20 YEARS
PL&B ANNIVERSARY
1987-2007

INTERNATIONAL NEWSLETTER

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

EU court rules that names of those attending Commission meeting must be disclosed

Lobbyists must be named – transparency is more important than privacy when it comes to revealing who attends meetings at the European Commission. By **James Michael**.

The EU Court of First Instance on 8 November overruled a Commission decision refusing to disclose names of those attending a Commission meeting. The Court ruled that the right of access to documents containing personal data must be guaranteed if disclosure does not undermine protection of the privacy and integrity of the person concerned.

The purpose of the meeting was to discuss whether to drop EU competition policy legal proceedings against the UK for refusing to allow imports of Bavarian beer. Many operators of pubs and bars in the UK were "tied" by exclusive purchasing contracts requiring them to obtain their beer from certain breweries. As a result, the Bavarian Lager Company, an importer of German beer, was not able to sell its product in the UK.

In 1993, the company lodged a complaint with the Commission, arguing that British legislation on tied public houses had the effect of a

Continued on p.3

Japan's High Court confirms record damages for a data leak

Will case set precedent for Japanese Airlines employees' privacy case? **Eric Kosinski,** of White & Case LLP, reports from Tokyo

On 8 February 2007, the Tokyo District Court issued a decision in a personal data leak lawsuit against Tokyo Beauty Center Group Co. Ltd (TBC), a large beauty salon chain, awarding ¥300,000 ($265) to 13 of the 14 plaintiffs, the highest per plaintiff privacy damage award to date. On 28 August 2007, the Tokyo High Court upheld this landmark decision. Although the damage award is still modest by other standards, this case demonstrates the increasingly serious attitude of Japan's courts towards privacy protection.

The State of Japan's Privacy Law

The Personal Information Protection Law (PIPL) is the central privacy legislation in Japan (*PL&B International*, February 2007, pp.12-13, September-October 2005, p.1). It came into effect in 2005 and imposes important restrictions on how business may use employee and customer information. It is enforced by the ministries (p.8), but its provisions provide evidence for the standard of care in a civil data leak suit. The TBC

Continued on p.3

Issue 90 **December 2007**

Electronic Versions of PL&B Newsletters now Web-enabled

To allow you to click from web addresses to websites

INTERNATIONAL newsletter
ISSUE NO 90 December 2007

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

EDITOR
James Michael
james.michael@privacylaws.com

DEPUTY EDITOR
Laura Linkomies
laura@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

NEWSLETTER SUBSCRIPTIONS
Glenn Daif-Burns
glenn@privacylaws.com

CONTRIBUTORS

Eric Kosinski
Attorney, White & Case LLP, Tokyo

Whon-il Park
Associate Professor of Law, Kyung Hee University, South Korea

Nigel Waters
Pacific Privacy Consulting

Dugie Standeford
PL&B Correspondent

Merrill Dresner
PL&B Correspondent

Muriel Faden da Silva
Lawyer, Vieira de Almeida & Associados, Lisbon

PUBLISHED BY
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200, Fax: +44 (0)20 8868 5215
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 Hendi +44 (0)20 7336 7300
ISSN 0953-6795 ©2007 Privacy Laws & Business

comment

Privacy and transparency

Open government prevails in two courts; liability for data breaches continues internationally; and the Greek DPA resigns in protest.

Data protection and freedom of information laws do sometimes conflict. All access-to-information laws have exemptions for personal privacy, and all data protection laws give affirmative rights of subject access to information. They are complementary measures, designed to redress the imbalance in society regarding control over information. Those who exercise power, usually do so with as much secrecy as possible while demanding as much information as possible about those who are subject to that power. Most countries with access to information laws also have privacy laws (but not all, e.g. South Africa, *PL&B International*, June 2005, p.9-11 and May 2006 pp.16-17). Some countries, such as France in 1978, legislated on both subjects simultaneously.

Two courts recently have ruled that government information must be released in cases involving privacy claims. The EU Court of First Instance (p.1) said that the names of those attending a meeting about competition in the beer business must be made public, including industry representatives and civil servants from the EU and UK, despite claims that their privacy should be protected. In the US a federal judge has ordered the Director of National Intelligence to disclose minutes of meetings with telecoms lobbyists (p.4). The meetings concerned privacy because they were about legislation to give telecoms immunity from liability for violating privacy laws by turning over sensitive personal information to government agencies without a legal order.

