20 YEARS
PL&B ANNIVERSARY
1987-2007

INTERNATIONAL NEWSLETTER

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Issue 86 February 2007

Dubai adopts first DP law in an Arab country

Regulations being drafted. **James Michael** interviewed DP Commissioner Dr Nasser H. Saidi.

Dubai is the latest country to join the club of nations with data protection laws, following on from Russia (*PL&B International*, August 2006, p.1). When it was founded in 2004, the Dubai International Financial Centre (DIFC) adopted a system of data protection principles. The data protection regime was previously administered by the Dubai Financial Services Authority (DFSA) under DIFC Law No.9 of 2004, which was enacted and came into force on 16 September 2004. This covered all entities registered within the DIFC, both regulated and nonregulated by the DFSA. DIFC Law No.1 of 2007 expands on and replaces the previous law with the Dubai International Financial Centre Authority (DIFCA) serving as the administrative authority.

In line with its commitment to upholding international best practices, and in order to fulfil its mandate for developing the financial sector in the region, the DIFC has issued a Data Protection Law and appointed a Data Protection Commissioner to ensure

Continued on p.3

EU DP Supervisor rules on SWIFT's secret DP breaches

Remedial action expected by April. Australia also investigates. By **James Michael.**

Peter Hustinx, the European Data Protection Supervisor, adopted an Opinion on 1 February directed at the European Central Bank (ECB) as overseer and user of the SWIFT international financial transactions system based in Belgium. Unlike his more usual role in advising on EU proposals with data protection implications, this opinion is a judgment that the scrutiny of SWIFT financial transactions in secret by the US Treasury violates European data protection law. His opinion is directed at the European Central Bank because it is one of the European institutions which it is his duty to advise.

He concludes that the secrecy that surrounded the transfers of data by SWIFT to the US for more than four years was "regrettable", and recommends that the ECB "urgently" explores and promotes solutions to bring compliance with data protection rules within the scope of oversight by the ECB of the SWIFT system.

With regard to the ECB as user of the SWIFT system, he regards the

Continued on p.7

INTERNATIONAL
newsletter
ISSUE NO 86 **February 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

Dr Michael D. Birnhack
Senior Lecturer and Co-Director of the Haifa Center of Law & Technology, Faculty of Law, University of Haifa, Israel

Franck Dumortier
Researcher at the Center for Computers and Law, University of Namur, Belgium

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

David E. Case
Attorney at White & Case LLP, Tokyo

Jan Willem Broekema
Ex-DP Commissioner, The Netherlands

Dugie Standeford
Freelance journalist

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

Design by ProCreative +44 (0)20 8429 2400
Printed by Hendi +44 (0)20 7336 7300
ISSN 0953-6795

“comment”

DP laws spread and bite

The spread of national data protection legislation continues apace, with the surprise of a nearly fully fledged Data Protection Law in Dubai in the United Arab Emirates (“nearly” because although the Law is now in force, the implementing Regulations on matters such as fees, notification requirements and fines have not yet been published) (pp.1-5). Data protection is now seen as a lure for financial institutions. Dubai is not the first country in the Middle East to adopt legislation, however. Israel has had a data protection law since 1981, and current developments are described on pp.6-7. Both Israel and Dubai are seeking an EU adequacy assessment.

“Adequate” has never been used by the EU Article 29 Working Party to describe US legislation. European data protection authorities continue to fume diplomatically at the apparent continuing disclosure to the US Treasury of financial transaction data by SWIFT. The EU Data Protection Supervisor’s Opinion follows on from the Opinion of the Working Party (*PL&B International*, December 2006, p.1), this time with a deadline for action and the possibility of sanctions (p.1).

Those who regard data protection as soft law will continue to be surprised. With the background of the Spanish data protection authority imposing swingeing fines and the French CNIL using its new power to levy a €45,000 fine on Crédit Lyonnais (and requiring them to advertise it), leading UK financial institution Nationwide has been fined £980,000 for security failings that emerged after the theft of a computer containing personal data of its account holders. The fine was imposed by the Financial Services Authority rather than the Information Commissioner, but that was because the FSA could punish more severely than the ICO, and the two authorities co-operated in the matter.

“It was 20 years ago today” (or this month, at least) that the *PL&B International Newsletter* was born, with a mission to report on what was happening in the world of data protection and to explain what it meant. The data protection world was pretty small and European then. Now it is truly global. We have asked five experts who have taken part from the very beginning to reflect on the past and speculate on the future (pp.22-25).

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.

Continued from p.1

the protection of all personal information in the DIFC. Data protection is an especially important issue for international banking and financial services firms, which increasingly process and exchange personal information electronically. The recently approved law will safeguard such information without hindering the flow of data.

The Data Protection Law

The Data Protection Law of 2007 (DIFC Law No.1 of 2007) prescribes rules and regulations regarding the collection, handling, disclosure and use of personal data in the DIFC, the rights of individuals to whom the personal data relates and the power of the DP Commissioner in performing his/her duties in respect of matters related to the processing of personal data as well as the administration and application of the Law. The Data Protection Law was drafted to conform to the principles of the OECD guidelines and the EU Directive. European law firms, including some in the UK, were consulted in the drafting, and the law was subject to 30 days of public consultation before it came into effect. Application for a finding by the EU Article 29 Working Party that the law provides "adequate" protection under the EU Directive is on the newly appointed Data Protection Commissioner's programme for 2007.

The DP Commissioner

The Commissioner, Dr Nasser H. Saidi, is the Chief Economist of the DIFC and Executive Director of the Hawkamah Institute for Corporate Governance at the DIFC. He is a former Minister of Economy and Trade and Minister of Industry of Lebanon. Before his government posts he was an academic economist, holding posts at the University of Chicago, and before that in Geneva and Beirut. He is appointed for a term of three years, and there is no bar to re-appointment. He could only be removed from office by written notice from the President for "inability, incapacity or misbehaviour" (Article 23).

He has the authority to appoint staff and to delegate his authority. So far, he is assisted by an Administrator, and he intends to appoint more staff, including a legal advisor. Under Article 30, he is to prepare funding estimates not later than 45 days before the end of the current financial year, which he is now preparing. He is also empowered by Article 33 to issue Directions. A data controller who fails to comply with a Direction of the Commissioner may be subject to fines and be liable for payment of compensation. He also has the responsibility to issue Regulations under Article 26(3)(h). He is now preparing the first Regulations, which will include the limits on fines which can be imposed.

He explained that "back office operations are being moved into the DIFC, whereas previously back office operations were located elsewhere. If you are processing data in Bangalore, you don't have the protection of data there, whereas here you do."

In 2003, Dr Saidi said that data protection and freedom of information laws were two of five essentials for the development of an e-economy in Lebanon. When asked if the DIFC would have a Freedom of Information Law following its Data Protection Law, he said: "We are concerned about it, but it needs to be taken step by step. Data protection is the first step, and then we will go on to the others.

"The DIFC and the DFSA were of the judgment that this [data protection] only reinforces the role and positioning of the DIFC as an international financial centre. For us, it's a natural thing. If international companies are going to play the international game they have to abide by international rules.

"Data Protection is one of the 12 core standards for a sound financial system. Countries in the Gulf in particular will be moving toward incorporating such principles, including corporate governance and accounting standards. Probably over the next two years, you will see strong developments, particularly as the EU and the GCC [Gulf Co-operation Council] come closer together. There are negotiations at the moment for a free trade agreement between the EU and the GCC. The GCC is considering a customs union, common currency and monetary integration. There are two forces at work: the financial industry itself and the GCC countries, which are getting more closely integrated."

Continued on p.4

THE DUBAI INTERNATIONAL FINANCIAL CENTRE

The law applies to all entities registered and operating in the Dubai International Financial Centre (DIFC), a federal wholesale financial services centre located in the Emirate of Dubai. The DIFC, established in 2004, is a federal financial free trade zone, to which the civil laws of Dubai and the United Arab Emirates do not apply (although the criminal law, which includes some privacy protection measures, does). The DIFC adopts its own civil laws, which generally follow the common legal system. There are now 320 companies, including 120 financial institutions, operating in the DIFC (the register of companies can be found at the DIFC website, www.difc.com). Among the benefits of setting up in the DIFC are: 100% foreign ownership, 0% tax rate on income and profits, a network of double taxation treaties available to UAE incorporated entities, no restrictions on foreign exchange, freedom to repatriate capital and profits without restrictions, and international standards of rules and regulations. The official language of the DIFC is English, and the currency is the US dollar.

The DIFC, with authority to self-legislate in civil and commercial areas, is designed to provide a regulatory regime for the creation and operation of a global financial centre. An amendment to the UAE Constitution and a resulting federal law concerning financial free zones allowed the government of Dubai to create a legal framework based on jurisdictions in Europe, North America and the Far East. The DIFC has its own geographical territory and comprises three independent centre bodies: the DIFC Authority, the Dubai Financial Services Authority (DFSA, which is modelled on the UK Financial Services Authority), and the DIFC Judicial Authority (DIFC Courts) and the Court. Other operating entities include the Dubai International Financial Exchange (DIFX), DIFC Investments and Hawkamah Corporate Governance Institute (CGI).

Both the DIFC Authority and DFSA have reviewed the laws and regulations of the world's major financial centres, and, with the assistance of professional advisers, have adopted and blended various concepts to produce a clear and flexible legislative framework that embodies international standards and best practice. DIFC Laws are written in English and are enacted by His Highness Sheikh Mohammed Bin Rashid Al Maktoum, Vice-President and Prime Minister of the UAE and Ruler of Dubai.

Continued from p.3

Data Protection Law 2007

The law itself is very closely modelled on the EU Data Protection Directive. The General Requirements for processing reflect the principles of data protection. Processed personal data must be processed fairly, lawfully and securely, for specific purposes and not for any incompatible purposes, adequate, relevant and not excessive for those purposes, accurate and up to date, and kept in a form which permits identification of data subjects for no longer than necessary. Every reasonable step must be taken by data controllers to ensure that inaccurate or incomplete personal data must be erased or rectified. Personal data may only be processed if there is written consent of the data subject, it is necessary for the performance of a contract to which the data subject is party, it is necessary for compliance with any legal obligation, or it is necessary to protect the vital interests of the data subject. Two further provisions seem to be specific to the DIFC. Personal data may be processed if "processing is necessary for the performance of a task carried out in the interests of the DIFC, the Dubai Financial Services Authority or the DIFC Courts, or in the exercise of the Commissioner of Data Protection's functions or powers vested in the data controller or in a third party to whom the personal data are disclosed, or when processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party or parties to whom the personal data is disclosed, except where such interests are overridden by compelling legitimate interests of the data subject relating to the data subject's particular situation".

Processing sensitive personal data

Sensitive personal data is defined as "revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal records, trade-union membership and health or sex life". It may only be processed with the written consent of the data subject, if it is "necessary for the purposes of carrying out the obligations and specific rights of the data controller", or it is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent. Sensitive data may also be processed by a non-profit body about its members, if the data have been made public by the data subject or if necessary for a legal claim, or if necessary for compliance with a legal obligation of the data controller. One provision which seems to be special to the DIFC is that sensitive data may be processed if "necessary to uphold the legitimate interest of the data controller recognised in the international financial markets, provided that such is pursued in accordance with international financial standards and except where such interests are overridden by compelling legitimate interests of the data subject relating to the data subject's particular situation". Sensitive data may also be processed if necessary to comply with regulatory requirements, anti-money laundering or counter terrorist financing obligations, as well as for medical purposes by a health professional bound by an obligation of secrecy. Such processing may also be done to protect members of the public from financial loss or seriously improper conduct in the provision of banking and related services ("either in person or indirectly by means of outsourcing"), or by written authorisation of the Data Protection Commissioner.

Sensitive personal data may also be processed if a permit has been obtained from the Commissioner and adequate safeguards are applied. If the Commissioner refuses to issue such a permit, there is a right of appeal to the Court, the decision of which is final.

Transfers of data outside the DIFC

Personal data can be transferred out of the DIFC if there is an adequate level of protection, which is determined either by the written approval of the Commissioner, or if the jurisdiction is listed as acceptable in the Regulations. The Office of the DP Commissioner will seek to apply adequacy standards in line with standards set out by the European Commission. A list of acceptable jurisdictions will be included in the Regulations. Until then, personal data may only be transferred out of the DIFC upon the written approval of the Commissioner confirming that there are adequate safeguards including laws and regulations with respect to the protection of this personal data in the jurisdiction it is intended to be transferred. Transfers to a jurisdiction in the absence of an adequate level of protection can only take place if one of 10 conditions is satisfied. Such transfers can be with the permission of the Commissioner and adequate safeguards are applied by the data controller (a refusal by the

UNITED ARAB EMIRATES FACT SHEET

The United Arab Emirates is a constitutional federation of seven emirates: Abu Dhabi, Dubai, Sharjah, Ajman, Umm al-Qaiwain, Ras al-Khaimah and Fujairah. The federation was formally established on 2 December 1971 by the then Trucial States after independence from Britain. Although each state maintains a large degree of independence, the UAE is governed by a Supreme Council of Rulers made up of the seven Emirs, who appoint the Prime Minister and the cabinet. It held its first national elections – for an advisory body – in December 2006. It has a federal court system, introduced in 1971, which applies to all emirates except Dubai and Ras al Khaimah, which are not fully integrated into the federal judicial system. All emirates have secular courts to adjudicate criminal and civil cases as well as Sharia Courts.

The Council of Ministers is appointed by the President. There is also a Federal Supreme Council (FSC), composed of the seven emirate rulers. The FSC is the highest constitutional authority in the UAE; it establishes general policies and sanctions federal legislation, and meets four times a year.

The President and Vice-President are elected by the FSC for five-year terms. The Prime Minister and Deputy Prime Minister are appointed by the president. The unicameral Federal National Council (FNC) has 40 seats. The members were appointed by the rulers of the constituent states to serve two-year terms until 2006, when elections for one half of the FNC (the other half remains appointed) were held in December. The FNC reviews legislation but cannot change or veto it.

