WORLD DATA PROTECTION REPORT

Volume 3, Issue 6 June 2003

Monthly news and analysis of data protection and privacy issues from around the world

LEGISLATION & GUIDANCE

News

PERSONAL DATA

SECURITY & SURVEILLANCE

Case Report

News

BNA International Inc., London

INTERNATIONAL INFORMATION FOR INTERNATIONAL BUSINESS

WORLD DATA PROTECTION REPORT

Publishing Director: **Deborah Hicks**
Editorial Director: **Joel Kolko**

Editor: **Nichola Dawson**
Production Manager: **Nitesh Vaghadia**

Correspondent:
Brussels: Joe Kirwin

Submissions by Authors: The editors of *World Data Protection Report* invite readers to submit for publication articles that address issues arising out of the regulation of data protection, either on a national or transnational level. Articles with an appeal to an international audience are most welcomed. Prospective authors should contact Nichola Dawson, World Data Protection Report, c/o BNA International Inc, 29th Floor, Millbank Tower, 21-24 Millbank, London SW1P 4QP, England. Tel. (+44) (0)20 7559 4807; fax (+44) (0)20 7559 4880; or e-mail: nicholad@bna.com. If submitting an article by mail please include a diskette with the article typed in plain text or in Microsoft Word or WordPerfect formats.

WORLD DATA PROTECTION REPORT is published monthly by BNA International Inc., a subsidiary of The Bureau of National Affairs, Inc., Washington, D.C., U.S.A. Administrative headquarters: 29th Floor, Millbank Tower, 21-24 Millbank, London SW1P 4QP, England. Tel. (+44) (0)20 7559 4801; Fax (+44) (0)20 7559 4840; e-mail marketing@bnai.com. In the U.S. call toll-free on: 1-800-727-3116.

Subscription price: U.K. and rest of world £525; Eurozone €850; U.S. and Canada U.S.$895. Web version (standard licence): £625/€995/$1050. Additional copies of this publication are available to existing subscribers at half price when they are sent in the same envelope as a standard subscription.

Website: *www.worldtaxandlaw.com*
ISSN 1473-3579

The international transfer of employees' personal data is an issue for all businesses operating inside and outside of the European Union. The stringent requirements of E.U. data protection law mean that achieving compliance is both lengthy and expensive for global businesses required to send personal data from offices inside the Member States to offices abroad.

Our article from Miriam Wugmeister, Karin Retzer and Cynthia Rich at Morrison & Foerster examines how the adoption of a code of conduct approach to cross-border data transfers may help international companies simplify their obligations in this regard. As the journal was going to press, the Article 29 Working Party adopted a Working Document on this topic. A full analysis of the Working Document and its implications will appear in the July issue of *World Data Protection Report*.

Also the subject of cross-border data transfers and of particular interest to U.S. companies with subsidiaries in the European Union, is our article on p. 21 from Shanti Atkins, Philip L. Gordon and Scott J Wenner of U.S. law firm Littler Mendelson.

While data protection and privacy laws are relatively well-established in the European Union, other countries are at an earlier stage in proceedings. Japan has struggled to implement its new privacy law, though progress is now being made. As the current Japanese Diet session comes to a close, David E. Case of White & Case LLP reports on the situation to date.

Your comments and feedback on both this issue, and the journal as a whole are welcomed. Please contact me at: nicholad@bna.com or by telephone on: (+44) (0)20 7559 4807. I look forward to hearing from you and hope you find June's *WDPR* useful and informative.

Nichola J. Dawson

We wish to thank the following for their contribution to this issue:

John Armstrong and *Lisa Benjamin,* CMS Cameron McKenna, London; *Shanti Atkins, Philip L. Gordon* and *Scott J. Wenner,* Littler Mendelson, San Francisco, Denver and New York, *and Gary E. Clayton,* the Privacy Council, Richardson Texas USA; *Paula Barrett,* Eversheds, *Martin Brodey* and *Florian Oppitz,* Dorda Brugger & Jordis, Vienna; *David E. Case,* White & Case LLP, Tokyo; *Alejandra López-Contreras* and *Mónica Garcia-Izaguirre,* Baker & McKenzie, Monterrey, Mexico; *Sarah Monk* and *Gary Brooks,* Berwin Leighton Paisner, London; *Alessandro del Ninno,* Studio Legale Tonucci, Rome; *Robert L. Raskopf,* White & Case LLP, New York; *Miriam H. Wugmeister, Karin G. Retzer* and *Cynthia J. Rich,* Morrison & Foerster.

The New Japanese Personal Information Protection Law

By David E. Case, Associate, White & Case LLP Tokyo Office

Introduction

On May 23, 2003, the Japanese Diet passed five bills relating to the protection of personal information (collectively, the "New Privacy Law"). Passage by Japanese lawmakers came only 10 weeks after Prime Minister Koizumi's cabinet finalised the bills on March 7, 2003. The relatively quick passage was due to two important agreements made between the ruling parties led by the Liberal Democratic Party ("LDP") and the four opposition parties led by the Democratic Party of Japan ("DPJ"). First, the parties agreed to create (or have created by certain ministries) industry specific laws and regulations that provide for a higher standard of care in handling Personal Information (defined below) by companies in those industries. The targeted industries are the medical, financial credit, and telecommunications. Secondly, the New Privacy Law is totally open to revision in three years.

But all has not been easy for privacy legislation in Japan. An earlier version of the same bill was left to expire in the previous Diet session at the end of 2002 due to widespread criticism that the freedom of journalists and academics would be impaired. With modest changes to those areas of the bill, the legislation flew through the Diet in this current session. Nevertheless, passage of the New Privacy Law marks only the beginning and not the end of the privacy debate in Japan.