Data breaches in both the private and public sector continue to have legal consequences around the world. In Japan, record damages for leaked information from beauty salons were upheld (p.1); in the US, penalties are imposed on banks involved in the TJX leaks (p.5), and in the UK the government loss of personal details on almost half the population has led to stronger powers for the Information Commissioner (pp.26-27).

In Greece, for the first time in the international history of data protection law, the head, deputy head and five members of the data protection authority have resigned in protest at a government ruling. A public prosecutor told police to use traffic surveillance cameras for purposes that were prohibited by a ruling from the authority.

James Michael, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B newsletters

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 James Michael on Tel: +44 (0)20 8868 9200 or e-mail james.michael@privacylaws.com.

ures are not violated if (i) an agent mistakenly delivers a package to the wrong party, and the name and address on the package is disclosed; or (ii) personal information is disclosed that is already available in a commercial publication. (METI Guidelines 2-2-3-2, p.29)

4 The following responses are required in case of a data leak or other PIPL violation: (A) investigate the facts, (B) determine the extent of the violation, (C) take measures to prevent reoccurrence, (D) contact data subjects who could be affected, (E) report to the competent minister, and (F) publicly announce the facts and reoccurrence prevention measures. The duty to publicly announce found in (F) does not apply when all the persons who are possibly affected were informed; the personal data that was lost. was immediately recovered without exposure to a third party; concealment measures such as advanced encryption were taken; or no one except the data handler could identify the data subject based on the leaked information. (METI Guidelines 2-2-3-2, 5, p.32)

5 Employers and contractors must now enter into agreements with their employees and agents whereby the employee or agent agrees to keep all personal information confidential. The new guidelines state that, in such agreements, the data handler must clearly distinguish between how the employee or agent should handle personal information and company confidential information/trade secrets. (METI Guidelines, 2-2-3-2, Human Security Control Measures, p. 40)

6 The new Guidelines now include a section regarding safety precautions for credit card personal information. (METI Guidelines, p.77)

To put the above discussion of the METI Guidelines into perspective, a data handler should also bear in mind that its business is subject to the following rules in order of general to specific: (1) the PIPL; (2) the PIPL Enforcement Regulations; (3) the Cabinet Basic Policy on Privacy Protection; (4) the competent ministry's guidelines; (5) industry self-regulatory guidelines; and (6) its own company policy. Therefore, a good knowledge of the relevant ministerial privacy guidelines is important for a successful compliance program, but other applicable rules should also be taken into consideration.

AUTHOR

Eric Kosinski is an attorney with White & Case LLP, Tokyo, www.whitecase.com/tokyo.

Recent DP developments in South Korea

Mobile phone voting used to select candidate; new DP laws after presidential election. By **Whon-il Park**.

South Korea's presidential election, scheduled for 19 December 2007, is producing a series of data protection issues, but major changes to Korea's data protection laws are on hold until after the election. During 2007, privacy guidelines with respect to state-of-the-art technologies have also been revised, reflecting the demand of business circles.

Revisions to RFID and Biometric Guidelines

Kaesong Industrial District, just over the North Korean side of the border with South Korea, was one of the topics discussed at the Inter-Korean Summit Meeting held at Pyongyang, North Korea, in early October. Raw materials and commodities moving to and from Kaesong district are bearing radio frequency identification (RFID) tags, which hold information about the items.

Previously, a state-of-the-art technology like an RFID system was allegedly controlled by the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. However, the United States has now allowed the attachment of RFID tags to items transported to and from Kaesong district, thus facilitating the customs clearance process at the North-South check points.

In South Korea, RFID systems are increasingly used by logistics businesses. Being afraid of the possibility of abuse and misuse of personal data recorded in, or linked with, these electronic tags, the government in 2005 established the RFID Privacy Protection Guideline. The Guideline was revised in September 2007 to modify provisions on RFID readers and RFID service providers. In particular, when RFID service providers use the information generated from the process linking commodity information recorded in the RFID tag to the personal information beyond the scope of the initial purpose of collection, or provide such information to a third party, they are required to obtain the consent of the relevant user. In cases where RFID service providers collect, use or provide the personal location information by means of the RFID system, South Korea's Location Information Act then applies to protect the personal location data.

Now that biometric information is widely used in Korea, the Biometric Information Privacy Guideline has also been implemented since December 2005. This Guideline was also revised in September 2007 following the demands of the security and medical industries. It requires the separation of unprocessed original data from characteristic data extracted therefrom.

Accordingly, the operator must segregate and maintain the original information collected by it apart from such information as name, personal ID number, address, the provider of which can be identified. The operator or the third party recipient should promptly destroy biometric information of the provider lest they should be restored insofar as the purpose of collection or use of biometric information is attained.