Commissioner to issue such a permit can be appealed to the Court). They can also be with the consent of the data subject, if necessary for a contract between the data subject and controller, or a contract in the interest of the data subject between the controller and a third party, or if necessary to protect the vital interests of the data subject. They may also be made if necessary or legally required "on grounds important in the interests of the DIFC" or the defence of legal claims. They may also be made if the transfer is from a public register, at the request of a government agency, when necessary "to uphold the legitimate interests of the data controller recognised in the international financial market" or necessary to comply with any regulatory requirements or "anti-money laundering or counter-terrorist financing obligations".

Obligations of data controllers

Data controllers have obligations to data subjects to inform them of the controller's identity, the purpose of the processing, information to guarantee fair processing, the recipients of personal data, whether replies to questions are obligatory or not, the right of a subject's access and the rights of rectification, whether the data will be used for direct marketing, and whether it will be processed to uphold legitimate interests of the data controller recognised in the international financial markets.

Here there has been a slip in drafting. Article 13.(1)(h) refers to processing "on the basis of Article 11(1)(g)", an article which does not exist. The provision probably should refer to Article 10(1)(g).

When personal data are obtained from sources other than the data subject, the controller has obligations to inform the data subject of the controller's identity, the purposes of the processing and any further information to guarantee fair processing, such as categorises of data, recipients, right of access and rectification, whether it will be used for direct marketing, and whether it will be processed for interest, recognised in international financial markets. This does not apply if the controller reasonably expects that the data subject already knows, or if providing such information would be impossible or involved disproportionate effort. Data controllers must implement appropriate security and must notify the Commissioner if there is any breach.

Rights of data subjects

Data subjects have rights to know whether their personal data are being processed, access to the data and the source of it, and a right of rectification, erasure or blocking. Data subjects also have rights to object to the processing of personal data, and to be informed before personal data are disclosed to third parties or used for direct marketing, and the right to object to such use. The DP Commissioner can initiate a claim for compensation on behalf of a data subject before the Court where there has been a material contravention of the Law to the detriment of the data subject (Section 25(3) (g)).

Regulations: notification and fees

Data controllers must notify the Commissioner in accordance with Regulations, which are now being drafted, and the Commissioner will keep a register of personal data processing operations notified to him. The Regulations will require a data controller to record and give notification to the Commissioner on its personal data processing operations, detailing among other things: a description of the personal data processing being carried out; an explanation of the purpose for the personal data processing; the data subjects or class of data subjects whose personal data is being processed; a description of the class of personal data being processed.

The Regulations have gone out for public consultation for a period of 30 days, and comment is sought from the general public as well as leading law firms and EU parties.

Fees will vary by the registered nature of entity and the DP risk associated with that entity. The DP Fee Schedule is being finalised and will be made public shortly. Together with the Law, the Regulations provide a framework for the regulation of data protection in the DIFC. The Regulations will cover the processing and transferring of sensitive personal data in and out of the DIFC, records and notifications and process of mediation.

Powers of the Commissioner and the Court

The Commissioner has powers to issue directions to controllers, which may be reviewed by the Court, and a controller who fails to comply may be subject to fines and be liable for compensation. The DP Commissioner has the right to impose fines in the event of non-compliance. Administrative fines associated with contraventions are being finalised and will be made public shortly. Currently, publicity is not imposed as a sanction for contravening the Law. However, this may be introduced as part of the Regulations in the future. The court may make any appropriate order, including remedies for damages, penalties or compensation.

INFORMATION

For a copy of the Law, a list of frequently asked questions or to find out further information on data protection in the DIFC, please refer to http://dp.difc.ae

Changes ahead for Israel's DP law to bring it in line with EU Directive

The Israeli Data Protection regime is constantly revised. In January, an expert committee recommended further changes. By **Dr Michael D. Birnhack** and **Franck Dumortier**.

The first change took place in August 2006 by means of the establishment of a new agency in the Ministry of Justice, in charge of legal aspects of Information Technology. Under the auspices of the new agency, the enforcement efforts regarding data protection are revised and accelerated. Although the new agency is located within the administration of the Ministry, it is designed to be independent in its activities, ranging from policy making to concrete actions.

The second change is the publication of the *Schoffman Report* in January 2007, based on an expert's committee that considered the matter for two years. The committee was chaired by the Deputy Attorney General Mr Yehoshua Schoffman and members included representatives of the government, academia, private sector and non-governmental organisations. The report was particularly influenced by the European and Canadian data protection regimes. It is now open to public comments and is likely to result in a governmental Bill to amend the Privacy Protection Act. The main recommendations of the report are:

Manual databases: The report proposes to extend the data protection regime to cover manual personal filing data systems. Accordingly, the report proposes to redefine a database: "A database is any set of personal data, which is accessible according to specific criteria." The language is very similar to that used in the EU Directive.

Personal data: The report proposes redefining "personal data" to mean "any information relating to an identified person or to a person who can be identified using reasonable measures". The Committee explicitly refrained from defining "sensitive data" as its only effect would be to trigger the registration of a database. The Committee was of the opinion that the sensitivity of the data can be a relevant consideration in judicial evaluation of violations of privacy.

Registration duty: The report proposes narrowing the situations where there is a duty to register a database with the Database Registrar, a process which is similar to the European notification requirement. The Committee was of the opinion that the current registration requirement is overbroad, impractical and has, *de facto*, failed. Accordingly, registration will be required when data are commercially traded or, in cases of sensitive data, is yet to be clarified. The report recommends that the Minister of Justice will be able to determine the kind of databases subject to the duty or exempt from it and that the Database Registrar has a similar authority regarding individual databases.

Stronger enforcement: The report proposes strengthening the powers of the Database Registrar, regarding the following: general enforcement powers, issuing binding rules, issuing individual orders regarding data security, receiving complaints from data subjects and acting upon them, and redefining the position as a Database Commissioner. All members of the Committee were of the opinion that these are much needed steps. A majority recommended that the Registrar be accorded independent status to join litigation regarding data protection, without being subject to the Attorney General's authority. The report further proposes to allow class actions. Current Israeli law enables such actions only in consumer-related settings. The recommendation would enable class actions also when the database operator is the state or an employer.

Data collector's duties: The report proposes not to add general duties to those already imposed on data collectors. A minority of the committee proposed that an explicit requirement be added, regarding the adequacy, relevancy and excessive collection of data. It also proposes broadening the notice requirement so that a collector should notify the data subject of the exact source of the duty to provide information, and of the data subjects' rights regarding the collector and means of contacting the collector.

Data security: The report proposes (1) to clarify that the duty to undertake data security measures is to be assessed according to a reasonability standard, (2) to authorise the Database Registrar to issue individual orders regarding data security and (3) to impose a duty on a collector to inform data subjects in case of a database security breach.

Access rights. The report proposes to widen the scope of the right of a data subject to access the data about oneself to cover the kind of personal data, the sources of the data, whether the personal data is transferred to third parties, to whom and for which purposes. The cost of the access to the data shall be pre-determined by the law but subject to the review of the Database Registrar.

Transfer to third countries: At the proposal of the Committee, the Ministry of Justice and the Ministry of Foreign Affairs approached the European Commission with a request that the adequacy of the Israeli data protection is assessed, under article 25(2) of the 1995 Directive.

Continued on p.7

Continued from p.1

ECB as a data controller, jointly with SWIFT. He uses his power under the regulation regarding personal data processing by EU institutions to urge the ECB to explore "solutions to make its payment operations fully compliant with data protection legislation and take appropriate measures as soon as possible". He invites the ECB to report back on the measures taken to comply with his opinion by April at the latest. After receiving this report, he will consider "taking into account possible coordination with other data protection supervisory authorities, any further action" on the basis of his powers. The further action obviously could include the imposition of sanctions.

Considering the ECB as policy maker he "stresses that it would not be acceptable that the architecture of the European payment systems would continue to allow and facilitate that personal data relating to any euro payment between Member States are transferred to third countries in breach of the data protection legislation and made available – routinely, massively and without appropriate guarantees – to third countries' authorities". He calls on the ECB "to ensure that European payment systems… are fully compliant with European data protection law".

He concludes that "a wide range of EU and international instruments aimed at fighting crime and terrorism while ensuring protection of fundamental rights are already available" and should be fully exploited before proposing new international agreements. "In any case, the fight against crime and terrorism should not circumvent standards of protection of fundamental rights which characterise democratic societies," he adds.

In his Opinion, the Supervisor remarks that "lack of compliance with data protection legislation may actually hamper … the financial stability of the payment system for at least two reasons: first of all, it could seriously affect consumers' trust in their banks; secondly, it might lead European data protection authorities, as well as judicial authorities, to use their enforcement powers to block the processing of personal data which are not in compliance with data protection law".

This follows a ruling by the data protection authority in Belgium (*PL&B International*, December 2006, pp.1-4), where SWIFT is located, that the secret and continuing disclosure by SWIFT of personal data regarding financial transactions to the US Treasury violated national data protection laws and the European Union Data Protection Directive. The Article 29 Working Party, whose members include all EU national data protection authorities and the Supervisor, also reached the same conclusion in November. There are no sanctions for violating the Directive itself, and neither the Article 29 Working Party nor the Supervisor has the power to impose sanctions. However, the effect of the Working Party's emphatic opinion in November and the Supervisor's equally strong opinion means that if there is no change in the arrangement between SWIFT and the US government when the ECB reports back by April, there is a strong possibility that the Belgian data protection authority may impose sanctions on SWIFT, and that other national data protection authorities may impose co-ordinated sanctions on banks using SWIFT for communicating their customers' financial transactions.

The Luxembourg Data Protection Commission has already (in December) been assured by banks in that country that "they are actually taking actions in order to ensure compliance with EU law". The Commission has said: "Enforcement could be envisaged in case the current situation remains unchanged. However, we trust that SWIFT and the financial institutions alike will be convinced of the necessity to comply with EU law with regard to SWIFT's transfers to the United States Treasury and will take the necessary steps to achieve this goal."

Australian Commissioner also investigates

In Australia, following a complaint by the Australian Privacy Foundation, the Federal Privacy Commissioner has commenced an investigation of the actions of Australian financial institutions in disclosing personal information. to the SWIFT inter-bank network, particularly once these institutions became aware of SWIFT's disclosures of personal information to the US government. Resolution of this investigation may involve the Commissioner having to consider whether the US provides protection to privacy comparable with that provided by the data export restriction principle (NPP 9) in the Privacy Act 1988's National Privacy Principles.

FURTHER INFORMATION

See www.privacy.org.au/Papers/SWIFT-AustbanksOFPC061012.pdf.

Continued from p.6

Conclusion

From a European point of view, the data protection regime of third countries should be assessed under the core criteria of adequacy, as stated by the 1995 Directive and interpreted by the Article 29 Working Party. As the criterion of "adequate protection" conceptually differs from "equivalent protection", one should not expect the Israeli law to be exactly identical to the law in the Member States. Nonetheless, the *Schoffman Report*'s recommendations would bring, if enacted, the Israeli regime much closer to the EU's regime and to the wording of Directive 95/46/EC. Moreover, the recent establishment of the Agency for Legal Aspects of Information Technologies promise a substantial strengthening of the enforcement of the data protection regime in Israel.

AUTHORS

Dr Michael D. Birnhack is Senior Lecturer and Co-Director of the Haifa Center of Law & Technology, Faculty of Law, University of Haifa, Israel.
E-mail: michaelb@law.haifa.ac.il,
website: http://techlaw.haifa.ac.il
Franck Dumortier is Researcher at CRID (Center for Computers and Law), University of Namur, Belgium. E-mail: Franck.dumortier@fundp.ac.be, website: www.crid.be

UK's FSA fines Nationwide £980,000 for lapses in data security and warns other firms

The UK's Financial Services Authority has set a precedent by fining an organisation for data security failings. The UK's Information Commissioner was content for the FSA to take the lead role. **Stewart Dresner** reports.

On 14 February, the UK's Financial Services Authority (FSA) fined the Nationwide Building Society nearly one million pounds for security failings that emerged after a laptop was stolen containing customer data. Nationwide is the UK's largest mutual savings and loans organisation with 11 million customers. This is the first time that the FSA has imposed a fine for data security failings.

The laptop was stolen from the home of a Nationwide employee last year (*PL&B UK Newsletter*, December 2006, p.4). Nationwide did not start an investigation until three weeks after the theft, when the employee in question returned from holiday. The firm claims that no customer has suffered a financial loss due to the incident and that the data in question was marketing data.

The FSA investigation found that the building society did not have adequate information security procedures and controls in place. It was found to be in breach of the FSA's Principle 3, which states that a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems. A further reason given by the FSA was that the firm "failed to implement adequate training and monitoring to ensure that its information security procedures were disseminated and understood by staff".

How was the Data Protection Act involved?

1. The Data Protection Act has similar requirements to the FSA's data security rules, but the Information Commissioner is mentioned only once in the FSA's eight page Final Notice. Why? It states: "Nationwide reported the loss of the laptop to the police, the Information Commissioner and to the FSA." The Data Protection Act is not mentioned at all. The reason is not directly given in the statement by Phil Jones, Assistant Commissioner at the Office of the Information Commissioner, who said: "The Information Commissioner's Office shares a common interest with the Financial Services Authority in ensuring customer information is held securely, and the two organisations are working closely together to do all we can to ensure breaches of this nature do not reoccur. The Information Commissioner's Office has issued guidance in our Code of Practice on Employment to help organisations that use mobile devices, such as laptops, comply with the law."

In fact, in an interview with Channel 4 Television news Phil Jones provided the reason why the Information Commissioner handed the case over to the FSA: "It didn't make sense for us to duplicate effort," he said. A further unstated reason is that the FSA has much stronger powers to impose penalties. The UK Information Commissioner can issue an Enforcement Notice but only the courts can impose a fine for Data Protection Act offences.