The New Privacy Law

The New Privacy Law seeks to regulate the use of personal information by both government ministries and entities, and private parties.[1] Currently, the collection and use of personal information is minimally regulated in Japan.[2] The New Privacy Law's stated objective is to lay down the basic philosophy and governmental policy regarding the proper handling of Personal Information.[3] But under the New Privacy Law, protecting the rights and welfare of individuals is balanced with recognition that excessive regulation or restrictions on the use of Personal Information will forestall the adoption of e-commerce business models and the use of online transactions by companies. To appease various opponents of the legislation prior to its passage, in its oral and written communications, the Koizumi administration duly acknowledged that the protection of individual welfare and the protection of freedom of expression were important aims of the legislation. Nevertheless, the privacy legislation introduced by his cabinet was decidedly pro-business.

There are several key definitions of the New Privacy Law. The first is the definition of Personal Information. "Personal Information" (*Kojin Joho*) is defined as information that relates to living individuals and which can be used to identify specific individuals by name, date of birth, or other description (including that which can be easily compared with other information to identify specific individuals).[4] A collection of Personal Information structurally constituted so as to permit specific Personal Information to be easily retrieved electronically is called Personal Data (*Kojin Deta*).[5]

A person or business that uses Personal Information in a business operation is called a "Business Handling Personal Information" (*Kojin Joho Toriatsukai Jigyo-sha)*. The phrase is a little ungainly in English, but it works in Japanese. I will refer to a "Business Handling Personal Information" as a "BHPI". The definition of a BHPI is not as broad as a "controller" under the E.U. Privacy Directive. The definition of a BHPI expressly excludes:

- organs of the national government;
- local public entities;
- certain independent administrative corporations; and
- "persons designated by government ordinance as being little or no threat to the rights or welfare of individuals from the standpoint of the quantity of Personal Information handled and the method of use".[6]

Finally, the specific individual identified by Personal Information is called a "Principal" (*Hon-nin*).[7]

Features of the New Privacy Law

The version of the privacy legislation that was left to expire in December 2002 included a set of basic principles or mores regarding the collection, handling and use of Personal Information. The basic principles provided that Personal Information be:

- used to the extent necessary to achieve a specific and appropriate purpose;
- acquired through a legal and appropriate manner;
- held in correct and current form;
- handled with safety and care; and
- handled in a way that the underlying person shall be involved in the handling process.

The lofty aims contained in these basic principles were deleted from the New Privacy Law. Instead, the New Privacy Law addresses these same matters without a lengthy introductory basic principles section. A summary of the major topics of the New Privacy Law follows.

Covered Persons and Entities

The New Privacy Law applies to any BHPI that collects, handles or uses Personal Information. Persons and companies with less than 5,000 records fall outside the law's coverage.[8] One of the rationales behind this

de minimus exemption was to permit salesmen, small shop owners and delivery trucks, *etc.*, that have programmed into their car navigation systems customer name, addresses and telephone information to continue to use such information without having to go back to each customer with notice of what data has been collected and how it will be used.

Purpose of Use

A BHPI must specify to the extent possible its intended purpose of use in the collection and handling of Personal Information (its "Purpose of Use"). Its actual use may not exceed a scope reasonably recognised as having an appropriate connection with the original Purpose of Use[9] and the BHPI may not collect Personal Information beyond that which is necessary to achieve the consented Purpose of Use.[10] If a BHPI changes its Purpose of Use, it must either directly notify the Principal or publicly announce its revised Purpose of Use.[11]

Notice

Fundamentally, the New Privacy Law codifies the opt-out system that has heretofore informally existed in Japan. When acquiring Personal Information, a BHPI must promptly notify the Principal of, or publicly announce, the Purpose of Use, except where that Purpose of Use has already been publicly announced.[12] The general standard is that the BHPI must either directly inform the Principal or place the Principal in circumstances where the identity of the BHPI, the Purpose of Use and BHPI contact information can be easily learned by the Principal.[13] BHPIs are also obligated to draft and publicly announce a privacy policy.[14] Most Japanese licensed attorneys familiar with the New Privacy Law believe that the "except where that Purpose of Use has already been publicly announced" portion of Article 18(1) may be satisfied, depending on the situation, by publicly announcing such changes in a privacy policy on a website, by letter or by announcement in a newspaper.

If Personal Information is collected in connection with execution of a contract or other document such as an electronic form or record, the BHPI must disclose its Purpose of Use to the Principal in advance of such collection.[15] Nevertheless, Article 18(4)(ii) states that a BHPI need not inform the Principal of its Purpose of Use if the BHPI fears that its rights or fair profits will be harmed by such notification or by public announcement of the Purpose of Use.

Accuracy and Disclosure

A BHPI must diligently maintain Personal Data in an accurate and up-to-date form to the extent necessary to achieve its intended Purpose of Use.[16] Principals have a right to request disclosure of their Personal Data held by the BHPI and to request corrections.[17] The BHPI may establish the process and procedure by which Principals may request Personal Data. However, Personal Data need not be corrected by a BHPI if the cost or expense is excessive. If the BHPI chooses not to correct the data, it must implement some safeguard to protect the welfare of the Principal.

Security

A BHPI must adopt measures to prevent unauthorised disclosure, loss or destruction of Personal Information within its control.[18] It must also provide necessary and appropriate supervision of employees who have access to Personal Information so as to achieve control of security of the Personal Information.[19] Under the Japan Civil Code as well as the New Privacy Law, a BHPI would remain liable for the conduct of its service providers or subcontractors. A BHPI must provide necessary and appropriate supervision of the service provider so as to maintain control and security of the Personal Data that has been outsourced.[20]

Onward Transfer

As a general rule, Personal Information may not be sent to a third party without the prior consent of the Principal.[21] A BHPI's service provider or subcontractor, a successor in interest, or a BHPI that jointly owns or has rights in the Personal Information is excluded from the definition of a third party.[22] In addition, unlike the E.U. Privacy Directive, the New Privacy Law does not place any special conditions or obligations on BHPIs when they use service providers or sub-contractors outside of Japan. Delegating some function such as data input or data processing to service providers or sub-contractors located outside of Japan does not require any special consent from the Principal, the use of any government approved agreements or notification to a Japanese government office or ministry. Transmission of Personal Information to a third party without the consent of the Principal is permitted to fulfill a contractual obligation. For example, a department store could send Personal Information to a shipping company in order for goods purchased by the Principal to be delivered.

