INTERNATIONAL NEWSLETTER

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Art. 29 WP sets short retention limit for search engines

Contrast with longer limits for service providers.

The EU Article 29 Data Protection Working Party decided on 4 April that Internet search-engine providers must reduce the time they retain users' online records to a maximum of six months. They unanimously adopted proposals that would force search engines to reduce storage time unless there is "a valid justification".

Alex Türk, the new chairman, said search engines must delete personal information "the moment they don't need it". In May 2007, the Working Party told Google that it could be violating EU privacy laws by preserving user data for as long as two years. Google then reduced the storage period to 18 months. Microsoft and Yahoo followed in July, saying they would limit the time they keep data records to 18 months and 13 months, respectively.

The six months time limit for retention contrasts with the time limits on data retention for electronic

Continued on p.3

French court bans teacher rating website. New Canadian employer rating site thrives

The ban by a French court of a teacher evaluation website pits the right to privacy against freedom of expression. How have other countries dealt with such websites? Could similar websites rating employers survive a similar challenge? By **James Michael**.

On 3 March the Paris Tribunal de Grande Instance (TGI) ordered note2be.com, a website where students evaluate their teachers, to suspend the processing of personal data about teachers (case 08/51650). The website had posted anonymous comments on 50,000 teachers in four weeks. The Tribunal ruled that the website collected and processed personal data on French teachers, such as names, schools and subjects taught, without obtaining their consent. Note2be.com claimed that the freedom of expression of students justified the lack of consent by teachers. The court said that the students' freedom of expression could be limited to protect the legitimate rights and interests of the teachers. The court asked the website to take all reasonable measures to preserve the privacy of the teachers ranked on the website, in particular by "moderating a priori" the content of a forum where students can exchange opinions on their teachers. A fine of €1,000 per day was imposed

Continued on p.3

Issue 92 **April 2008**

INTERNATIONAL newsletter
ISSUE NO 92 April 2008

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
Nigel Waters
Principal, Pacific Privacy Consulting, Australia

Eric Kosinski
Attorney, White & Case LLP, Tokyo

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

Professor Dr Paul Roth
Faculty of Law, University of Otago, New Zealand

Dr Gerrit Hornung
Director, Projektgruppe verfassungsverträgliche Technikgestaltung, University of Kassel, Germany

Eleni Martsoukou
Yale Law School Fellow at the American University in Cairo, Egypt

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 six 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

"comment"

Harmonising laws without levelling down standards?

Technology-specific legislation is rarely a good idea. Either the technology evolves so quickly that the law no longer applies or (at least) two legal regimes emerge, applying different rules to technologies doing the same thing. Data protection began by being limited to (in the words of the Council of Europe Convention in 1981) "automatic processing" but has now evolved via the EU Directive and national laws to apply the same standards to manual processing.

The EU has now said, by the Article 29 Working Party, that search engines should retain personal data no longer than necessary, and at the most for no more than six months (p.1). Telecoms service providers, however, are obliged by the EU Data Retention Directive to retain data for at least six months and at most two years. So telecoms companies that also provide search engines will have two regimes for personal data, depending on whether it was generated by telecommunications or by search engine use. There is little evidence that one class of data is more sensitive than the other, or that one is more relevant to law enforcement than the other. The Directive is now being challenged in the European Court of Justice.

Despite attempts using the Council of Europe Convention and the EU Directive to harmonise national laws in Europe on data protection and privacy, national differences persist. In France, courts have closed down a teacher rating site (p.1) and awarded damages to President and Madame Sarkozy for the unathorised use of their images in an advertisement (p.15). In the UK, at least, similar teacher rating sites are tolerated (thus far) and are protected under a German court ruling. The unauthorised use of someone's image in the UK is generally lawful (but subject to the industry's Code of Advertising Practice). Such differences may be resolved by the European Court of Justice (or simply left to the states, as in *Promusicae* (*PL&B International*, February 2008, p.21)), or perhaps the subject of a revised directive, as proposed by the UK Information Commissioner (*PL&B UK*, September 2007, p.5), which on 14 April became the subject of a consultancy tender to explore a more practical approach.