2. Why did the FSA not use the opportunity to warn its constituency of financial services firms of their data security responsibilities under the Data Protection Act? *PL&B* understands from the FSA that its notices deal only with offences within the organisation's jurisdiction.

3. Why was the fine so large? In fact, it could have been £1.4 million if Nationwide had not co-operated fully with the FSA. Nationwide received "full credit" for settlement of the dispute at an early stage and agreed not to appeal the decision. So Nationwide qualified for a 30% reduction of the fine. The building society has written to all its members apologising for the incident and is now looking to strengthen its security policy.

How does the FSA decide on the size of a fine? The general factors which determine the size of a fine are given in the FSA's Handbook section 13.3 (see http://fsahandbook.info/FSA/html/handbook/ENF/13/3) and the specific factors underlying the Nationwide case are spelled out in section 5 of the Final Notice. Factors included "helping to deter other firms from committing contraventions and demonstrating generally to firms the benefit of compliant behaviour".

Mistakes can happen, but Phil Jones said: "The first step is to assess the risk and mitigate that risk."

Clearly the fine could have been even higher, but the FSA stated that since September 2006 "Nationwide has taken steps to address the risks to customers by undertaking a number of actions to address this failure, including: taking a range of additional measures to increase security around accounts; informing customers of the loss of information; affirming its existing policy to reimburse any customer that has suffered financial loss as a result of this incident; and commissioning a comprehensive review of its information security procedures and controls."

In addition, Nationwide had not

been the subject of enforcement action previously.

4. What is the role of publicity in the sanction? The FSA explicitly sees publicity as a valuable tool and, indeed, the Nationwide story attracted national attention in both business and consumer media.

The Nationwide is clearly responding energetically to the security failings. Philip Williamson, Chief Executive stated: "We have extensive security procedures in place, but in this isolated incident our systems of control were found wanting. We have made changes to fill the gap and improve our procedures further.

"Towards the end of last year we sent a letter to every one of our members telling them about this matter and apologising for any concern it may have caused them. We would like to reiterate that apology to our members and assure them that we have taken action to tighten our already high security procedures.

"There has been no loss of money from our customers' accounts as a result of this incident. All Nationwide's customers are protected by the Society's promise that 'If you are the innocent victim of fraud, you will not lose out.'"

In view of this decision, not only businesses regulated by the FSA will now urgently need to reassess their data protection and data security risks and training programmes. In addition, the Information Commissioner is expected to take action in the coming weeks after investigating the disposal of confidential waste left in sacks outside a number of financial institutions (*PL&B UK Newsletter*, December 2006, p.5).

Of course, the Information Commissioner's jurisdiction is not limited to financial organisations. He has all organisations in his sights.

AUTHOR

Stewart Dresner is Editorial Director, PL&B's Newsletters.
E-mail: stewart@privacylaws.com

HP privacy cases continue

Although the California civil action against Hewlett-Packard was settled in December, former HP executives now face federal prosecutions. James Michael reports.

As reported in *PL&B International*, December 2006, p.1, the civil action against Hewlett-Packard (HP) by the California Attorney-General was settled when HP agreed to pay $14.5 million, $13.5 million of which was to fund law enforcement against privacy invasions, identity and intellectual property theft.

The state criminal indictments of former HP Chairwoman Patricia C. Dunn and four others continue. They are also facing prosecutions under federal law for the same invasions of privacy, including obtaining telephone records by "pretexting".

Despite the US Constitutional prohibition of double jeopardy, it is possible to be prosecuted in the federal courts for the same acts which have been the subject of a state prosecution. Although it is constitutionally possible to be prosecuted in federal courts for acts which previously had been prosecuted in state courts, it does not work that way the other way around in California. The law of that state provides immunity for prosecution for acts which have been the subject of a prosecution in another jurisdiction, including the federal courts.

In January, there was an unexpected development in the HP case. Bryan Wagner, a private investigator who had been hired by HP to pose as a reporter to get telephone records for the company's internal inquiry into boardroom leaks, pleaded guilty to federal charges of identification theft and conspiracy in return for a reduced sentence.

The California criminal charges against him have now been dropped. He has agreed to testify against the other defendants in the federal prosecutions, which probably will follow the state prosecutions.

The Securities and Exchange Commission is conducting a formal investigation into the HP affair, and the Federal Communications Commission has requested documents.

On 12 January, President Bush signed the Federal Telephone Records and Privacy Act Protection Act into law, making it a federal crime to obtain confidential telephone records by "making false or fraudulent statements" to a telephone company employee, by "obtaining false or fraudulent documents to access accounts", or by "accessing customer accounts through the internet".

The Act imposes penalties of fines and up to 10 years in prison. Fines are doubled and five years may be added to the prison sentence if the violations involve more than $100,000 or more than 50 customers.

SEOUL CENTRAL DISTRICT COURT ORDERS DAMAGES FOR LEAKED PERSONAL DATA

Last time online games players, this time bank customers, reports Whon-il Park, Associate Professor of Law, Kyung Hee University, South Korea

In March 2006, a big commercial bank in Seoul that sells lottery tickets to customers carried out a campaign to entice lottery players who use the internet to buy more lottery tickets and receive prize money through their bank accounts. A bank employee who sent out promotional e-mails mistakenly attached a file to them that contained the personal information – including names, e-mail addresses and resident registration numbers – of more than 32,000 of the bank's customers. The bank quickly realised

Continued on p.11

Israel asks EU to assess its DP law for adequacy

After a short description of the Israeli data protection regime, which was passed in 1981 and amended since, **Dr Michael D. Birnhack** and **Franck Dumortier** assess the main principles of the Israeli law according to the core criteria suggested by the EU Art. 29 DP Working Party.

Article 25.1 of European Union Directive 95/46/EC prohibits transfers of personal data from Member States of the European Union (EU) to "third countries" – that is, countries outside the EU (and EEA) if the third country in question does not ensure an "adequate level of protection". The power to make binding adequacy determinations lies with the European Commission (Art 25(6)).

The principal methodological criteria for assessing the adequacy of a data protection regime are set out by the Article 29 Data Protection Working Party in WP12: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive. WP12 reflects the main requirements of Directive 95/46/EC and other international data protection instruments. While the core criteria listed in WP12 do not have any formal legal standing, they serve, *de facto*, as the measure against which the adequacy of data protection regimes is evaluated.

The Israeli DP regime

The highest norm protecting privacy is found in s.7(a) of Israel's Basic Law: Human Dignity and Liberty, which provides that "All persons have the right to privacy and to intimacy." As the Israeli Supreme Court has recognised, the Basic Law elevated privacy to a status of a constitutional right. The second level in the normative pyramid is the Privacy Protection Act of 1981 (hereafter: PPA), which has been amended eight times (*PL&B International*, September 2002, pp.25-27).

Chapter 1 of the PPA applies to both manual and electronic data. It prohibits the violation of privacy of any person without that person's consent, and provides for civil and criminal liability. Chapter 2, which regulates databases, includes both a general arrangement (subchapter 1) and concrete rules regarding direct marketing (subchapter 2). Chapter 4 of the PPA contains rules about the transfer of data held by the government and other statutory bodies among themselves and to private bodies.

The PPA's database regime defines a database as "a collection of data, kept by magnetic or optical means and intended for computer processing". Manual records are thus excluded from chapter 2 of the PPA. However, manual databases are subject to the general right to privacy.

The law distinguishes between "information" and "sensitive information". "Information" is defined as details regarding a person's personality, personal status, private affairs, health, economic situation, professional qualifications, opinions and faith. "Sensitive information" includes all elements of "information" with the exceptions of personal status and professional status. Therefore, it should be underlined that the concept of "sensitive information" in Israeli law encompasses a much broader set of data than it does in the European Directive 95/46.

The PPA vests most of the powers for enforcing the data protection regime in the Database Registrar. The Registrar is appointed by the government and integrated within the structure of the Ministry of Justice and, in that sense, is part of the executive branch. However, in practice, we are unaware of any intervention with the decisions of the Registrar. Moreover, having several quasi-judicial powers (mostly the registration of databases), some of the Registrar's decisions can be appealed to a court, and all activities are subject to general judicial review under principles of constitutional and administrative law.

Is the Israeli DP regime adequate?

According to the European Commission's WP12, the concept of adequate protection differs from the concepts of equivalent protection or sufficient protection. Equivalency would have required a strict analytical comparison between the third country's legal scheme and the EU Directive. In other words, the criterion of an equivalent protection would have required third countries to adopt legislation which might be considered as an exact copy of the Directive. With the adequate protection requirement, the question is different. The use of the term "adequate" is meaningful and perfectly translates the pragmatism of the European approach.

As stated in WP12, the approach takes into account the content of the applicable regulations (the purpose limitation principle, data quality and proportionality principle, transparency principle, security principle, rights of access, rectification and right to object, restrictions on onward transfers) and the effectiveness. We examine the Israeli data protection regime according to this approach.

1. The purpose limitation principle is a central pillar of the PPA: In the context of the general right to privacy, it appears in s.2(9), which defines, as a violation of privacy, the "using or transferring information on a person's private affairs, otherwise than for the purpose for which it was given". As for databases, s.8(b) states: "No person shall use information in a database that must be registered under this section, except for the purposes for which the database was set up."

2. Accurate and up-to-date data: No explicit provision in the PPA imposes on the owner or possessor of manual data or manual databases a requirement to update or amend inaccurate data. However, in the context of electronic databases, these principles are assured through s.14 of the PPA, which accords data subjects the right to require the amendment of data.

3. Adequate, relevant and not excessive data: Unlike article 6(c) of the European Directive, the PPA does not explicitly require that data should be "adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed", nor does the PPA contain a provision ensuring that data are only conserved for a reasonable time given the purpose for which they were collected. However, given the importance of the data subject's consent in the underlying philosophy of the law (PPA s.1 reads: "No person shall infringe the privacy of another without his consent"), one could claim that it has the same effect as the European principle. When inadequate, irrelevant or excessive data collection is required by a contract, a data subject can petition the special court on "standard contracts" and request that the contractual section be invalidated. Usually, it is the Attorney General who initiates such procedures, including in the Bank Leumi case, in which the court interfered with the standard contract on data protection issues.

4. Principle of transparency: In the context of manual data and manual databases, no explicit provision in the PPA requires a data controller to notify the data subject as to the purpose of the processing. As for the database regime, PPA, s.11 requires that an application to a person to collect information for the purpose of keeping it in a database should be accompanied by a notice, referring, *inter alia*, to the purpose of the processing and the identity of the data controller. Furthermore, a database that meets one of several situations listed in s.8(c) needs to be registered with the Database Registrar.

5. Security principle: An owner of a database, its possessor or operator, are under duty to maintain the security of the data (s.17). Data Security is defined as the "protection of the integrity of data, or protection of the data against exposure, use or copying, all when done without due permission".

6. The rights of access, rectification and objection: Israeli law accords the data subject with rights of access and rectification, accompanied with procedural guarantees. Moreover, in the context of databases having a direct marketing purpose, the PPA grants the data subjects a right to object to the processing of data relating to them.

7. Onward transfers to third countries: Special regulations address the transfer of data to databases which are located outside Israel: Regulations for Protection of Privacy (Transfer of Data to Databases outside the Country), 2001. It is evident that these regulations are inspired by the EU Directive since these are based on the same principles.

8. Sensitive data: An additional particular safeguard concerning sensitive information is the fact that if a database includes such information, this immediately triggers the duty to register the database with the Database Registrar.

9. Direct Marketing: The operation and holding of a database for the purpose of direct marketing triggers stricter regulation than a "regular" database. In addition to the duties imposed on regular databases, a direct marketing database must be registered with the Registrar. Moreover, s.17F(b) allows a data subject to object, in writing, to the processing of data relating to him, that is, the data subject can require that data referring to him or her be deleted. Alternatively, the data subject can require the database owner that the data referring to him or her will not be transferred by the database owner to third parties, for a limited time or for any time.

10. Automated decisions: Current Israeli law does not contain any specific instructions regarding automated decisions. However, it is clear that when such automated decisions are taken by a public body, they are subject to judicial scrutiny like any other executive decision.

11. Enforcement: Apart from the informal Registrar's competence to receive individual complaints, administrative and judicial routes of enforcement are foreseen. The Registrar can impose administrative fines and the PPA provides for dissuasive criminal sanctions and private civil enforcement.

Continued from p.9

its mistake and stopped sending the e-mails. Although most of the messages sent were retrieved with the help of a portal site operator, 640 had already been opened.

Coincidentally, a decision taken by a court in South Korea at the same time provided the affected bank customers with some encouragement. An online game-site operator that had managed its users' information poorly (*PL&B International*, December 2006, pp.12-13) was ordered by the court to pay 500,000 won ($500) compensation to each to game player in question. In April 2006, the court ruled that the online game company has contractual and legal responsibilities to protect the private information of game players. In other words, providers of internet-based services, such as online game operators, are required to perform a duty of special care to protect the private information of their users as they make commercial profit from their services.

The internet lottery players demanded 3 million won ($3,000) per person from the bank for the mental suffering that arose out of their private information being leaked. The total amount of compensation demanded by the plaintiffs amounted to more than 4 billion won ($4 million).

On February 8, 2007, the Seoul Central District Court held that the bank in the case of the internet lottery players should pay 100,000 won ($1,000) to each person whose name, e-mail address and national ID number were accidentally leaked. The court said that the plaintiffs suffered because their fundamental right to preserve their private information in safety was trespassed contrary to their will and that they deserved the compensation for the mental suffering they experienced. Also, the court pointed out that the bank had made every effort to stop the leakage of private information and there was no report of actual damage. Accordingly, the court limited the compensation to 100,000 won ($100) per person. The representative lawyer was disappointed to hear the court ruling but was satisfied with the court's acknowledgement that in this information society a simple leak of personal information can cause mental suffering.