Principals may demand that a BHPI cease using its Personal Data or that a BHPI stop providing Personal Data to a third party, but in either case, a BHPI may refuse such request if the cost or expense to do so is excessive. If the BHPI refuses, it must implement substitute measures to protect the rights and welfare of the Principal.[23] No standard or identification of what rights of the Principal are stated.[24]

Penalties

Finally, the New Privacy Law has civil and criminal penalties ranging from admonishment orders, to fines of ¥100,000 to ¥300,000, and criminal sanctions.[25] Penalties were absent from the previous version of the law and this was a source of much criticism.

While no one can be sure how Japanese courts will interpret the provisions of the New Privacy Law, it is important to note that the obligations and restrictions placed on BHPIs are not as stringent as under, for example, the E.U. Privacy Directive. For example, if a BHPI changes its Purpose of Use, it must either directly notify the Principal or publicly announce its revised Purpose of Use.[26] It is currently unclear whether posting a revised privacy policy on a website would be sufficient notice under the New Privacy Law, but that may very well turn out to be the case. Another example is that a BHPI must diligently maintain Personal Data in an

accurate and up-to-date form *to the extent necessary to achieve its intended Purpose of Use.*[27] The New Privacy Law does not require that accuracy be maintained to the extent necessary to protect the welfare of the affected Principal. There is also no restriction on where data may be transferred to and no special disclosure requirements in the event a BHPI uses service providers to process data on its behalf. BHPIs may also use service providers located outside of Japan without any additional oversight or conditions.

What Is Not Included in the New Privacy Law

To understand the scope of the New Privacy Law it is as important to understand what is not in the legislation as what is in it. On March 28 and April 3, 2003, the four opposition parties led by the DPJ disseminated their own views on the New Privacy Law (still in bill form at the time) and proposed their own privacy legislation. The following proposals made by the DPJ in their privacy bill were not included in the New Privacy Law.

Independent Oversight

The DPJ proposed that a Personal Information Protection Committee be created as an external organ to the Cabinet Office. The committee would have been independent from the Prime Minister's office and operated similarly to the Japan Fair Trade Commission. The role of the Personal Information Protection Committee would have been to issue warnings to BHPIs in the event of suspected violations in handling Personal Information. Because the establishment of an independent body was rejected, as of today, there is no Japanese government agency specially assigned the task of enforcing the New Privacy Law.

Individual Control

The DPJ declared in its press release that provisions in the LDP's proposed privacy bill regarding the right of individuals to control information about themselves were unclear and insufficient. The DPJ believed that by creating a Personal Information Protection Committee the rights of individuals to control information about themselves (*i.e.*, with the actual individual involved in the collection, use and disclosure to a third party of such Personal Information, along with other personal rights and interests) would be stronger. Instead of the opt-out system formalised by the New Privacy Law, the DPJ's privacy legislation would have decidedly shifted control of Personal Information to the Principal and perhaps even created an opt-in framework. The fundamental principle that an individual controls his or her data was rejected in the current form of the New Privacy Law.

Sensitive Data

The DPJ's privacy bill stipulated within its basic principles that the handling of certain sensitive information by BHPIs must be carried out with extreme caution. Specifically, in principle, without the prior consent of the individual to which such information belongs, BHPIs would not have been permitted to handle the information regarding beliefs and religious faith, medical information, welfare payment records, criminal records, race, ethnicity, social status, place of birth or domicile of origin. No such distinction regarding the type of Personal Information being handled by BHPIs is made in the New Privacy Law.

Conclusion

The privacy battle in Japan, at least for this current Diet session which ends in the middle of June, is at a rest. But future battles will be waged as industry specific legislation is drafted by the ministries charged with specific industry oversight. Commentators here believe that the first ministry out of the gate with a framework for its industry may set a standard that other ministries will be forced to follow. As a result, companies who extensively use or rely upon their customer's Personal Information to do business are already approaching Ministry officials with their concerns and suggested resolutions.

1 This article focuses only on the portions of the New Privacy Law applicable to private parties.
2 Other laws that protect privacy include the law governing computerised processing of personal information by administrative agencies (Law No. 95, which became effective on October 1, 1989); *see also* Specified Commercial Transaction Law "SCTL", Law No. 57, 1976, Art. 11 regarding unsolicited e-mail and direct marketing laws and regulations.
3 New Privacy Law ("NPL" at) Article 1.
4 NPL at Article 2(1).
5 NPL at Article 2(2).
6 NPL at Article 2(3). Under Articles 4, 5 and 6, public authorities have a duty to draft and execute measures necessary to secure the appropriate handling of Personal Information according to the characteristics of the regions under the jurisdiction of such local public authorities.
7 NPL at Article 2(6).
8 This exemption, not yet finalised, will ultimately take the form of a Cabinet Order (*seirei*) but will not be officially adopted until a public notice and comment period is complete.
9 NPL at Article 15.
10 NPL at Article 16(1).
11 NPL at Article 18.
12 NPL at Article 18(1).
13 NPL at Article 24.
14 NPL at Article 43.
15 NPL at Article 18(2).
16 NPL at Article 19.
17 NPL at Articles 25 and 26.
18 NPL at Article 20.
19 NPL at Article 21.
20 NPL at Article 22.
21 NPL at Article 23.
22 NPL at Article 23(4).
23 NPL at Article 27.
24 Generally, the provisions of the New Privacy Law do not apply to a BHPI's use or disclosure of Personal Information if pursuant to a law, ordinance or official order, or if necessary for the protection of human life, safety, or property, or if necessary in to improve public hygiene or promote the health of children, provided in both cases only when it is difficult to obtain the consent of the Principal. *See, e.g.*, NPL at Article 16(3).
25 NPL at Article 56-59.
26 NPL at Article 18.
27 NPL at Article 19.

