressee's explicit refusal. Spammers in violation of this prohibition can be fined up to 30 million won (equivalent to U$31,000). E-mail senders are required to indicate "AD" or "DM" in the e-mail's subject line. The content should include an explanation as to how to refuse the unsolicited message, the source where the e-mail address(es) were collected, and some useful information about the sender. Using technological means to avoid refusal or to register e-mail addresses for the purposes of DM automatically is also subject to a fine.

If a data subject suffers any damage as a result of the information service provider ("ISP") violating the data protection provisions, the data subject may claim for damages against the ISP. Claims for damages may be filed with the Personal Information Dispute Mediation Committee ("PIDMC") or with the court depending on the amount of damages.

## Further anti-spam amendments

During the last couple of years, there have been anti-spam amendments to the Act. The amendment in January 2004 called for ISPs to protect Internet users' personal information by preventing spammers from collecting, abusing or misusing such information:

**a.** When an ISP wants to obtain the consent of a user, it shall notify the user of the installation and operation of automatic data collection devices including Internet log-in data files, and it shall stipulate such matters in the general terms of a service contract.

**b.** The Minister of Information and Communication ("MIC") may develop and distribute the software to stop, and report to the authorities, the unsolicited commercial e-mails.

**c.** A user's right is confirmed with respect to the provision of his or her personal information. The MIC may implement mandatory data protection guidelines for the security measures of the information and communications network to enhance security. The MIC may establish some standards necessary for data protection.

**d.** In order to facilitate a dispute settlement, a 15-member PIDMC will put minor personal information disputes to a sub-panel composed of five or less Committee members.

**e.** ISPs shall not make an agreement in violation of data protection provisions.

**f.** Attempts at invasion without authorization or beyond the authorized capacity to access another's information and communications networks, for illegal purposes, is subject to imprisonment for up to three years or fines not exceeding 30 million won.

In December 2004, when some lawmakers were busy making proposals for comprehensive data protection, the National Assembly passed an amendment with its entry into force three months later. It purported to prevent illegal and harmful information in cyberspace and to minimize users' inconvenience by curtailing non-selective unsolicited messages.

**g.** The MIC is required to make a policy to develop and to distribute data protection technologies.

**h.** Anybody, and this includes - of course - ISPs, is strictly prohibited from transmitting or exhibiting media and contents which are harmful to minors. ISPs whose daily website viewers and average sales for the previous three months exceed a certain criteria, shall have an in-house guardian protecting minors from any harmful content and receiving complaints from youngsters in line with a self-regulatory framework.

**i.** Any transmission of commercial messages via telephone and facsimile without prior permission of the addressee is prohibited. However, only small businesses with home offices are allowed to transmit commercial messages, without prior permission, to the addressees with whom the senders have established a seller-customer relationship and have collected the addresses like telephone numbers by themselves.

**j.** Automatic extracting programs to collect e-mail addresses without prior permission from the Internet homepages

are prohibited to stop making an easy mailing list for spammers.

**k.** Nobody shall post any commercial message or advertisement on the Internet homepage contrary to the explicit "No Advertisement" policy of the homepage administrators. And the administrators may delete at any time such message or advertisement in breach of their policy.

### Recent anti-spam provisions

In December 2005, there was another important amendment to prevent Internet users from collecting other's personal data by "phishing" or other deceitful activities on the Internet. Any violator of such prohibition is subject to imprisonment of up to three years, or fines not exceeding thirty million won. Also spammers are punished with either imprisonment for one year or less, or a fine of up to ten million won.

The MIC has a legal basis to claim for the personal identification of spammers and to crack down on illegal spammers. ISPs have been granted a right to terminate services of spammers. In this regard, the MIC is required to notify in advance to ISPs the inspection date and plans before the enforcement of laws, in order to enhance the transparency and foreseeability of administrative inspection.

However, it remains to be seen whether this legal and administrative shield will defeat the sleepless spears.

**AUTHOR**

Professor Whon-il Park, Asst. Prof. of Law at Kyung Hee University, South Korea

# EU DP Commissioners condemn e-mail tracking

EU privacy commissioners warn that the tracking of e-mails without the recipients' knowledge is in breach of the EU Data Protection Directive. **Laura Linkomies** reports

The company behind *DidTheyReadIt* software proudly announces on their website that "When you use *DidTheyReadIt*, every e-mail that you send is invisibly tracked without alerting the recipient. But when they read your message, you will immediately receive the following information: when, exactly, your e-mail was opened, how long your email remained opened, and where, geographically, your e-mail was viewed."

The Florida-based software developer, Rampell software, is now at the centre of unwanted attention by the EU Data Protection Working Party, which identifies *DidTheyReadIt* as a privacy intrusive product in its recent opinion on the provision of e-mail screening services (see box on next page). The group says that this type of processing is secretly performed and in breach of the data protection principles requiring transparency in the collection of personal data. The privacy commissioners continue to say that unambiguous consent from the recipient of the e-mail is necessary.

As there are other similar products on the market, Rampell software feels that the group has taken an unfair aim at them.

Michael Hansen, Administrative Manager of Rampell Software, says: "Nearly every single commercial e-mail is tagged in a way to know if you received it using the exact same system as *DidTheyReadIt* uses. This is not a novel technology that we designed; it has always existed since the days that e-mail began. We just made it available to consumers."

But the tricky issue is that recipients are not aware that the e-mails are being tracked. E-mail programmes such as Netscape and Outlook Express also allow the sender to request a return receipt from the recipient. However, the recipient can choose not to reveal whether, and when they opened the e-mail.

A representative from the French Data Protection Commission, the CNIL, explained to PL&B: "When one changes the way a technology is used, in this case web bugs, the whole picture changes - and data protection rules lead to different conclusions. Technology as such is hardly ever illegal. What causes problems is the use organisations make of it. It is a clear fact that the very functioning of *DidTheyReadIt* runs against the principle of fair collection of data and does not provide for basic data protection rights."

Rampell software is of the view that the Working Party has not fully understood the technical issues at hand. The company states that it respects privacy, and that the product does not pose any privacy risks to individuals.

### How e-mails are tracked

The service Rampell software provides is not new - in fact, the software was launched in 2004. The service can be used in two ways, either by downloading a progamme called *DidTheyReadIt Background Tracker*, that automatically tracks all the e-mails that are sent, or by adding "didtheyreadit.com" to the end of the recipient's e-mail address. Subscribers are charged $50 a year for the service.

*DidTheyReadIt* tracks e-mails by using web bugs that are embedded in the e-mail. They are imperceptible image files that detect the IP address of the recipient's computer, and can then guess where the recipient is located. There are limitations, however, as the software cannot display a web bug in e-mail clients configured to display text only.

Rigo Wenning, Staff Counsel at the World Wide Web Consortium, explains that web bugs have been used by marketers at least since 1998, and does not see *DidTheyReadIt* as a new