Japan's privacy law to be revised

Possible revisions to Japan's Personal Information Protection Law could impose an even greater burden on businesses, says **David E. Case**.

Just when Japanese and multinational companies were getting comfortable with the requirements of the Personal Information Protection Law (PIPL) and its guidelines, there are now signs that the law could be amended in the near future, placing additional burdens and complexity on companies already stretched thin.

On 28 July 2006, the Quality of Life Policy Bureau, a policymaking bureau within the Prime Minister's Cabinet Office, released an issue paper for public comment entitled *Primary Issues for Consideration Regarding Personal Information Protection*.[1]

Industry practitioners, consumer groups, academics and lawyers alike used the issue paper and the invitation to submit public comment as an opportunity to air their views on the state of the PIPL. Although collecting opinions from stake holders was one of the stated aims of the Bureau in releasing this paper, it also reads in parts like a response to critics of the Bureau and the PIPL and a pre-emptive strike on future debate.

One gets this impression because while most items presented by the Bureau in the issue paper are phrased in an open-ended manner designed to elicit broad response, others are phrased in a purely rhetorical manner with the apparent intention of ending discussion or at least guiding it to a conclusion favoured by the Bureau. At still other times, the Bureau seems to have dropped any pretense of a desire to receive public comment regarding an issue and has responded directly to critics inside and outside the government as to what it thinks the answer is or should be. Finally, in addition to these mixed messages and multiple aims, it also reads like a trial balloon for future amendments being considered by the Bureau. For this reason, perhaps more than any other, practitioners should pay close attention to data protection developments in Japan over the next 12 months.

WHAT THE ISSUE PAPER SAYS

What follows is my summary of the many issues raised by the Bureau in the paper. For those issues that I felt read more like policy statements or were phrased rhetorically, I have tried to capture that nuance in my summary:

1. Provide comments on the fact that while some businesses have taken compliance with the PIPL very seriously, other businesses have failed to take sufficient measures. In addition, provide comments on the fact that because some small and medium-sized businesses are not subject to the PIPL, they are lagging in their efforts to protect data.

2. Provide comments on the so-called over-reaction by some businesses in their attempt to comply with the PIPL and whether the Bureau needs to clarify when personal information may be disclosed to third parties[2] as well as on the perceived burdens and obstacles faced by businesses publishing directories in obtaining consent from individuals.[3]

3. Comment on whether Japan should amend its definition of personal information to be consistent with the international view contained within the OECD guidelines that defines personal information to "mean any information relating to an identified or identifiable individual…"[4] Furthermore, provide comments on whether in light of the nature or the intended uses of personal data, whether stricter measures and rules should apply.

4. Comment on whether resident associations, alumni associations or businesses with fewer than 5,000 individual records should be relieved from complying with the PIPL.

5. Comment on whether interpretation of the PIPL should be made consistent with the predominant practices of business. And comment on whether some differences in interpretation, meaning an application among the 34 different guidelines covering 22 industrial sectors released by Japanese ministries is inevitable, but whether there are some areas of these guidelines that could be standardised and made consistent from one guideline to the next.

6. Comment on whether adhering to a privacy mark certification programme helps businesses protect personal information. And comment on the perception that small and medium-sized businesses are burdened by information management costs associated with complying with the PIPL.

7. Comment on whether direct mail marketing campaigns used by businesses have been made more difficult under the PIPL. Also, what additional measures might be taken to prevent the misuse of personal information aside from the prohibitions currently provided in the PIPL?

8. Although the level of security demanded by society changes overtime, what level of data security should be implemented by businesses? Moreover, considering that security risks faced by businesses vary, should the security measures employed by a business meet the specific risk faced?

9. Although small and medium-sized businesses may not have the same resources as larger businesses to sufficiently manage and secure personal data, isn't it important that such businesses nevertheless improve their data security procedures?[5]

10. Comment on the perception by some that attempts by businesses to increase the protection of personal information in those areas where the security risk is particularly high have resulted in excessive burdens being placed on employees. Provide comments on employee video monitoring and the appropriate manner by which a business might implement such monitoring. Also comment on the appropriateness of the practice of including in employee pledges to protect personal information protection pledges to protect company trade secrets and provisions subjecting employees to damages for any breach.

11. Provide comments on the fact that security obligations placed on delegatees and sub-contractors handling personal data are being strengthened and increased. Also, comment on whether the outsourcing of data to a delegatee should be made more transparent to the data subject.[6]

12. Comment on whether businesses should be allowed to handle personal data obtained through publicly available directories separately from other personal data that they hold?

13. Comment on whether amendments to the PIPL are needed to prevent the scope of use of personal information from expanding in cases of delegation to a subcontractor, merger or joint use?

14. Comment on the perception of some businesses that the level of specificity required when disclosing a business's purpose for use is excessive.[7]

15. Comment on the opinion of some that businesses should be required to disclose to data subjects their sources of personal information. Because the apprehension of data subjects will likely not be dispelled, should not businesses generally disclose in their privacy policies the sources of held personal data?

16. Currently, under the PIPL, individuals may only demand the cessation of use or deletion of their data in cases when data is improperly obtained or illegally used. Is the scope of this right appropriate?

17. Should approved personal information protection organisations be empowered to provide guidance and recommendations to (member) businesses in the case of, for example, data leakage or other violations?

18. Comment on whether Japan should have a more global perspective in how it protects personal information so as to make its system compatible with other systems around the world. Also, comment on the lack of any rules in the PIPL regarding cross-border transfer of data, which is different to the laws of most countries.

19. Comment on whether it is necessary to establish a neutral, independent data protection agency separate from the current competent ministry system as is the case in other countries around the world.

20. Provide comments on the fact that the PIPL does not generally protect the personal information of deceased individuals.[8]

As can be seen from the above, the paper covers a broad range of issues, including several that stand out as particularly concerning, which I turn to next.

Definition of personal information

The first issue that stood out to me was the possible expansion of the definition of personal information to include information that relates to an "identifiable" individual. Currently, the PIPL provides that personal information means information about a living individual that can identify the specific individual by name, date of birth or other description contained in such information (including such information as will allow easy reference to other information and will thereby enable the identification of the specific individual). By adding the portion from the OECD definition to include information "relating to an identified or identifiable individual" the definition of the PIPL would be expanded, but it is arguable whether any such amendment would make the meaning of personal information any clearer for businesses to bring their practices into compliance or provide any additional protection to individuals.

Even if information on its own does not identify an individual, if it can be combined with other information accessible by the data controller, all such data falls within the scope of personal information. As a result, information that relates to an "identifiable" individual is likely already subject to the PIPL in most cases.

Standardisation among guidelines

A second concern is the paper's fatalistic comment that conflicting obligations between ministry guidelines might be inevitable and irresolvable. While there are likely high structural and political hurdles to overcome in trying to get the various ministries to agree to a common interpretation of important concepts and obligations under the PIPL, the belief that such hurdles can never be overcome, or are not worth trying to overcome, places the cost of this political disagreement on businesses.

Identity of delegatees

A third concern is the possibility that companies may have to disclose delegatee and outsourcing subcontractors. Currently, under the exceptions provided in Article 23 of the PIPL, a business may delegate data processing activities to a service provider without the consent of or notice to the data subject. For many global multinationals, it may not be possible to stay on top of and disclose in a privacy statement, on an ever-changing basis, the identity of every delegatee. The obligation that businesses disclose the identity of service providers might also provide a powerful tool to protectionists masquerading under the guise of data protection by labeling companies that outsource data overseas as less trustworthy.

Source of personal information

A fourth concern that stands out is the possibility that businesses might be required to disclose to data subjects the sources of their personal information. The Bureau also seems to half conclude that by disclosing the source of data, the apprehension of data subjects regarding the collection of their data will be reduced. But business may fear reprisals from customers for having shared data or for having been the source of data, legitimately shared, and this may lead to businesses becoming more hesitant to share data, which will unnecessarily restrict the flow of information and data.

Cross-border transfers

A final concern raised by the paper is the prospect of restrictions being placed on cross-border transfers of personal data. The PIPL currently does not place any restriction on cross-border transfers of data. Instead, it requires businesses to obtain the consent (including opt-out consent) of data subjects before any personal data is disclosed to a third party, which includes any third party other than a delegatee, a merging company or a "joint user". Instead of viewing data transfers myopically by focusing on the geography of the parties, the PIPL, rightly in my opinion, focuses on obtaining consent from the data subject regarding the transfer. Hence, in exchange for not having restrictions on cross-border transfers, Japanese businesses are required to obtain consent from individuals prior to the transfer. If the PIPL were to be amended to include restrictions on cross-border

APEC puts emphasis on binding corporate rules

APEC's Privacy Sub-group met in Canberra, Australia, on 24 and 25 January. The question remains whether it can encourage the 21 member countries to do anything productive about privacy protection. **Graham Greenleaf** reports.

Australia hosts Asia-Pacific Economic Cooperation (APEC) in 2007, so the first meeting of APEC's Privacy Sub-group of the Electronic Commerce Steering Group (ECSG) was held in Canberra on 24-25 January, following a two-day seminar open to business and other groups. Colin Minihan of the Australian Attorney-General's Department was elected Chair of the Sub-group. It will next meet in Cairns, Australia, in June, at the same time as the second Senior Officers Meeting (SOM II).

The outcomes of the closed meeting of the sub-group are not yet available, but it is noteworthy that representatives of almost all 21 APEC economies attended the meeting and, to a large extent, the preceding seminar. This APEC process retains the potential to engage the attention of Asia-Pacific government representatives on privacy issues three times per year.

The seminar was the First Technical Assistance Seminar on International Implementation of the APEC Privacy Framework, entitled "Creating Trust in developing Cross-Border Privacy Rules: Making Compliance Possible and Enforcement Credible when Personal Information Moves between Economies". The seminar agenda (available from webpage www.ag.gov.au/apec_privacy), papers and discussion, suggests that the principal agenda of APEC on privacy, at least for 2007, concerns the development of "cross-border privacy rules" (CBPRs). There seems to be relatively little attention being paid to the development of privacy legislation in APEC economies.

This approach originates from a concept paper put to the Privacy Sub-group at its meetings in Vietnam in 2006 by the Cross-Border Rules Study Group (Australia, Korea, Mexico, the United States and the International Chamber of Commerce), which proposed development of a Cross-Border Rules Implementation and Operating System (CBRIOS). The paper noted that "development of CBPRs has been one of the ECSG Data Privacy Subgroup's principal work items in 2006 and, together with cross-border information sharing and enforcement cooperation issues, will be the principal focus of this Subgroup in 2007."

At the 2007 seminar, a paper by the consultants on the development of CBPRs (led by former Australian Privacy Commissioner Malcolm Crompton), defined CBPRs. It read: "Cross-border privacy rules means a set of rules developed by an organisation that is a personal information controller that relate to the handling of personal information transferred across borders and that the organisation commits to apply in its activities involving transfers of personal information across borders."

CBPRs are a particular form of binding corporate rules aimed at ensuring consistent handling of personal information in activities across more than one economy. In the APEC context they are aimed particularly at companies that operate in economies which protect privacy in very different ways. Four elements of CBPRs were identified: self-assessment; compliance review; recognition/acceptance; and dispute resolution/enforcement. The third element requires that "some form of status needs to be given by economies to CBPRs that have undergone review". How this can be done depends on the legal and administrative environment in each economy. The expectation stated at the seminar was that only a number of APEC economies would be in a position to work on developing CBPRs to start with, and probably only in relation to some parts of their business sector.

The next issue of *PL&B International* will include a more detailed explanation of CBPRs and how the Privacy Sub-group is proposing to advance their use within APEC.

AUTHOR

Graham Greenleaf is PL&B International Newsletter's Asia-Pacific Editor and Co-Director, Cyberspace Law & Policy Centre, Faculty of Law, University of New South Wales,
e-mail: graham@austlii.edu.au

Enforcement under Hong Kong's Ordinance

Enforcement of Hong Kong's Personal Data (Privacy) Ordinance is becoming much more visible under new Commissioner Roderick Woo (*PL&B International Newsletter*, October 2006, pp.10-13). Three new cases highlight this trend.

TELECOMS COMPANY FINED FOR 'OPT-OUT' FAILURES

A telecommunications company was convicted in Kwun Tong Magistrates Courts on 17 January 2007 of breaching s34(ii) of the Ordinance. Four summonses were laid against the company for contravening s34(ii) of the Ordinance, which requires data users to cease further contact with the individual if he chooses to opt-out. The company pleaded guilty to all summonses and was fined HK$14,000.

It began contacting the complainant by phone to promote its IDD services in July 2005. The complainant asked the company several times to stop calling him for direct marketing purposes but they failed to do so. In July 2006, after investigation of the complaint, the Commissioner's office issued a written warning to the company requiring it to cease making direct marketing calls to the complainant. But in August 2006, the complainant received at least four marketing calls from the company.

The magistrate, Mr Chan Yan-tong, remarked that such direct marketing calls were "disgusting and annoying". Privacy Commissioner Roderick Woo, said, "I concur with the magistrate that the general public will not tolerate breaches … which may cause nuisance to their daily life." In response to magistrate Chan's comment that the maximum penalty of HK$10,000 hardly acted as a deterrent for large organisations, Mr Woo said his office was reviewing the adequacy of penalties as part of a broader review of the Ordinance, and that he would consider consulting the public on penalties.

DEBT COLLECTOR FINED HK$5,000

On 27 December 2006, a debt collection agent was convicted of an offence under s64(7) of the Ordinance for contravening an enforcement notice (EN) issued by the Commissioner and was fined HK$5,000. The complainant was the referee of a debtor who had borrowed money from a financial institution which appointed the agent to recover the debt. In doing so, the agent posted notices containing the complainant's name in public places. The Commissioner considered that this was a contravention of Data Protection Principle 3, which stipulates that personal data shall not be used for a purpose other than its original purpose of collection or a directly related purpose unless it is done with the prescribed consent of the data subject.