David E. Case *is a senior associate in the Tokyo Office of White & Case LLP practicing in the area of intellectual property licensing, litigation and acquisition. He currently serves as the Co-Chair of the Privacy Law Task Force of the American Chamber of Commerce Japan. Qualified in New York, U.S. and in Japan as a Gaikokuho Jimu Bengoshi. He can be reached at dcase@tokyo.whitecase.com or 81-3-3259-0149.*

Codes of Conduct: The Solution For International Data Transfers?

By Miriam H. Wugmeister, Karin G. Retzer and Cynthia J. Rich, Morrison & Foerster

In its long-awaited *Report on the implementation of the Data Protection Directive 95/46/EC,*[1] which was published on May 15, 2003, the European Commission recognises the enormous difficulties that companies are facing when transferring data on a global basis. E.U. Member States' laws governing cross-border transfer are complex, burdensome, and, often contradictory. Compliance with these regulations can be a Herculean task, involving considerable time and expense.

Rather than being forced to satisfy diverging rules for transferring data on a country-by-country basis, more and more companies are pushing for the development of global codes of conduct that would govern their global data processing practices and at the same time facilitate all their international data transfers. In the Report, the European Commission now too is encouraging industry and Member States to experiment more widely with a code of conduct approach to cross-border data transfers.

Rules on Cross-Border Data Transfers

The Directive[2] restricts cross-border transfers to third countries that have been found to ensure an "adequate" level of protection (Article 25). To date, the European Commission has deemed adequate the laws of Canada, Hungary, and Switzerland, as well as the U.S. safe harbor principles. An adequacy finding with respect to the Argentine data protection legislation is under way. While the Commission continues to assess laws in other countries, it has made clear in various public statements that it does not have the resources to issue "adequacy decisions" more frequently.

For those countries that are not covered by a "adequacy decision", data transfers can only take place if one of several conditions are met (Article 26 of the Directive):

- the individual to whom the data relate (the data subject) has provided unambiguous consent to the transfer;
- a contract with the organisation receiving the data has been established;
- the transfer is necessary for the performance of a contract between the data subject and the organisation exporting the data;
- the transfer is necessary for the performance of a contract concluded in the interest of the data subject;
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject; or
- the transfer is made from a register which, according to laws or regulations, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest.

Despite the fact that the Directive provides a means for transferring data to non-adequate countries, the divergent implementations of the Directive among Member States makes it virtually impossible for companies to select a single safeguard to protect the data as they transfer data out of the European Union. For example, the transfer of personal data based on consent of the data subject may be restricted to non-employee data situations in many Member States.[3] In addition, the "necessary to complete the contract between the controller and data subject" basis for transfers has been interpreted narrowly in some Member States, which limits its usability.[4] The end result is that companies must analyse and satisfy fifteen different standards for transferring data, thus defeating the harmonising intent of the Directive.[5] The European Commission acknowledged this difficulty in its Report, and stated "More work is needed on the simplification of the conditions for international transfers."

The Directive's rules on cross-border data transfers have influenced heavily the development of other countries' rules in this area. Argentina, Brazil, and Mexico in Latin America and Australia, Malaysia, South Korea, Taiwan, and Thailand in the Asia-Pacific Rim have either adopted or are considering adopting legislation that would impose varying degrees of restrictions on cross-border transfers. In addition, E.U.-style cross-border restrictions have been or will be implemented in the near future by all of the New Member States, *i.e.,* Cyprus, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia, Slovenia, (anticipated population of 75 million).

Codes of Conduct: An Alternative Approach

Given the growing number of cross-border data transfers, the idea of relying on global rules for all cross-border data transfers is attractive. The code of conduct concept is a simple one. Related companies doing business in multiple E.U. Member States would apply just one set of rules to govern their data transfers from within the European Union to outside the E.U. rather than 15 different rules that comply with the specific requirements of each of the 15 Member States. Companies could also draft these codes so that they comply with the privacy rules in non-E.U. countries.

What the Directive Says about Codes of Conduct

The Directive clearly provides for the use of codes of conduct. To contribute to the proper implementation of

the Directive at the national level, Article 27 of the Directive directs the Member States and the Commission to encourage the development of codes of conduct. Member States are required to facilitate the approval procedure of draft codes and amendments or extensions to existing codes prepared by trade associations and other bodies. Organisations representing certain industry sectors, and established in multiple Member States, may submit draft Community codes, and amendments or extensions to existing Community codes, to the Article 29 Working Party to determine whether the drafts comply with the Directive.

The extent to which companies can use codes of conduct as a means to transfer data globally within their organisations is unclear, however. Codes of conduct are not expressly mentioned in the sections of the Directive that addresses data transfers to third countries (Articles 25 and 26). Article 26, as explained above, establishes the safeguards, which must be in place for a Member State to authorise transfers to third countries that do not provide an adequate level of protection. Member States are authorised to approve such transfers, provided the appropriate legal bases have been satisfied, and if the organisation provides evidence that it has adequate safeguards in place to protect the data. Contractual clauses are cited as an example ("in particular") of such safeguards and traditionally have been the most common way of providing the required "adequate protection," but the wording of Article 26 (2) suggests that codes may be equally provided by other means, *i.e.*, codes. Unfortunately Article 26(4) is silent about whether the Commission has the right to approve "standard codes of conduct" similar to the right of the Commission to approve standard contractual clauses.

Growing Support for Codes of Conduct

The Commission and some Member States support the idea of codes of conduct as a means to facilitate data transfers. During his closing remarks at the 2002 data protection conference,[6] Commissioner Bolkestein acknowledged that the promotion of self-regulatory approaches and in particular codes of conduct can contribute to the free movement of personal data and that the idea that approval by one data protection authority should in principle work in all Member States needs to be pursued. Some data protection authorities believe that self-regulatory codes of conduct could serve as a simple and effective means to achieve adequacy. Moreover, in the case of Germany, section 4 (c) of the German Data Protection Act expressly provides for the possibility to legitimise international data transfers via binding company rules.