On the subject of international standards, the Council of Europe is on the verge of adopting a Convention on Access to Official Documents (p.15). If the Council succeeds, whatever a Convention's limitations, can an EU Directive on the subject be far behind?

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.

1. A data controller may not provide to its data processor personal data that is not necessary to fulfil the duties delegated to the data processor.
2. A data controller must take care to choose a data processor that takes adequate data protection measures.
3. The data processing contract between the data controller and its data processor must state the personal data protection measures to be taken by the data processor and must state that the data controller understands the conditions under which the personal data will be handled by the data processor.
4. A data controller must inspect its data processor's data protection measures as appropriate from time to time. The standard for this surveillance is higher when the personal data being provided to the data processor is of the type that, upon a data leak, would likely cause secondary damage beyond the initial infringement of the data subject's privacy (credit card information, for example).

The third new rule stated above (the data processing contract shall state (1) the data protection measures to be taken by the data processor, and (2) that the data controller understands the conditions under which the data will be handled at the data processor) appears to be a response to a defendant's argument in the landmark Tokyo Beauty Center Group (TBC) data leak case (*PL&B International*, December 2007, p.1). TBC delegated the handling of customer data to an IT specialist that caused a large data leak. The court rejected TBC's argument that a company, such as itself, that has no IT specialisation, should not be expected to understand and oversee the data protection measures of its data processor. The new METI Privacy Guidelines have adopted the court's view that data controller ignorance cannot excuse failure to oversee a data processor.

In conclusion, data controllers will need to (1) scrutinise systematically the necessity of transmission of data to data processors, (2) be careful to choose only data processors that have proper data protection measures in place, (3) specifically state in the data processing contract the security measures to be taken by the data processor and that the data controller understands the circumstances of data handling by the data processor, and (4) inspect the data processor's security measures on a reasonably frequent basis. Since these amended METI guidelines have the potential to dampen the growth of data outsourcing by Japanese companies, it will be interesting to see how industry will react.

AUTHOR

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

New 'smart' ID cards for Taiwan's resident foreigners

Taiwan's National Immigration Agency (NIA) has begun issuing integrated circuit Alien Resident Cards (IC ARC) to resident non-Taiwanese and overseas Chinese people. The NIA plans to replace all current paper-based ARCs with the new versions by the end of 2008. The IC ARC will also include an individual's permit for multiple re-entry if issued.

At present, there are currently over 500,000 ARC holders, including about 330,000 foreign blue-collar workers in Taiwan, mostly from the countries of South East Asia. Taiwan claims that the new IC ARCs are necessary to facilitate the digitalisation of information regarding foreigners, streamline immigration and travel, reduce forgery, and assist anti-terrorism operations.

The NIA has yet fully to disclose what data will be stored on the IC ARC. It has stated that the chip's design follows the electronic international ID cards implemented in a number of other countries. Although the NIA began issuing new IC ARCs in July 2007, relevant legislation and regulations governing the collection and use of biometric data have yet to be implemented. The IC ARC holder's nationality, passport number, date of birth, purpose of residency and residential address appear on the front of the new card. The NIA has also indicated that data will likely include fingerprint and iris scans and information on employment and spouses or relatives in Taiwan.

Taiwan attempted to institute a national integrated circuit ID card for Taiwanese nationals in 1997. The cards were to include a range of existing identifications and cards, including driver's licence and information on national health insurance and taxation information. Fingerprints were also to be included. The initiative was suspended due to strong public opposition given concerns that personal data would not be adequately protected. Taiwan, however, switched the former paper National Health Insurance cards to the IC cards in 2003-2004. This has, however, not been without opposition as the current programme calls for the cards increasingly to store more and more personal medical information. Subsequent plans to switch from the mandatory paper national ID cards for Taiwanese nationals continue to meet opposition over security and privacy concerns as well as the proposal that fingerprints be included. Taiwan proceeded in 2006 with the issuance of a new paper national ID card.

• *By Marcus Clinch and Shan Lee, members of the legal staff of Winkler Partners, Taipei. See website www.winklerpartners.com.*

events diary

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