The Commissioner commented that "a debt collector should only use personal data of the referee in locating the whereabouts of the debtor rather than exerting pressure on the referee to repay the debt".

After investigation, the Privacy Commissioner served the EN on the Agent in June 2006. The agent's failure to respond contravened s64(7), so the case was referred to the police for prosecution against the agent. The agent entered a plea of guilty at Tsuen Wan Magistrates Court on 27 December 2006 and was fined HK$5,000.

ENFORCEMENT NOTICE AGAINST CATHAY PACIFIC

Hong Kong's Privacy Commissioner served an Enforcement Notice on Cathay Pacific Airways Limited on 18 January 2007 for contravention of the collection principles of the Ordinance, directing it to take steps to remedy the contravention and/or matters occasioning it. In response to a press release by Cathay about the matter, the Commissioner has confirmed that he carried out an investigation in March 2006 concerning Cathay's collection of medical data from its employees, and that it has been advised of its rights to appeal to the Administrative Appeals Board.

APPA website

The Asia-Pacific Privacy Authorities (APPA) now have a website provided by the Australian Commissioner's office at www.privacy.gov.au/international/appa/index.html.

APPA comprises the privacy authorities of the Hong Kong SAR, Australia, New Zealand and South Korea. The website provides APPA's Statement of Objectives, Statement of Common Administrative Practice on Case Note Citation and Statement of Common Administrative Practice on Case Note Dissemination.

APPA meets twice per year, next in Cairns, Australia, in June 2007 to coincide with the APEC meeting.

Wide review of NZ's privacy laws

New Zealand's Law Commission has started a "review of privacy values, technology change and international trends, and their implications for New Zealand law". The project will proceed, and report, in stages.

In stage 1, now underway, the Commission is undertaking a high-level policy overview to assess privacy values, changes in technology and international trends, and their implications for New Zealand civil, criminal and statute law. It is conducting a survey of these trends in conjunction with the Australian Law Reform Commission.

Stage 2 will consider whether the law relating to public registers requires systematic alteration as a result of privacy considerations and emerging technology.

Stage 3 will cover both the adequacy of New Zealand's civil law remedies for invasions of privacy, including tortious and equitable remedies and the adequacy of New Zealand's criminal law to deal with invasions of privacy.

Finally, in stage 4 the Commission will review NZ's Privacy Act 1993 to update it.

Australia's ID Card Bill: Function creep guaranteed

Graham Greenleaf takes a critical look at Australia's ID Card Bill, introduced into the legislature this month.

Australia's Federal Government introduced the Human Services (Enhanced Service Delivery) Bill 2007 on 7 February 2007 to establish its "access card" ID system. It goes to a Senate Committee for investigation and report in five weeks. The Bill is only half of the blueprint for the ID system, the other half is to come in a Bill not yet seen. The Bill is contentious and its passage not a certainty. Four Federal Government MPs have publicly raised doubts about it. One former Minister says, "It fails the Nazi test." The Labor opposition is posing criticisms but not yet declaring outright opposition. A draft Bill received over 100 submissions, including a very critical one from the government's own Consumer and Privacy Taskforce. The following points summarise critically some of the Bill's more important or objectionable aspects.

The legislative framework (Bill No 1). The Bill's objects state that "access cards are not to be used as, and do not become, national identity cards" (which are undefined), but incongruously that they are also objects "to permit access card owners to use their access cards for such other lawful purposes as they choose".

To obtain a card, anyone who is eligible for a Commonwealth benefit (almost everyone over 18 years of age) must apply to the Secretary of the Department of Human Services for inclusion on the Register. He has discretions to determine what particulars and supporting documents they must provide that are not disallowable by Parliament, thereby allowing function creep. Among other things, the Register will contain a card holder's names ("legal", "preferred" and aliases), date of birth, date of death, Australian citizenship or resident status, indigenous status, sex, contact details, registration status (suspended or cancelled, "full" or "interim" proof of identity), everything that appears on the face of the card (see below), and a "numerical template" of the photo on the card. It will also include copies of any documents that a person has produced to prove their identity (called POI), that the Secretary so chooses. The Register's potential as a honeypot for ID fraud and privacy invasion therefore remains. Ministerial decisions about extra content that can be added are disallowable.

The card surface will contain the cardholder's name ("legal" or "preferred"), unique card number, card expiry date, photograph, digitised signature and various benefit-related items. These details can only be changed by legislation. The Taskforce criticised the voluntary inclusion of date of birth because it "devalues the security protection of the card and materially enhances the opportunities for fraud and identity theft". The probability of the card turning into a national ID card is also enhanced. The Minister can change the name of the card (initially the Health and Social Services Access Card) without Parliamentary scrutiny.

This Bill only defines what is in the Commonwealth's area of the chip, but not in the card-holder-controlled area, so many dangers remain unknown. The Commonwealth's area will include everything on the surface of the card plus a lot more, including a person's "legal name" (protected by their PIN), sex, residential address, any PIN or password ("protected by encryption or other technological protection measure"), benefit information, and whether the person's POI is "full" or "interim". The potential for function creep in the government's part of the chip is as dangerous as it is for the Register, because the Secretary has the same unchecked discretions.

The Bill facilitates a wide range of uses of the card while maintaining the pretence that such uses will be voluntary. Card holders are expressly entitled to use the card (defined to include the chip) "for any lawful purpose", so no use of the card is unlawful unless legislation makes it so. Six defined "participating agencies" are only entitled to use the card for the purposes of this Act, or with the card-holder's consent.

Other organisations do not face such express restrictions. It is an offence to require a person to produce their card for identification purposes or in connection with the provision of a widely defined list of benefits, and an attempt is made to prevent implied requirements. But the offences are excessively complex and beg the question why the Bill does not simply prohibit requirements to produce a card for any other purpose than those expressly allowed? An astonishing loophole is that the Crown (in all Australian jurisdictions) is purportedly bound by the Act but is in fact immune from prosecution for any offence under it, leaving card holders defenceless against wrongful demands for production by the Crown. These offences can easily be sidestepped in any event, simply be refusals to accept successively proffered items of identification until a person "voluntarily" produces their "access card" in desperation – "pseudo-voluntary production".

If a person produces their card, it is an offence to copy or record the number, photograph or signature on the surface of the card, but the protection can be avoided by standard forms providing consent. There is no offence in relation to copying any information in the chip. The question of who can read what information on the chip is thus crucial but unanswered. The government is immune from prosecution in any event.

The worst is yet to come in Bill No 2. Who can challenge the refusal or cancellation of a card? Which agencies will have access to the Register? Will individuals know who has access to

Continued on p.17

German court says customers have right to deletion of IP logs

The Supreme Court in Germany has ruled that internet service providers (ISPs) must delete customer logs when asked to by a user. A German citizen, Holger Voss, wanted to have his internet usage records deleted. He had been sued unsuccessfully over comments he made in an internet forum in 2002, accused of glorifying a criminal act, the terrorist attacks in the US on 11 September 2001. He said that his comments were heavily sarcastic, and then took a separate case against his ISP, T-Online, alleging that its retention of his dynamic IP address and handing over of information about the address and its use to German authorities were illegal. The ruling means that German ISPs will have to delete internet usage records, called IP logs, when customers requests it.

The EU Data Retention Directive, approved by the European Parliament in February 2006, requires member states to adopt laws requiring ISPs and phone companies to keep information for a period between six months and two years, with each country choosing its time period.

Governments and security agencies generally want ISPs to keep records for as long as possible so that the activities of users are recorded and retrievable for use as evidence.

The records kept relate only to the time of communications and the identity of the caller, not the content of communications. Germany has not yet legislated in compliance with the Directive, but when it does the legislation will conflict with this court ruling. (www.out-law.com).

Continued from p.16

their records? Will individuals be able to access what the Register says about them? How will the card number be determined? What will be on the card holder's area of the chip? Who can read what information is on the chip? All of these questions remain unanswered.

There is little to distinguish the "access card" scheme in this Bill from the rejected Australia Card of the 1980s, except that it is far more dangerous than that primitive proposal. This is a national ID system with no meaningful protections, being put beyond Parliamentary control.

• *This is an abbreviated version of a more detailed paper available at www.cyberlawcentre.org/privacy/id_card.*

REFERENCES

1. Greenleaf, G. 2006b, Australia's Proposed ID Card: *Still Quacking Like A Duck*, Computer Law & Security Report, Vol. 23, 2007; UNSW Law Research Paper No. 2007-1, at http://papers.ssrn.com/sol3/papers.cfm? abstract_id=951358
2. Greenleaf, G. 2006b, *Quacking like a duck: The national ID Card proposal (2006) compared with the Australia Card (1986-87)*, 12 June 2006, see www.cyberlawcentre.org/privacy/id_card/OzCard_comparison.pdf.
3. Human Services (Enhanced Service Delivery) Bill 2007, at http://parlinfoweb.aph.gov.au/piweb/view_document.aspx?ID=2450&TABLE=BILLS.
4. Taskforce 2007 Consumer And Privacy Taskforce Submission To The Department Of Human Services Human Services (Enhanced Service Delivery) Bill 2007 Exposure Draft, January 2007.

Continued from p.13

transfers, the current, carefully crafted balance might be undermined and businesses may find it even harder to transfer data in and out of Japan because of the extra cross-border hurdle being placed in front of them.

Conclusion

Whether and how the PIPL will be amended is, at this point, unanswerable by anyone outside of the Bureau or the Cabinet, but any movements to amend the PIPL should be closely watched by businesses and practitioners alike.

AUTHOR

David E. Case is an Attorney at White & Case LLP, Tokyo
E-mail: DCase@tokyo.whitecase.com

REFERENCES

1. www.cao.go.jp/seikatsu/kojin/index.html (no English translation available).
2. The most frequently cited example was the refusal by some hospitals to release information to relatives inquiring whether loved ones were hospitalised after a large train crash shortly after the PIPL went into effect.
3. In relation to this issue, the Bureau inserted a commentary note that the issue of individuals refusing to consent to being included in directories may not be a problem with the PIPL so much as a heightened sense of privacy now held by individuals and that individuals should be informed about opt-out procedures to resolve this issue.
4. Currently, Article 2 of the PIPL defines personal information to mean "information about a living individual that can identify the specific individual by name, date of birth or other description contained in such information (including such information as will allow easy reference to other information and will thereby enable the identification of the specific individual)".
5. The Issue Paper further queried whether greater government involvement in training was necessary to support the efforts of businesses in light of Japan's strong national policy on information security and whether within "information security management systems", there might not be some way to increase the overall level of security.
6. Currently, under the PIPL there is no obligation to disclose the identity of outsourcing delegatees to the data subject.
7. The Bureau then commented that because the PIPL provides that the purpose of use must be described as concretely as possible, shouldn't businesses' attitudes towards specifying its purposes be improved (instead of the law).
8. Unlisted here were a few more issues regarding the personal information practices of local and regional governments in Japan.

Information security versus DP

Privacy by design minimises the data set. By **Jan Willem Broekema**.

Article 17.1 of the EU Data Protection Directive, on security of processing, says: "Member States shall provide that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access..."

In a hospital, for example, sensitive personal (medical) information is processed. People tend to trust hospitals and their staff because medical staff have their own professional code of conduct. Your medical care is dependent on people having access to the data. However, not all people in a hospital are medical staff. Should the financial department have access to your records? Of course they should have access, otherwise they would be unable to send invoices. But should the doctor have access to details like your financial status and the bookkeeping department to your medical records?

This is where the Directive states that the controller (the hospital) should take the necessary steps to ensure the prevention of "unauthorised disclosure or access". We can set rules that prevent even physicians from having access to those parts of the record that have no information relevant to their profession or to records of patients that are not in their care. A tracking mechanism, an audit trail, in the design might help to counter unauthorised access.

Then there is the patient (the data subject). They have, the Directive says, the right to access to all relevant information about them. The hospital system should allow a patient access to their address record, financial status and medical records, not necessarily within one system but the information should be accessible. Other questions need to be addressed too. Medical records may also include (personal) information on the medical staff, for example which nurse or orderly did what, when, why and, last but not least, authorised by whom?

The example shows that the protection of personal data is far more complex than a system of user names and passwords.

Information security is normally set up by an organisation to protect its assets because of a fear of the loss or corruption of business information. Any organisation should be aware of losing sensitive information to competitors, and business continuity may be compromised if information held by the organisation is unreliable. That may lead to liability for non-delivery of goods, services or payments.

Data protection, here understood as protection of personal data, is something any organisation should undertake in the interest of the data subjects. It is the protection of the personal sphere of your client, prospect, patient, citizen or, as the Directive states, the protection of the rights and freedoms of individuals, and in particular the right to privacy. While information security is something that is primarily being put in place for "the inside" of the organisation, data protection is aimed at the protection of "the outside".

Information security and data protection have things in common but are not identical. In a case in which information security is breached, the reactions of outsiders will be about the company involved. But if personal data is corrupted or stolen or used in an inappropriate way, people will be outraged. Both information security and data protection will, at least in an environment of information and communications technology, rely on the same (technical and procedural) principles.

It is sometimes very hard to get the message across in the boardroom. In the EU at least, and in more and more other countries, business has a legal obligation to protect personal information.

Chief privacy officers (CPOs) may play different roles in different companies. They can form the complaints office, where clients and employees can ask about the processing of their personal data. They may have a role to play in alternative dispute resolutions on privacy matters.

On a more strategic level, the CPO will be able to prescribe the manner in which the company should handle the processing of personal data. Such prescriptions may lead to (internal or external binding) codes of conduct for a company or group of companies, as part of the set of common business principles. The privacy officer might also check on the processing in design and development phases, in the "Privacy by Design" model.

In each case it must be obvious that, while the privacy and the security officer do share a playing field, they are not to be confused.