The primary obstacle to using codes of conduct is that there is no streamlined mechanism for approving enterprise-wide codes. During the 2002 conference, the Commission was urged by some in industry to ensure that any proposal it makes to revise the Directive includes a proposal that expressly allows the Commission to approve such enterprise-wide codes of conduct in a streamlined manner. Such a proposal also should allow individual Member States to approve codes of conduct under their own law and for those codes then to receive mutual recognition throughout the E.U. Member States. Mutual recognition of codes would eliminate the need for some adequacy rulings and help alleviate the European Union's already over-taxed system for issuing adequacy decisions. Alternatively, Member State authorities could institute co-operation mechanisms to facilitate the needs of multinational companies with establishment in several jurisdictions.

Experimenting with Codes of Conduct

To date, the Dutch Data Protection Authority ("DPA") has approved fifteen codes of conduct, mainly in the financial services, pharmaceutical, and direct marketing services sector, that can be used to satisfy national requirements for the processing of personal data. These codes are used to promote compliance with sector specific data protection requirements. To our knowledge, these rules have not been used for the purpose of satisfying requirements imposed on transfers to non-adequate third countries.

Discussions about the use of corporate codes of conduct specifically for cross-border data transfers are underway, however. The Dutch DPA is discussing with Royal Dutch/Shell Group of Companies the use of a corporate code of conduct to facilitate the transfer of human resources data from Shell's headquarters in the Netherlands to its 2,200 subsidiaries in 140 countries. The project would involve approval of the Shell code, and co-operation between the authorities in the Netherlands and the United Kingdom.

DaimlerChrysler has obtained approval from the German authorities for its Code of Conduct for Human Resources. The authorities have found that the conditions stipulated in the codes under which personal data can be transmitted between countries provide sufficient protection throughout the group and therefore allow transfers of data outside of the European Union without additional safeguards.

The hope of these DPAs is that once the process starts, other DPAs might follow. There also have been discussions with these DPAs about the possibility of mutual recognition of codes that are compliant with the laws of the country in which the data controller has a "centre of activities". Acceptance of this concept is not expected in the short term, however. The more likely approach will be to experiment with co-operation mechanisms between a limited number of DPAs.

Article 29 WP – Lack of Consensus on Codes

During the April meeting of the Article 29 Working Party, codes of conduct were discussed but no agreement was reached on EU-wide codes of conduct. (Only 11 Member States refer expressly to codes of conducts in their national laws implementing the Directive, and approaches to codes differ from Member State to Member State.) Some members of the Article 29 Working Party appear either opposed or at best lukewarm to the idea of using codes of conduct. Further discussion is

likely to remain on hold until these differences of opinions are resolved.

Although some representatives in the DPAs and the Commission believe that Article 26 of the Directive allows single sets of rules to serve as a legal basis for international transfers, the Commission is not expected to push right away for E.U.-wide codes. Lack of Member State political will and the lack of consensus within the Article 29 Working Party are to blame. It appears that the Article 29 Working Party will continue the discussion and a working document that outlines its initial views on codes of conduct or binding corporate rules is expected to be published soon. Companies should take this opportunity to voice support for codes and identify potential problems and solutions.

Conclusion

While the development of a code of conduct approach to data protection and cross-border transfers will not happen overnight, a code of conduct approach holds promise for global companies looking to simplify and facilitate their cross-border transfers. Experimentation with codes at the Member State level is likely to continue for some time, though, before action on an E.U.-wide basis is taken. Companies interested in exploring and promoting the use of codes should take the opportunity to voice their support for codes of conduct and identify potential problems and solutions directly to the Member State data protection authorities and government policy makers, the Commission, and the Article 29 Working Party. When the Article 29 Working Party issues its working document on codes of conduct, companies should review its conclusions carefully and, may make their views known, either on an individual basis or through trade associations or other business groups directly to the Working Party, the Commission, and/or the Member States. Continued expressions of interest in pursuing this and other innovative solutions to global data transfers will add to the growing momentum for change in the global privacy/data protection field.

1 First report on the implementation of the Data Protection Directive (95/46/EC) of May 15, 2003, COM (2003) 265 final, available at *http://europa.eu.int/comm/internal_market/privacy/lawreport_en.htm*.

2 Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal* L. 281, 23/11/1995 p. 0031-0050 (1995).

3 Many data protection authorities are of the opinion that employees do not have the necessary freedom to consent meaningfully to the transfer of such data because of their inherent dependence on their employers. *See* Article 29 Data Protection Working Party Opinion 8/2001 on the processing of personal data in the employment context, September 13, 2001 available at: *http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs*.

4 For example, German commentary suggests that the criteria "necessary" for the performance of the labor contract had a meaning of "indispensable;" see Wolfgang Däubler: Internet und Arbeitsrecht, 2001, p. 143.

5 The only uniform method of complying across the E.U. is with standard clauses/model contracts. If a global company, however, elected to utilise model contracts to transfer data among affiliates, it is perfectly possible that it would have to enter into hundreds of contracts which would be administratively burdensome and complex.

6 See Commissioner Bolkestein's closing speech at the 2002 data protection conference, available at *http://europa.eu.int/comm/internal_market/en/dataprot/lawreport/programme_en.htm*

Miriam Wugmeister, *a partner in the New York office of Morrison & Foerster, may be reached at wugmeister@mofo.com;* ***Karin Retzer,*** *an associate in the Brussels office, may be reached at kretzer@mofo.com; and* ***Cynthia Rich,*** *a legal analyst in the Washington, D.C. office, may be reached at crich@mofo.com.*

Editor's Note: *The Article 29 Working Party has recently adopted (on June 3, 2003) a document entitled, "Working Document on Transfers of Personal Data to Third Countries: Applying Article 26 (2) of the E.U. Data Protection Directive to Binding Corporate Rules for International Data Transfers" (dealing with so-called company "codes of conduct"). The document is available on the DG Internal Market's website, at www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp74_en.pdf*

Implementation of the Privacy and Electronic Communications Regulations in the U.K

By Paula Barrett, a Partner in the IT and E-Commerce Group of Eversheds. The author specialises in data security and online liability issues and may be contacted on tel: +44 (0)113 243 0391; or at: paulabarrett@eversheds.com

Following the adoption in July 2002 of the Electronic Communications Privacy Directive, (Directive 2002/58/EC), the United Kingdom is required to enact implementing legislation into U.K. law by October 31, 2003. In anticipation of this, the U.K.'s Department of Trade and Industry (DTI) commenced consultation on implementation of the proposed Privacy and Electronic Communications Regulations 2003 on March 27, 2003 with comments to be submitted to the DTI by June 19, 2003. The Directive both updates and replaces the current Telecoms Data Protection Directive 97/66/EC to encompass new forms of electronic communication network technologies, in particular Short Messaging Service (SMS) and e-mail communications.