These RFID and biometrics guidelines are based on the privacy protection principles provided in Korea's Data Protection Act. As the title "guideline" indicates, they are not norms with legal effect, but a kind of soft law which provides a self-regulatory guideline to RFID or biometric businesses. The authorities concerned were afraid a legal frame could dwarf the burgeoning RFID or biometric industry in Korea. However, some enforceable regulations will come up to the surface when the advancement of the technologies and increasing commercial use result in privacy infringement.

Presidential politics and privacy

With a presidential election near at hand, allegedly leaked personal information of presidential candidates has become an epicentre of political disputes. It was reported that several officials at the National Intelligence Service (a Korean CIA equivalent) and the National Tax Service accessed the databases maintained by the administration to examine the properties of one candidate, the front-runner of the opposition group, beyond their explicit authorisation. The opposition party was suspicious that the Presidential Office might be behind such investigation despite its denial. On the other side, in October, the name of the President, Roh Moo Hyun, was found on a list of elector groups for the primary election of a presidential candidate of the ruling party. It was stolen by somebody from other lists, contrary to the intent of President Roh, the National Police said.

The ruling United New Democratic Party introduced mobile phone balloting for the first time in electing its presidential candidate. The electors were chosen at random from the pool of applicant-constituents. Although this kind of balloting raised drastically the election participation rate of primary electors, there were complaints that the principle of secret ballots was threatened by the procedure and that personal information was probably abused. Mobile phone balloting will not be used in the main event, the presidential election in December, but this brand-new experiment with information technology attracted public attention at home and abroad.

New privacy legislation awaits election results

The government's plan for "new legislation on data protection" will have to wait until a new President is inaugurated in late February 2008. Three draft Bills on comprehensive data protection have been placed before the National Assembly. However, lawmakers are hesitant because those Bills are hard to reconcile with each other, and no one regards their passage as urgent. In fact, they have nothing to do with this year's presidential election.

The Ministry of Information and Communication (MIC) held public hearings regarding its legislation proposal on 28 August 2007. MIC officials planned to spin off the current overall Data Protection Act, which covers three parts – communication network maintenance, personal information protection and minor computer user protection. After detailed research and deliberations for a year, the MIC unveiled its proposal at the hearings to segregate the existing law into a draft "Act on the Protection of Broadcasting and Communication Systems", "Data Protection Act" and "Act on the Protection of Information and Communication Users".

As far as data protection is concerned, MIC officials are increasingly anxious about incidents of the leakage of personal data and are willing to expand the scope of persons who are regulated by the Data Protection Act to cover all personal data handlers from the current "information service providers" (ISPs). This would seem to abolish the grey zone of personal data collectors who are not ISPs. The MIC also proposes to increase the amount of a penalty imposed on privacy violators. They proposed to incorporate into law the guidelines to protect personal information related to RFID tags and biometric devices and minimise the process to identify the user by means of the controversial "resident registration number". They are going to adopt the mandatory use of alternative IDs such as vertical resident registration numbers, personal identification keys or certified authentication certificates issued by credit-rating agencies.

For the time being, the MIC proposal is in the process of receiving comments, suggestions or criticism from academia, NGOs and business circles. Either the MIC proposal or the dormant Bills on comprehensive data protection will be considered by a new government with a fresh mindset in 2008.

AUTHOR

Whon-il Park is Associate Professor of Law, Kyung Hee University, South Korea
E-mail: onepark@khu.ac.kr

events diary

Events organised by *PL&B*

11 December 2007, **European Privacy Officers Network: Asia-Pacific Briefing,** London. Professor Graham Greenleaf, Asia-Pacific Editor, *Privacy Laws & Business International Newsletter*, is giving an Asia-Pacific briefing. Papers available.

22 and 29 January 2008, **Direct Marketing Association Data Protection Compliance Workshop**, London.

29 January 2008, **European Privacy Officers Network: EPON/IPON members only issues meeting**, London.

11 & 12 March 2008, **European Privacy Officers Network: Spain Roundtable**, Madrid. Briefing and Roundtable with the Director of Spain's Data Protection Agency and his senior colleagues.

20 & 21 May 2008, **European Privacy Officers Network: Luxembourg Briefing and Roundtable**. With Luxembourg's Data Protection Commissioner and his senior advisors.

7 to 9 July 2008, **Annual Conference 2008**, St. John's College, Cambridge, UK. *Privacy Laws & Business*'s 21st Annual International Conference.