To sum up the two main issues addressed here: privacy is not data protection. Privacy is a wide concept, of which informational privacy is but a subset. In the European Union, the DP directive is all about the processing of personal data, about informational privacy. Data protection is, in this setting, the whole of procedures and processes in place to prevent the processing of personal data without proper safeguards for the person concerned.

Also, data protection is not information security. We should never forget that, while trying to make a distinction, we must not create false boundaries. "The outside" works with "the inside" because there is trust, trust that information will be used according to good entrepreneurship. If you fail in your data protection, you lose trust. "Privacy by design" promotes minimalisation of the data set, anonymisation wherever possible and reduction of long storage. Information security is the set of procedures to facilitate, among other things, personal data protection, which then becomes a target of information security measures.

In the EU and in more jurisdictions around the world, the processing of personal data is being limited by law. Collection, storage and further use of personal data are off limits by law unless you meet some minimum safeguards for the data subject. Information security specialists and their managers have a pivotal role to play in the future.

AUTHOR

Dr Jan Willem Broekema is ex-DP Commissioner of the Netherlands
A longer version of this article is available by e-mailing glenn@privacylaws.com

Do you really want to tell your customers you lost their data?

An EU proposal on data breach notification would mean that network providers and internet service providers would, in future, have to inform their regulators of any privacy incidents that put personal data at risk. **Laura Linkomies** reports.

The Review of the EU Regulatory Framework for electronic communications networks and services (COM(2006) 334 final) includes a small but interesting paragraph on security. It includes a proposal to make providers of electronic networks responsible for notifying their data breaches. The Commission would oblige service providers to notify the national regulatory authorities (NRAs) of security breaches that have led to the loss of personal data. The NRAs would also have the opportunity to inform the public if they considered that it was in the public interest. Customers could be informed of a breach of security that has led to the loss, modification or destruction of, or unauthorised access to, their personal data.

This Communication and the accompanying Staff Working Document, published in June 2006, launched a public consultation which ran until the end of October 2006. The Commission received more than 200 responses, some of which supported the idea as a means to enhance security. However, when talking about data breach notification, emotions run high.

Industry views

A random selection of three responses makes clear that telecommunications firms and network operators do not welcome the idea of notifying the regulatory authorities or customers. Ericsson, the Swedish telecoms giant, says that the Commission's proposal should be reconsidered. "The Data Protection and e-Privacy Directive already govern this issue, and notification requirements may divulge vulnerabilities which could lead to new security risks," the company says.

BT does not agree with the idea either: "It is not clear what would constitute a breach of security for these purposes. Nor is it clear what would be the test of the public interest. Disclosure of a breach could lead to further breaches or damage. If no observable harm were sustained as the result of a breach, notification 'for notification's sake' would erode rather than sustain confidence and provide no meaningful benefit."

> "It is not clear what would constitute a breach of security for these purposes. Nor is it clear what would be the test of the public interest. Disclosure of a breach could lead to further breaches or damage"

Portugal Telecom observes that "the measures that the Commission is proposing will represent a burdensome obligation on operators … current data protection regulations already impose on operators specific obligations related to security processes and systems. Therefore we do not see how the measures proposed by the Commission will result in an improvement of security standards."

The European Internet Service Providers Association (EuroISPA), which represents more than 900 ISPs across the EU, says that breach notification provisions should be considered as part of a review of the Data Protection Directive, where they would be accurately targeted at all data controllers. In its response to the Commission consultation, EuroISPA accepts that ISPs are responsible for the security of their customers. They need to ensure that the security of the transmission is not compromised and that their subscriber databases are safe.

EuroISPA states that "before moving ahead with any legislation in this field, the Commission should investigate whether there is any evidence that there is any significant level of incidences of security breaches of network infrastructure leading to the loss of personal data that would demand a regulatory response. Should any breach notification regime be implemented in Europe it must be done in a harmonised manner, be technologically neutral, limited to narrow circumstances in which there is a significant risk of harm from financial fraud, and be open and flexible."

Furthermore, EuroISPA stresses that website operators are not public electronic communications network providers and are rarely public electronic communications service providers, so they would not be caught by the scope of the legislation. Accordingly, the provisions on notifications of security breaches are mis-targeted at ISPs out of a misunderstanding of their role in the field of communications.

Why now and why ISPs?

Can we assume that ISPs have experienced more data breaches than organisations in other industries? Or is the Commission planning to introduce data breach notification rules more widely, and just thought that ISPs are a suitable place to start?

There is no official wisdom on this but the example of the US must have had an impact, especially California's Security Breach Information Act 2003 (see *PL&B International*, February 2006, pp.29-30).

Although its aim is to prevent identity theft, the Commission's basic idea of informing individuals is the same.

The European Commission has decided to introduce the new measures for network operators because it sees that ISPs carry an extra responsibility: "Network operators and ISPs, as the gatekeepers for users' access to the online world, carry a special responsibility … A requirement to notify security breaches would create an incentive for providers to invest in security but without micro-managing their security policies," its communication says.

Professor Dr Ian Walden, a consultant at law firm Baker & McKenzie and a member of the Legal Advisory Board at the Information Society Directorate-General of the European Commission, thinks that notification is a good idea in principle: "I think breach notification is an appropriate regulatory obligation, which recognises that the data processed by an organisation can engage the private interests of individuals, as subjects of the processed data, as well as public interests, which may not coincide with the private interests of the victim organisation. However, it strikes me that imposing obligations on ISPs is hitting the wrong target. Although ISPs are the gatekeepers in terms of access, there is no evidence I have seen that suggests they are subject to more security breaches than those that provide other 'information society services' such as electronic commerce websites, for example internet banks, etc."

The EU Art.29 Data Protection Working Party, which consists of EU Privacy Commissioners, welcomes the proposal but has pointed out that the plans do not envisage any sanctions if a network operator or ISP fails to inform the NRA. The group also stresses that none of the major security breaches of the recent past, such as Choicepoint, LexisNexis, Bank of America, Time Warner, involved ISPs. The group has, in fact, suggested that notification duty should also be considered for data brokers, banks or other online service providers.

Finally, the Commissioners propose that data breach rules should classify different levels of breaches and require that all customers be informed at the time of a breach.

Is this needed?

Evidently, if customers are notified that their sensitive personal information has been leaked, they can monitor their accounts and possibly correct any damage done. However, due to issues with enforcement, is this too much of a burden for companies? One would hope that reputable companies inform their customers anyway of any data breaches. For example, in the UK, banks that have leaked personal data have claimed to inform all customers concerned. Also, in the US, many financial institutions have notification systems in place. Discussions in the US Congress, which has seen numerous data breach Bills, have not centred on whether notification is worthwhile but on how to build up an effective notification system.

Francis Aldhouse, consultant at law firm Bird & Bird and previously the UK's Deputy Information Commissioner, says that although the Commission proposal is welcome, it is discriminatory in applying only to the telecommunications industry, and that the experience of the US is that the bigger problem is in other businesses, such as financial services: "Any European legislation should learn from the US experience. The duty to notify can be subject to exemptions, such as where the data are strongly encrypted and there is minimal risk to individuals. Such an arrangement provides an incentive to business to implement technical security measures, but it is clearly a stronger incentive if the duty is to notify all individuals rather than just a national regulator."

What do the EU privacy directives say?

Currently, the e-Privacy Directive states that providers of a publicly available communications services must take appropriate technical and organisational safeguards to ensure the security of their services (Article 4). In some EU Member States, there are specific requirements as to the appropriate technical and organisational measures. However, in many others there are not. And importantly, while the directive requires notification of any security *risks*, there is no obligation to notify about actual security *breaches*, such as loss of personal data.

The Commission now proposes that such clarification should be offered. Companies could be asked to include, in their consumer contracts, a clause that would specify how they would address a security threat or incident.

The general EU Data Protection Directive obliges organisations to take measures to protect data against loss, alteration and unauthorised disclosure or access. The Directive also provides for compensation for damages in case there has been a breach of security.

Conclusion

The Commission will report on the public consultation during June/July 2007 and possibly publish draft legislation. It is expected that any new measures would be implemented during 2009-10. It is possible that the changes would mean amending the e-Privacy Directive. However, as data breach notification is just a small part of the revision of several Directives that affect the telecommunications network, it is too early to say yet where the changes will be made.

Professor Walden thinks that data breach notification is likely to be considered as a policy initiative in other areas over the coming years, depending in part on how successful it is perceived to be. There are several problems, though. Companies would incur an extra cost no matter in which form or to whom the notification would be made. Other problems include ensuring compliance and deciding on remedies for non-compliance. Also, on whom should the obligation to notify be placed?

AUTHOR

Laura Linkomies is Editor of PL&B's UK Newsletter.
E-mail: laura@privacylaws.com

FURTHER INFORMATION

The staff working document, which expands on the EU Communication, can be found at http://europa.eu.int/information_society/policy/ecomm/doc/info_centre/public_consult/review/staffworkingdocument_final.pdf.

The consultation responses can be seen at http://ec.europa.eu./information_society/policy/ecomm/info_centre/documentation/public_consult/review_2/index_en.htm.

Data breaches spark new forms of insurance coverage

The spiralling number of high-visibility data breaches has prompted some insurers to offer innovative coverage aimed at helping businesses cope with network and privacy breach liabilities. The question is: Will they buy it? **Dugie Standeford** reports.

When news of the TJX Companies data security breach broke in January, Texas law firm Scott & Scott LLP took the opportunity to remind businesses that "there is no such thing as a completely secure network". Instead, it warned, companies must put proactive processes and controls in place to "minimise the risks of legal liability and damage to the corporate brand as a result of a data security breach".

Alongside the usual litany of technical and administrative security measures, the firm recommended that businesses explore network security insurance coverage on offer by "forward-looking" providers. Although it is a new form of insurance, a range of coverage is available, including inside job, service provider, employee claimant, regulatory and third-party handling, says partner Robert J. Scott of the software compliance practice group.

The average costs associated with a data intrusion can exceed $10 million in expenses, services to customers and legal fees, Scott says – not to mention the incalculable costs of harm to the corporate brand. Since 2005, US businesses and government agencies have seen more than 100 million consumers compromised because of lost or stolen data, at an estimated cost per person of $180. Insurance can "go a long way towards helping to mitigate these costs", Scott says.

But traditional insurance is not designed to cover the specific damages corporate security failures cause, such as protection for privacy-related risks, the financial impact of complying with breach notification laws, or issues related to government data compliance regulations that penalise firms that cannot effectively defend their information, Scott says.

Privacy and network-security coverage merging

When the internet took off around five years ago, the business community awoke to the fact that it had exposures not covered by traditional insurance, says Nancy Callahan, Vice-President of the American International Group, Inc. (AIG) identity theft and fraud division. Recognising that commerce had moved online, AIG pioneered "cyberliability" and network security insurance to protect the new electronic dependencies between companies. Those years also saw the evolution of ID theft from the consumer perspective, and AIG created new coverage for that as well.

Since then, consumer concerns over ID theft and business network security fears have merged, Callahan says. Some 35 US states have enacted data breach notification laws to help consumers better manage risk, but the business community is just coming to grips with the consequences of mandatory notification, she says. There is also a growing belief that companies should help consumers manage the threat of ID theft. And firms are coming to realise they could be subject to oversight from state attorneys-general as well as to civil liability from lawsuits.

In response, AIG developed a suite of products aimed at companies that hold personal information on customers and staff. "Security and privacy insurance" policies address consequences of data breaches arising, for example, from stolen laptops or thieving employees as well as from technological or system risks that compromise personal information, Callahan says. There is a policy for small and mid-size enterprises and one for larger companies or those with more complex information management issues. Limits range from up to $5,000,000 for the former to as high as $25,000,000 for the latter.

Both policies pay for claims arising from data breach, legal fees from regulatory actions, and crisis management costs – lawyers, public relations consultants, notification costs and customer access to credit counsellors.

Industry slow to adopt

The highly-monitored financial and health industries were the first to buy into such coverage, Callahan says: "The interest follows where the regulatory actions have taken place." Now, the emergence of state and, possibly, federal breach notification laws and the Federal Trade Commission's beefed-up anti-ID theft activities are driving takeup of the policies among other sectors. Firms at the heart of the information society – websites, portals, e-commerce firms and the like – are also more likely purchasers, she says. However, AIG's products are not currently available in Europe.

"In the privacy area, takeup is still in growth stages," Callahan says. The coverage is still viewed as a "discretionary buy".

"Executives are embracing this with more fervour than in years past," says Scott, but they continue to take reactive, rather than proactive steps to protect their enterprises. He adds: "As we continue to see more advanced attacks on corporate networks, such as the recent T.J. Maxx incident, I think businesses will begin to take advantage of the insurance options being made available to them."

AUTHOR

Dugie Standeford is a freelance journalist.

Privacy laws 1987-2007 and beyond

James Michael and **Stewart Dresner** put some questions about data protection, past and future, to several of the international authorities on the subject who have been involved in it for at least 20 years, all of whom have spoken at PL&B conferences.

Here are the responses of Francis Aldhouse, former United Kingdom Deputy Information Commissioner and currently consultant solicitor at Bird & Bird; Peter Blume, Professor of Information Technology Law, University of Copenhagen; Dr David Flaherty, consultant and former Information and Privacy Commissioner, British Columbia, Canada; Masao Horibe, Professor of Law, Chuo Law School; and Peter Hustinx, European Data Protection Supervisor.

1. Twenty years ago, would you have predicted that data protection legislation has grown and spread as much as it has? Has the growth been more or less than you anticipated?

Peter Blume: First, my congratulations to Stewart and all the people who are or have been associated with PL&B during the first 20 years. Reading this newsletter is one of the best ways to keep up to date with the ever developing world of data protection.

The volume of data protection legislation is today much larger than I would have anticipated in 1987. At that time only few countries had comprehensive laws, and although a European Directive was contemplated it was not at all certain that it would become a reality. Outside Europe the situation was even more bleak, and the thought that countries such as Argentina, Australia and Canada would have federal laws was much more a hope than a probability. With respect to growth, these 20 years have been a success for data protection law.