How the Directive will Affect U.K. Businesses

The Directive will apply to businesses:

- using unsolicited e-mails or SMS when undertaking direct marketing;
- collecting data about customers through the use of website cookies or other information tracking devices;
- processing "traffic data" from an electronic communications network for billing purposes or to market communications services.

Corporate Subscribers

The Consultation Document invites views on the distinction made between individual subscribers and corporate subscribers. The Directive requires Member States to specifically create rights for individuals in certain areas but gives them freedom to decide how to accommodate corporate subscribers. This prevents safeguards, which are in place for individual subscribers, unnecessarily burdening larger business. As English law considers partnership as a natural rather than a legal person, large partnerships could benefit from the safeguards attached to individuals. The Consultation Document therefore questions how the individual/corporate subscriber distinction should be managed.

"Opt-in" Requirement

The Directive will make it a legal requirement for businesses to obtain consumers' prior consent to the use of details provided by them before sending unsolicited direct marketing in the form of e-mails or SMS messages. The good practice guidelines concerning e-mail and SMS advertising suggested in the recently published 4th edition of the Committee of Advertising Practice's Code on Direct Marketing will therefore be given legal force.

Existing Customers

Direct unsolicited marketing to existing customers who have made previous purchases will not require prior consent, providing those details were obtained through a "sale" of a product or service. Unsolicited marketing to potential customers' who have simply registered interest in being kept informed about products and promotions is unlikely to sufficiently constitute a "sale". Businesses must inform consumers at the time of purchase about the potential use of consumers details for the purpose of future marketing and have given the consumer the opportunity to object to use of their details in this way. Additionally, customers must be given the opportunity to object to future marketing occurring following each subsequent marketing e-mail or SMS message.

"Similar Products"

Any marketing undertaken must be in respect of "similar products" to the product purchased when the customer originally provided their details. The concept of a "similar product" remains unclear but may prevent a business marketing a substantively new and different product range, which has little or no connection with the product originally purchased. The customers' details may also only be used by the same entity to whom they were originally given. Although this reflects current practice under the U.K. data protection regime, it may affect the "sharing" of customer lists between group companies.

Cookies and Similar Devices

Businesses using any type of cookie or other software tracking device, which identifies, monitors or stores information will be required to clearly and comprehensively inform consumers of their use and allow them the option to decline access to a site regardless of whether the cookies process information. The consultation seeks views on:

- whether this requirement should apply to all cookies or only those which process personal data;
- how businesses using cookies should inform Internet users about their use of cookies and how the opportunity to refuse cookies should be presented to subscribers;
- whether the Regulations should make specific reference to the ability of a user to override a subscriber's consent, for example in relation to shared network systems where an employee of a corporate subscriber could disable or block a cookie of the subscriber which prevents the functioning of the programme.

Access to an alternative cookie-free site will not be necessary if use of cookies is essential to the online service(s) being provided or a "legitimate purpose" of the website such as to monitor the identity of users engaged in online transactions.

It is likely that businesses will be required to publish cookie statements, which may form part of an online privacy statement. Where businesses use cookies to process personal data then any processing must be done in accordance with the Data Protection Act's requirements on fair processing of personal data.

Other Provisions

The Directive will enable subscribers to access publicly available directories of electronic communications services, to decide whether or not they wish to be included in such directories and if so, choose the extent of subscriber personal data to be included. Consumers' consent will also have to be obtained for inclusion in "reverse search function" directories, popular in European countries, which allow a subscriber's name and address to be obtained through entering their telephone number. Businesses, in particular mobile phone operators, will additionally require customers consent to provide "value added services" or advertising dependent upon the location of the user's terminal equipment, such as the provision of traffic guidance services to drivers, weather forecast or tourist information. Before consent is given, the data processing implications must be explained to the consumer, who must be allowed to subsequently withhold consent.

Network and service providers will also be required to safeguard the security of their networks and to inform subscribers of any particular security risks and the remedies being addressed to manage risk such as informing subscribers about their use of encryption technology.

Enforcement and Sanctions

The Information Commissioner will be responsible for enforcement of the Directive's provisions in the

United Kingdom. This may result from a complaint or on his initiative. Close liaison with regulatory agencies such as OFCOM (Office of Communications) is expected. Following a breach of the legislation, an Enforcement Notice may be issued or further information requested through an Information Notice. A fine may be imposed for breach of an Enforcement Notice together with the damage to business reputation and goodwill, which may ensue as a result. Alternative sanctions, similar to those available to OFCOM under the new Communications Act, are expected to be introduced including the direct imposition of fines up to £5000, the seeking of injunctions to ensure the terms of an enforcement notice have been complied with and potential criminal liability.

All businesses should now consider compliance with the Directive. Following closure of the consultation period on June 19, 2003 and considering points raised in that consultation, final implementing Regulations are expected to be published in August 2003. This will allow a period of familiarisation to follow before the deadline set for implementation of the Directive of October 31, 2003.

A copy of the Consultation Document and further information can be found at: *www.dti.gov.uk/cii/regulatory/telecomms/telecommsregulations/comms_dpd.shtml*

Privacy and the Media after the U.K. Human Rights Act

By Sarah Monk, Berwin Leighton Paisner, London. The author may be contacted at: sarah.monk@blplaw.com

It has been almost three years since the implementation into U.K. domestic law of the European Convention on Human Rights in the form of the Human Rights Act ("HRA"). Arguably, the two Articles which have caused the most debate are Article 8 (respect for private life) and Article 10 (freedom of expression). Nowhere is this tension more apparent than in the competing interests of celebrities, who seek to keep details of their private life confidential; and the press, who seek to profit from publishing such details. Guidance for the press in this complex area has come from the Judiciary, the Press Complaints Commission and the Department of Culture, Media and Sport. However, commentators have voiced concern that clear guidelines need to come from the Legislature, not from piecemeal Judge-made law or from a self-regulating body, which lacks the power to prevent a tabloid from publishing a story. Recent cases have developed some guidelines but have they gone far enough to avert the need for privacy legislation?

The Cases

It is important to note that since the implementation of the HRA, only a handful of claims involving press intrusion into privacy have gone to court and indeed all of these cases were brought by celebrities. This highlights the narrow application of Article 8 and a so-called privacy law to ordinary people, who cannot afford costly litigation. To add to the ambiguity, Judges appear to be broadening the law of confidentiality in an attempt to circumvent a law of privacy. The three cases highlighted below have laid down some guidelines for the press in these circumstances.

R on application of Anna Ford v. Press Complaints Commission

The newsreader, Anna Ford, complained to the Press Complaints Commission ("PCC") that long-lens photographs taken of her on a beach and published in the *Daily Mail* and in *OK*! magazine constituted an invasion of her privacy and breached clause 3(ii) of the PCC Code, which provides that taking photos of people in private places without consent is unacceptable. The PCC rejected her complaints and Ms Ford sought a judicial review of the decision. In upholding the decision of the PCC (although his task in this case was not to determine if Ms Ford's rights to privacy were infringed) Mr Justice Silber commented that what would constitute an infringement of privacy is a matter of personal judgment and not an area on which the courts are well equipped to adjudicate. Rather, the PCC is a body whose membership and expertise makes it better equipped than the courts to resolve the difficult exercise of balancing the conflicting rights of an individual's privacy and those of the newspapers' to publish. The threshold laid down in justifying interference by the court in a decision of the PCC is that it must be "clearly desirable to do so". The court held that this was not such a case for intervention, as the PCC had ample material, which entitled them to reach the decision on whether the particular beach was a place where Ms Ford had "a reasonable expectation of privacy". As the Anna Ford ruling shows, clause 3(ii) is interpreted as implying that taking long-lens photographs of people in public places is permissible.

A v. B & C

The Court of Appeal in this case allowed an appeal by a newspaper to publish details of a footballer's extramarital affairs. The first instance Judge granted an injunction preventing publication and held that the protection of confidentiality should, in the context of modern sexual relations, also be applied outside marriage. The Court of Appeal decided that the case properly falls outside the limits of what should be regarded as confidential. The Court confirmed that applications for injunctions pending a full trial in cases of breach of confidence now have to be considered in the context of Articles 8 and 10; and that the importance of the latter has been enhanced by section 12 of the HRA. The Court emphasised that in striking the right balance between freedom of speech and privacy, Courts must recognise that any interference with publication has to be justified, whether or not there is a public interest in the story. However, the greater the public interest, the less willing the Court will be to ban the publication. Finally, the

Court in *A v. B & C* also said that this was not the correct forum for such disputes. The Lord Chief Justice stated, "Courts should not act as censors or arbiters of taste", but instead this should be the remit of the PCC.

This decision was also supported by judgments around the same time in the Jamie Theakston and Naomi Campbell privacy cases. The guidance coming through from these cases is that celebrities who court publicity may compromise their rights to privacy and that cases of press intrusion are better dealt with by the PCC than by the Courts. However, critics of the PCC have argued that it is not the correct body to decide upon fundamental human rights, such as privacy. A further theme running through these cases is that Judges have shied away from confirming that a law of privacy is emerging.

Probably the cruellest example of the need for a privacy law for cases that fall outside the laws of confidence is that of Gordon Kaye, lying seriously ill in hospital and photographed by paparazzi. Since then, given the ambivalence of the Government to intervene, many celebrities had hoped for a case that would press the Judiciary into taking action in recognising an individual's right to privacy.

Douglas v. Hello!

The Court handed down its long awaited judgment in this case in April 2003. At issue was whether the Douglases have rights to confidentiality and/or privacy recognised in this country and whether, in publishing unauthorised photographs of their wedding, *Hello*! infringed those rights.

The Judge accepted the evidence of the Douglases that they entered into an agreement with *OK*! magazine, *Hello*! magazine's rival, in order to control the images that were published from their wedding, rather than to earn a substantial sum for their publication. The Douglases took steps to ensure that security at their wedding in November 2000 was as tight as possible. Coupled with the exclusive deal with *OK*! magazine, they hoped that this would dissuade other magazines and paparazzi from taking and publishing unauthorised photographs.

However, unbeknown to the Douglases and to *OK*!, a photographer managed to outfox the security measures and take a number of poor quality photographs, which ultimately ended up in the hands of *Hello*! As soon as this was discovered, the Douglases and *OK*! went to Court to obtain an urgent injunction to prevent *Hello*! from publishing the photographs in a competing issue. The application, although successful at first instance, was discharged on appeal. As a result, the offending issue was eventually published in direct competition with the issue of *OK*! that contained the set of authorised photographs. The Appeal Court, on discharging the injunction, placed particular weight on the balance of convenience weighing in favour of publication by *Hello*!, due to the loss they would suffer if the issue was not published. On holding that the Douglases would still be able to pursue claims in damages, the Appeal Judges indicated that there was arguably a right to privacy under English law, which could step in where the law of confidence failed to protect an individual.

This was the first judicial confirmation of an emerging law of privacy.

Fast forward to the trial in 2003. The Douglases claimed on a number of bases, the most important being breach of confidence and, bolstered by the comments of the Appeal Judges, privacy. But all of these causes of action were problematic.