David Flaherty: As a historian, I resist predicting the future, but I am astonished at what big business data protection has become, not only in a business sense, and necessarily so. With more than 40 countries in the data protection fold, it is becoming a global phenomenon, as it needs to be. Advanced industrial countries without robust data protection laws and oversight agencies in place are now at risk of being branded as outlaws.

Masao Horibe: Please accept my sincere congratulations on 20 years of Privacy Laws & Business.

Twenty years ago, there were about 12 countries which enacted data protection acts. While I was writing a book entitled *Privacy in an Advanced Information Society*, which was published in 1988, I had a feeling that ideas of data protection would spread all over the world. The growth has been more than I anticipated because former socialist countries began to make laws in the 1990s and 2000s.

Peter Hustinx: Twenty years ago, the present number of national laws and initiatives around the globe was inconceivable. However, it fully confirms the continued relevance of data protection principles in a world increasingly dependent on widespread use of information and communications technology.

2. How has data protection changed from its international origin in the Council of Europe Convention?

Peter Blume: The centre of data protection has shifted from the Council of Europe to the European Union, but comparing the 1981 convention and the attached recommendations with the directives and connected EU law there are many similarities. Basically, the principles and the general structure of the regulation are the same but due to the legal setup of the EU, it has been possible to make the regulation more comprehensive and detailed. It is mainly in this way that the regulation of data protection has changed.

David Flaherty: I date the origins of fair information practice to the US and the UK in the early 1970s. I prefer to think of the phenomenon as a product of concern for the human rights and dignity of each individual, even though the push for legislation from country specialists and privacy advocates has often masked the human rights concern beneath commercial imperatives for free trade that were more saleable. We will take our legislative victories anywhere that we can find them.

Masao Horibe: There have been some similarities and dissimilarities among data protection laws in the world. Those laws reflect the legal tradition and culture of each country. In some east Asian economies in particular, the system of data protection has changed from its international origin in the Council of Europe Convention.

Peter Hustinx: The origins in the Council of Europe Convention No. 108 and the OECD Guidelines are of similar importance internationally. The Convention has been specified in the EU Directive 95/46 [Recital 11] and the geographical scope of both has increased due to profound changes in the European landscape. The influence of the European model around the world has also been quite considerable. However, more important in my view is the growing emphasis on effective implementation, and inclusion of technological and self-regulatory approaches for better protection. This is necessary and inevitable to make sure that legal principles continue to be a practical reality in a changing world.

3. Are there any countries that you could identify as being particularly effective or ineffective at data protection in the content of the laws themselves, the interpretation of the laws or in law enforcement?

Peter Blume: The world is very differentiated with respect to data protection regulation and enforcement. Some countries, such as the EU Member States, have general and sectoral laws, some countries have only some sectoral laws and others do not have any laws. However, it is very difficult to compare, and it is well known that there is no field of law with so many mistakes as comparative law. I will not pinpoint specific countries as better or worse than others. This is too risky. An example is that the level of sanctions is much higher in southern Europe than in Northern Europe, but this is not a sufficient indication of where data protection is performing best.

David Flaherty: Despite its plethora of specific legislation, the US and its states continue to do a very poor job at implementation because of the lack of institutionalised oversight agencies with an ongoing focus on the articulation of privacy interests at stake in any situation. I favour a generic oversight body rather than the sectoral approach in the US. While Canada is often held up as a model of effective implementation, I am only too aware of how much remains to be done to make privacy rights meaningful for the individual at the federal, provincial and territorial levels. If one looks around the world, the institutionalisation and implementation of privacy rights in most countries are quite weak or non-existent.

Masao Horibe: From the Japanese viewpoint, the data protection laws of many countries which implemented European Union Directive 95/46/EC are effective in terms of rules and law enforcement.

Peter Hustinx: It would not be appropriate or feasible for me to single out individual countries as particularly effective or ineffective. But from my previous reply, it follows that it would be those countries most – or least – successful in creating the crucial mix of elements that is required for making data protection a practical reality.

4. Some countries extend data protection legislation to legal persons as well as natural ones. Do you have a personal opinion about this question?

Peter Blume: Data protection concerns physical persons as they have integrity and a need of privacy. In my opinion, the extension of data protection rules to other entities such as legal persons blur the purpose of the regulation as the reasons for protection are very different. A physical person can feel shame and embarrassment; a legal person cannot. It may in some cases be practical that specific data protection rules also cover legal persons, for example rules on credit reporting, but in general this should not be the case.

David Flaherty: Legal persons, as such, have no moral or ethical claims to privacy rights. Only the people who work there have such rights, and I regard the protection of employee privacy rights as another neglected area of data protection.

Masao Horibe: In the context of human rights, data protection legislation is closely related to the right of privacy and personal data of natural persons.

Peter Hustinx: There are legitimate reasons to include legal persons, but from a practical point of view, it is not a first priority. This is what most countries seem to have concluded. At this point, it is a typical non-issue.

5. What do you think are the most pressing issues in data protection today?

Peter Blume: Although it is tempting to mention international surveillance together with refined and complex new technologies, that is, pervasive computing, as the most pressing issues, I will prefer to focus on somewhat less spectacular issues. First, data sharing within the framework of e-government. Although we have stopped talking of Big Brother, he has not entirely disappeared, and it is a huge risk that e-government will create an environment where personal data are merged in one big database or network, providing the state full knowledge of its citizens, at the same time as processing is not at all transparent. Secondly, increasing the general public's knowledge of data protection. The survival of data protection in the long run depends on real support from citizens. This presupposes knowledge and much more effort should be put into explaining the reasons for and the rules of data protection

David Flaherty: Getting privacy and data protection commissioners, and their staff, to do the jobs they were appointed to do in an expeditious, brave, and articulate way. In this regard, I have very high regard for the current work of the U.K. Information Commissioner and his office.

Masao Horibe: One of the most pressing issues in data protection is how to develop international mechanisms of cross-border enforcement of privacy laws. The OECD Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy will be adopted in spring, 2007.

Peter Hustinx: First of all, there is a continued great need to raise awareness and to ensure effective implementation of data protection principles. This is why the initiative adopted at the 28th International Conference in London in 2006 is entitled: "Communicating Data Protection and Making It More Effective". Secondly, the question how to deal with various new technologies, such as RFID and other building blocks of "intelligent environments". Thirdly, making sure that security concerns are not seen as necessarily overwhelming legitimate privacy interests. In my view, we need an integration of both in a sound world.

6. How, and when, do you think the issues of SWIFT and PNR between Europe and the US are likely to be resolved?

Peter Blume: I believe that these issues will be solved this year. Whether they will be solved in a satisfactory way is not at all certain. I will not guess what the solution will be. They will probably be different as it is my impression that citizens are more worried with respect to PNR than Swift. However in both cases the terror/crime argument that life is more important than private life will be persuasive. There will be restraints due to data protection but they will be modified.

Peter Hustinx: It will not be very easy in the short term, but there is a growing potential to think of these and other current issues in transatlantic relations, in a wider and more balanced perspective. The European Parliament is presently trying to set up a dialogue with the US Congress, which might be a good step. However, both issues are truly global and should be dealt with accordingly. Whatever happens in EU-US relations is therefore also an important benchmark for future arrangements.

7. What do you think data protection will be like twenty years in the future?

Continued on p.24

PL&B's 20th Anniversary

Stewart Dresner on 20 years of the *Privacy Laws & Business International Newsletter*.

In 1987, the basis for data protection laws was, in Europe, the Council of Europe Convention, and elsewhere in the world the OECD Guidelines. The EU Data Protection Directive was nearly a decade away, and therefore the US Safe Harbor was not envisaged. There were also no national privacy laws in the Asia-Pacific region. Many in the private sector in the US thought that data protection laws should not apply to companies. Data Protection Commissioners' Conferences were cosy affairs, sometimes around one table. Fax machines were new, e-mail, the internet and websites hardly existed. Information on international data protection laws was scarce. When discussing my plan for this newsletter, large companies, law firms and Data Protection Commissioners were supportive. They remain so.

Maximum value

I wrote in the editorial for the first newsletter: "You will get maximum value from your subscription if you use Privacy Laws & Business as a forum for sharing your data protection experience with other companies in what is for everyone a non-competitive area." I still agree with the first part of the sentence, but my view on the second part has changed. Although many companies want to merely make sufficient compliance efforts, some are going further and making privacy a competitive advantage.

Twenty years ago this month, when I started the *Privacy Laws & Business Newsletter*, my intention was to provide authoritative news and analysis of data protection laws around the world, how they have an impact on organisations and how companies could integrate privacy laws into good business practice. This goal has remained the core of our activities, as you see in this 20th anniversary edition. This mission has been sustained by the enthusiasm of our subscribers from all sectors, including many privacy regulators, worldwide. Many of them have remained subscribers throughout the period.

Our contributors from all around the world have enabled the *Privacy Laws & Business International Newsletter* to become the authoritative source of information on privacy laws worldwide. The *PL&B UK Newsletter* joined the family in 2000 and also covers the UK's Freedom of Information Act.

It is a continuing pleasure to meet you at our conferences, where you provide unrivalled insights and share your expertise with the global privacy community. Some of them reflect on the past and next 20 years in this issue (p.22).

Privacy Laws & Business continues to stay ahead by providing you, for example, with the first analysis of new laws in Russia (PL&B International, August 2006, p.1) and now Dubai (p.1). Privacy laws now have a far greater impact on both organisations and individuals than could have been forecast in 1987. A list of factors would include customer relationship management, employee monitoring, closed-circuit TV, webcams and doing business via the internet. Privacy laws will always have to develop to deal with new challenges, such as the recent reversal of privacy norms represented by social networking sites (*PL&B International*, December 2006, p.28-31). While people have heightened concerns about privacy issues in advanced societies throughout the world, privacy has become a social as well as a legal issue.

Major privacy trends

We have monitored the major privacy trends over this period, such as:

1. The *growth of an international framework of law*, such as the EU Data Protection Directive and its continuing influence via the decisions of the EU's Art. 29 Data Protection Working Party.

2. The *considerable increase in the number of countries with a data protection law* from the 10 European countries we listed in our first issue in February 1987 to the 36 worldwide listed (pp.26-27) which have Data Protection Authorities accredited to the DPAs' conference.

3. The *working together of countries* both within the EU framework and in the APEC framework (p.14) aiming to provide organisations with a somewhat consistent framework, or at least an understanding, of privacy norms underpinning good practice. Legal certainty is an ambivalent value, as some companies say that legal certainty is not a worthwhile goal if pitched at too high a level.

4. The *powerful combination of data protection law and other laws*, such as employment law, evident even in 1987 in Germany, consumer law and criminal law.

5. *Starker conflict*, particularly between Europe and the US (p.1), with Canada striving to provide a middle way.

6. *Stronger enforcement*, leading not only to larger fining powers for national data protection authorities, such as in Spain and France (*PL&B International*, October 2006, p.1), but also the deployment of the supporting big guns of other enforcement bodies, such as the Federal Trade Commission in the US (*PL&B International*, August 2006, p.14), and now the UK's Financial Services Authority (pp.8-9).

PL&B's 20th Annual International Conference

Many of the above issues will be covered in our 20th Annual International Conference: *Global Warning! Privacy Climate Changes Ahead*. It takes place at St. John's College, Cambridge, on 2-4 July. A list of speakers and their subjects will be available from early next month.

This month, we have moved into new offices with new telephone and fax numbers. Our new website, www.privacylaws.com, also to be launched around the end of this month, now has many more features, including:

- headline news on the home page
- a search facility and sitemap
- secure electronic payments
- instant access to newsletter back issues
- a greatly expanded links section.

Continued on p.25

Continued from p.23

Peter Blume: In the next 20 years there will many developments and they will be influenced by the fact that a greater proportion of the population only knows a digital world. It seems likely that the scope of data protection will have been limited so that it only will cover sensitive data. Article 6 [Principles relating to data quality] of Directive 95/46 will have been repealed. As there have been no major scandals, widespread surveillance is generally accepted. People think it provides safety. Privacy is not dead and in their own homes citizens want to be private. In public, data sharing is common and generally accepted.

David Flaherty: In 1987, I predicted that by the year 2002, data protectors were at risk of being individuals trying to hold back the flood of abuses with their finger in a dyke; I think the same risks will continue to exist into the foreseeable future because of the powerful forces of technological innovation, the inadequacy of resources to achieve robust data protection, the adoption of electronic health records (with the accompanying huge risks), and the ongoing digital revolution.

Masao Horibe: Developments in global communication networks will change the relationship of most economies in the world and most of them need data protection laws. At the same time, it will be necessary to harmonise them.

Peter Hustinx: Data protection will have been recognised as a core asset of democratic states based on the rule of law, and other states will follow similar principles to ensure and protect global information infrastructures, which have become essential in a highly integrated world environment. Multinational enterprises have a considerable leverage: "good client relations" and "seamless efficiency" could together make a good business case.

Francis Aldhouse: First, I congratulate Stewart Dresner and Privacy Laws & Business for twenty years of publishing its newsletters. The growth of the business over that period has been a mirror of the growth in public and organisational concern about privacy issues.

Look back to 1987 and remind ourselves of the concerns of Eric Howe, the first UK Data Protection Registrar. His Annual Report for that year, three years after the passing of the first UK Data Protection Act, told us not just of the mechanics of setting up a new office and the registration system. More importantly it alerted us to the development of "massive collections of personal data" covering the bulk of the UK population. These databases were typically in the public sector, but the early enforcement action against the credit reference agencies demonstrated equal concern about the policies and practices of equally large private sector data processing schemes. At the same time, research showed that the general public attached great importance to the protection of individual privacy.

Twenty years on we seem to be faced with the same concerns: an identity card scheme, "spy-in-the-sky" vehicle tracking and other manifestations of the "surveillance society". Citizens have, however, become sensitised to the issues and "identity theft" stories makes headlines in a way they did not twenty years ago. Should we look to the future with optimism or not? Every modernising initiative by government seems to propose another invasion of privacy – justified either by public security or efficiency of public administration. But the public and their representatives are fighting back and perhaps the wave of "breach notification" laws across the US is a sign that all is not lost.

Continued from p.24

PL&B an active participant

Privacy Laws & Business is not only an observer of the scene but is also an active participant. For example:

- PL&B arranged workshops in Denmark, Switzerland and the Netherlands in the late 1980s for many national data protection authorities to discuss and coordinate their policies on credit referencing, insurance and direct marketing respectively.
- PL&B provided expertise to the European Commission in its assessment of attitudes of public and private sector data controllers towards national data protection laws in seven EU member states in 1993/4, shortly before the adoption of the EU Data Protection Directive; and in the late 1990s and into the current decade, the adequacy of the first group of countries to receive approval, such as Switzerland, Canada and Argentina and those which have not yet, such as the US and New Zealand.
- PL&B researched, tested and wrote the Data Protection Auditing Manual for the United Kingdom's Data Protection Commissioner, published in July 2001, which develops auditing procedures based on ISO 9000 quality management principles and is now freely available on his website.
- PL&B is currently preparing a white paper for Canada's Privacy Commissioner for discussion at this year's DP Commissioner's Annual Conference, to be held in Montreal, to assess the use and value of privacy law audits drawing examples from several countries.
- PL&B provides the secretariat for the European Privacy Officers Network, established in 2001, which holds roundtables with privacy managers and data protection commissioners, so far in Spain, Italy, the Czech Republic, France, Germany and Ireland.

PL&B is also frequently used by many of the world's multinational companies, major law firms and the public sector for information, training, recruitment, contacts and advice. Some of these statistics are on the back page. It is gratifying to find PL&B's website, www.privacylaws.com, generally in the top five if you use a major search engine to look for information on "privacy laws", a result achieved without website optimisation.

Thank-you

Finally, I am delighted to acknowledge the enormous contribution made by our *International* and *UK Newsletter* editors, James Michael and Laura Linkomies, with whom I have worked for 30 and 10 years respectively, our worldwide network of consultants, and former and current PL&B colleagues, who form an outstanding team so we can, together, fulfil our mission.

As many of PL&B's innovations have come from you, the international privacy community, I ask you to keep the ideas flowing in. We at PL&B will do our best to keep you informed and engaged with the ever changing privacy law scene.

Accredited DP Authorities

The following authorities have been accredited to the International Conference of Privacy and Data Protection Authorities in accordance with the Criteria and Rules for Credentials Committee. The list was published by the UK Information Commissioner, who hosted the 28th conference in London in November *(PL&B International Newsletter*, December 2006, pp.5-6). Where an authority has a title in a language other than English, this is given in brackets (where known). Links to the websites of most data protection authorities are at www.privacylaws.com.

ACCREDITED DATA PROTECTION AUTHORITIES

Country	Name of authority	Member of European Economic Area	Council of Europe Convention on Automatic Processing of Personal Data*	Additional Protocol to the Council of Europe Convention**
National authorities				
Andorra	Data Protection Agency (Agència Andorrana de Protecció de Dades)			
Argentina	National Direction for Personal Data Protection (Director Nacional de Protección de Datos Personales)			
Australia	Federal Privacy Commissioner			
Austria	Data Protection Commission (Datenschutzkommission)	✓	P	S
Belgium	Privacy Commission (Commission de la vie privée)	✓	P	S
Canada	Privacy Commissioner of Canada (Commissariat à la protection de la vie privée du Canada)			
Cyprus	Personal Data Protection Commissioner	✓	P	P
Czech Republic	Office for Personal Data Protection (Urad Pro Ochranu Osobnich Udaju)	✓	P	P
Denmark	Data Protection Agency (Datatilsynet)	✓	P	S
Estonia	Data Protection Inspectorate (Andmekaitse Inspektsioon)	✓	P	
Finland	Data Protection Ombudsman (Tietosuojavaltuutetun Toimisto)	✓	P	S
France	Data Protection Commission (Commission Nationale de l'Informatique et des Libertés)	✓	P	S
Germany	Federal Data Protection Commissioner (Bundesbeauftragten für den Datenschutz)	✓	P	P
Greece	Hellenic Data Protection Authority	✓	P	S
Hungary	Parliamentary Commissioner for Data Protection and Freedom of Information	✓	P	P
Iceland	Data Protection Authority	✓	P	S
Ireland	Data Protection Commissioner (An Coimisinéir Cosanta Sonraí)	✓	P	S
Italy	Data Protection Commission (Garante per la protezione dei dati personali)	✓	P	S
Korea	Korea Information Security Agency (KISA)			
Latvia	State Data Inspectorate (Datu Valsts Inspekcija)	✓	P	
Liechtenstein	Data Protection Commissioner	✓	P	
Lithuania	State Data Protection Inspectorate (Valstybine Duomenu Apsaugos Inspekcija)	✓	P	P
Luxembourg	National Data Protection Commission (Commission nationale pour la protection des données)	✓	P	P
Malta	Data Protection Commissioner	✓	P	
Netherlands	Data Protection Commission (College bescherming persoonsgegevens)	✓	P	P
New Zealand	Privacy Commissioner (Te Mana Matapono Matatapu)			
Norway	Data Inspectorate (Datatilsynet)	✓	P	S
Poland	Inspector General for Personal Data Protection (Generalny Inspektor Ochrony Danych Osobowych)	✓	P	P
Portugal	National Data Protection Commission (Comissão Nacional de Protecção de Dados)	✓	P	P
Romania	National Supervisory Authority for Personal Data Protection (Autoritãii Nationale de Supraveghere a Prelucrãrii Datelor cu Caracter Personal) to replace previously accredited authority, The People's Advocate (Ombudsman) (Avocatul Poporului)	✓	P	P

ACCREDITED DATA PROTECTION AUTHORITIES

Country	Name of authority	Member of European Economic Area	Council of Europe Convention on Automatic Processing of Personal Data*	Additional Protocol to the Council of Europe Convention**
National authorities (continued)				
Slovakia	Inspection Unit for the Protection of Personal Data	✓	P	P
Slovenia	Human Rights Ombudsman (Varuh Èlovekovih Pravic)	✓	P	
Spain	Data Protection Commissioner (Agencia de Protección de Datós)	✓	P	
Sweden	Data Inspection Board (Datainspektionen)	✓	P	P
Switzerland	Federal Data Protection Commissioner (Préposé Fédéral à la Protection des Données et à la Transparence)		P	S
United Kingdom	Information Commissioner	✓	P	S

Authorities with a limited sub-national territory

Country	Name of authority
Australia	
New South Wales	Privacy Commissioner
Northern Territory	Information Commissioner
Victoria	Privacy Commissioner
Canada	
Alberta	Information and Privacy Commissioner
British Columbia	Information and Privacy Commissioner
Manitoba	Ombudsman (L'Ombudsman du Manitoba)
New Brunswick	Ombudsman
NW Territories	Information and Privacy Commissioner
Nunavut	Information and Privacy Commissioner
Ontario	Information and Privacy Commissioner (Commissionaire à l'information et à la protection de la vie privée)
Quebec	Information Access Commission (Commission d'accès à l'information)
Saskatchewan	Information and Privacy Commissioner
Germany	
Bavaria	Privacy Commissioner (Bayerische Landesbeauftragte für den Datenschutz)
Berlin	Data Protection and Freedom of Information Commissioner (Beauftragter für Datenschutz und Informationsfreiheit)
Brandenburg	Data Protection and Access to Information Commissioner (Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht)
Hamburg	Data Protection Commissioner (Hamburgischer Datenschutzbeauftragter)
Hesse	Data Protection Commissioner (Hessische Datenschutzbeauftrage)
Mecklenburg-West Pomerania	Data Protection Commissioner (Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern)
Rhineland Palatinate	Data Protection Commissioner (Landesbeauaftragte für den Datenschutz Rheinland-Pfalz)
Saxony-Anhalt	Data Protection Commissioner (Landesbeauftragter für den Datenschutz Sachen-Anhalt)
Schleswig-Holstein	Privacy Commissioner (Unabhängiges Landeszentrum für Datenschutz) *continued*
Germany *continued*	
Thuringia	Data Protection Commissioner (Thüringer Landesbeauftragte für den Datenschutz)
Gibraltar	Data Protection Commissioner
Guernsey	Data Protection Commissioner
Hong Kong	Privacy Commissioner for Personal Data
Isle of Man	Data Protection Registrar (Oik Recortysser Codey Fysseree Ellan Vannin)
Jersey	Data Protection Registrar
Spain	
Basque Country	Data Protection Commissioner (Agencia Vasca de Protección de Datos)
Catalonia	Catalan Data Protection Agency (Agència Catalana de Protecció de Dades)
Madrid	Data Protection Agency of the Region of Madrid (Agencia de Protección de Datos de la Comunidad de Madrid)
Switzerland	
Canton of Basel-Landschaft	Data Protection Commissioner (Datenschutzbeauftragte des Kantons Basel-Landschaft)
Zurich Canton	Canton Data Protection Commissioner (Datenschutzbeauftrager des Cantons Zürich)
Zug Canton	Data Protection Commissioner (Datenschutz-beauftragter des Kantons Zug)

Authorities within an international or supranational body

Country	Name of authority
Council of Europe	Data Protection Commissioner
European Union	• Customs Info Joint Supervisory Authority System • European Data Protection Supervisor (Contrôleur Européen de la protection des données) • Joint Supervisory Body of Europol • Joint Supervisory Authority for Schengen Information System
Interpol	Commission for the Control of Interpol's Files (Commission de Contrôle des Fichiers de l'OIPC - Interpol)

* Convention for the protection of individuals with regard to automatic processing of personal data (ETS No.108, 28 January 1981) and Explanatory Report. Open for signature 8 January 1981, entry into force: 1 October 1985

** Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows. Open for signature on 8 November 2001 and entry into force on 1 July 2004

P = Party **S** = Signatory

Your Newsletter Subscription **Includes**

1. Five Newsletters a year
The *Privacy Laws & Business (PL&B)* International Newsletter, published since 1987, provides you with a comprehensive information service on data protection and privacy issues. We bring you the latest privacy news from 50 countries – new laws, bills, amendments, codes and how they work in practice.

2. Helpline Enquiry Service
Subscribers may telephone, fax or e-mail us with their questions such as: contact details of Data Protection Authorities, the current status of legislation and amendments, and sources for specific issues and texts.

3. E-mail updates
We will keep you informed of the latest developments.

4. Index
Subscribers receive annually a cumulative Country, Subject and Company index. Multiple headings include advertising, data security, Internet, police, transborder data flows and sensitive data. The index is updated after every issue on our website www.privacylaws.com.

e-Newsletter

Electronic Option
The newsletter is available, for an additional enterprise license fee, in PDF format for uploading onto your Intranet or network. This format enables you to see the Newsletter on any computer on your network as it appears in the paper version. It allows you to print out pages at any location.

Privacy Laws & Business has clients in over 45 countries, including the UK Top Ten, 8 of the Global Top Ten and 7 of Europe's Top Ten in the Financial Times lists; and 10 of the US Top 20 in the Fortune list.

Privacy Laws & Business also publishes the United Kingdom Newsletter, a publication, which ranges beyond the Data Protection Act to include the Freedom of Information Act and related aspects of other laws.

Newsletter Subscription Form

Subscription Packages

(Please add 17.5% VAT to prices for the PDF format within the EU)

❑ **Print** ❑ **PDF** (please tick preferred delivery format)

❑ Send a FREE sample of the *UK/International* newsletter

❑ *PL&B International* Subscription **£360/$720/€550**

❑ *UK/International* Combined Subscription **£580/$1,150/€870** or an extra **£305/$600/€450** for existing UK subscribers)

❑ Special academic rate – 50% discount on above prices

Multiple Subscription Discounts

❑ 2-9 copies: 30% discount (indicate no. of copies .....)

Intranet Enterprise Licence (inc. up to 10 printed copies)

❑ *PL&B International* **£1,800/$3,600/€2,750**

❑ *PL&B UK* **£1,375/$2,750/€2,100**

❑ Both *International/UK* newsletters **£2,900/$5,750/€4,350**

❑ I wish to receive *PL&B's* FREE e-mail news service

Data Protection Notice: *Privacy Laws & Business* will not pass on your details to third parties. We would like to occasionally send you information on data protection law services. Please indicate if you *do not* wish to contacted by: ❑ Post ❑ E-mail ❑ Telephone

Name:

Position:

Organisation:

Address:

Postcode: Country:

Tel:

E-mail:

Signature:

Date:

Payment Options

Address of Accounts (if different):

Postcode:

❑ Purchase Order

❑ Cheque payable to: *Privacy Laws & Business*

❑ Bank transfer direct to our account:
Privacy Laws & Business, Barclays Bank PLC, 355 Station Road, Harrow, Middlesex, HA1 2AN, UK.
Bank sort code: 20-37-16 Account No.: 20240664
IBAN: GB92 BARC 2037 1620 2406 64 SWIFTBIC: BARCGB22
Please send a copy of the transfer order with this form.

❑ American Express ❑ MasterCard ❑ Visa

Card Name:

Credit Card Number:

Expiry Date:

Signature: Date:

I am interested in:
❑ Consultancy/Audits
❑ In-House Presentations/Training
❑ Recruitment Service

Please return to: Newsletter Subscriptions Department, Privacy Laws & Business, 2nd Floor, Monument House, 215 Marsh Road, Pinner, Middlesex HA5 5NE, UK, Tel +44 20 8868 9200
Fax: +44 20 8868 5215, e-mail: sales@privacylaws.com 21/02

www.privacylaws.com

Guarantee

If you are dissatisfied with the newsletter in any way, the unexpired portion of your subscription will be repaid.