Rather than confirming the comments of the Appeal Judges on privacy, the Judge rejected the suggestion that there is a separate right to privacy in this country based upon Article 8. He said the existing law of confidence provides sufficient protection to people in the position of Michael Douglas and Catherine Zeta Jones to protect their Article 8 rights.

The Judge found that *Hello*! magazine had acted in breach of confidence. *Hello*! knew that the Douglases were seeking to protect the private nature of their wedding and the images that were generated as a result. The Judge also held that, far from undermining the Douglases rights to confidentiality, the sale of the rights in their wedding photographs to *OK*! magazine arguably strengthened their claims. This is because they were not merely seeking to protect their rights not to have a private wedding gate-crashed by the Paparazzi, but being famous individuals who traded on their image, they were simply seeking to protect what they trade in. In this respect, there is no difference between film stars in the Douglases' position and a manufacturer trying to protect a trade secret or confidential business method.

Comment

The Douglas judgment has alarmed the press. If they wish to feature a celebrity in a publication engaging in essentially private acts, then they will have to pay for the use of the celebrity's image and may have to comply with controls over how the images are used.

But the Judge also offered some words of comfort to the Press. He recognised that even though *Hello*! magazine committed a breach of confidence, the right to protect confidence has to be balanced against the right to freedom of expression enshrined in Article 10 of the Human Rights Convention. The media may therefore have a defence to breach of confidence claims on this basis.

In balancing the rights set out in Articles 8 and 10 of the Convention, the Judge placed great weight on the provisions of the PCC Code that sets out standards for journalists to follow. In carrying out the balancing exercise the Judge looked at whether *Hello*! had complied with the Code and found that they had not. The PCC has often been seen as a toothless body and so its Code is often ignored. However, by giving prominence to the Code in looking at whether the Press can justify breach of confidence, the Courts are introducing, by the backdoor, a greater significance to its provisions. This was also seen in the Anna Ford judgment. If the press can successfully demonstrate adherence to the Code, any complaint regarding breach of confidence is unlikely to succeed. The courts are therefore offering

incentives to the media to follow their self-regulatory standards.

This is a very significant decision for anyone involved in the media industry and provides welcome clarification in this area of law. It is likely to be used as a benchmark in determining how the media deal with issues of celebrity confidences and give greater prominence to the PCC Code. It seems that the case has gone far enough to avert the need for legislation – at least for the moment.

The Mexican Response to Personal Data Protection

By Alejandra López-Contreras and Mónica Garcia-Izaguirre, members of Baker & McKenzie's Intellectual Property and Information Technology Practice Group, based in Monterrey, Mexico. The authors can be contacted by telephone on (52-8) 399-1318, or by e-mail at alejandra.lopez-contreras@bakernet.com

There is no doubt about the fact that information is power. In today's information based society, handling large quantities of information, accessing and delivering it around the world in seconds is becoming easier every day. The constant evolution of information technologies has impacted upon the way in which people and companies value their data.

Many countries have recognised the need to protect individual privacy from abuse by others. However, the study of privacy law has recently come to a division between two systems: the European model and the North American practice. While the North American System tends towards self-regulation to protect individual's privacy, the European, on the other hand, tends to create government agencies and courts in charge of data protection, as well as establishing strict legislation on the management, treatment and collection of sensitive and personal data.

A most recent type of data protection called "Habeas Data" is rapidly growing amongst Latin American countries such as Paraguay, Argentina and Peru, following the example set by Brazil. The "Habeas Data" consists of the right to protect, by means of individual complaint presented to a constitutional court, the image, privacy, honor, information and freedom of information of a person. Although some of these countries have a strong preference for the European trend, they incorporated this right into their constitutions.

Current Legislation on Personal Data

For a long time, Mexico has been left behind in regard to the protection of personal data. No significant regulations in this regard were in force, except for the dispositions included in the Copyright Law and the Consumer's Protection Law regarding the use, distribution, sale, or other use of personal information. The Copyright Law regulates the use, access, communication, transmission, *etc.*, of databases that include personal information. It states that the authorisation of the owner of the data is required before performing any of the above-referred actions.

Moreover, there was no uniformity in the way "private information" was referred to in the law. While the Copyright law talks about "private information about a person", the Consumer Law refers to it as "information provided by the consumer", which appears to be a much wider term. It could be argued that the latter includes any and all information provided by the consumer in the process of a transaction. Unfortunately not even Profeco (the authority in charge of enforcing the Consumer's Protection Law) is sure what the concept includes.

Until very recently, Mexicans became aware of the convenience and need to protect their personal data and privacy. As part of this awareness, the "Law of Transparency and Access to Public Government Information" (the "Law of Transparency") was enacted in June 2002. Although its main purpose is to provide the individuals access to Government information, it includes the stipulation of certain Data Protection principles, such as:

- purpose limitation – by the inclusion of statutes that provide that the personal data should only be processed and obtained for a specific purpose;
- data quality – personal data should be true, accurate and kept up-to-date;
- transparency – individuals should have the right to know the purpose of the processing of their data.
- security – including all the technical and organisational security measures taken by the controller of the information in order to keep it safe and accurate;
- right to access, rectification and opposition – it is provided that the individual should be able to know the personal information handled by any government agency and has the right to modify inaccurate data. The individual also has, in some cases, the right to object to any further use of the data related to him;
- transference restrictions – personal information should only be assigned to third parties if they can guarantee at least the same level of security as provided by this law.

New Amendments on Data Protection

On April 30, 2002 the Senate of the Republic sent to the House of Representatives its approved project for the enactment of the Data Protection Law. The Senate based this proposed law on both systems, the North American and the European, including as well the "Habeas Data" right, which is not currently included as a Constitutional right.

The new Data Protection Law seeks to protect personal data and it's processing according to the guarantees of freedom of information and individual honor, granted by the Mexican Constitution. If approved, the Law would be applicable to companies and individuals that manage personal data, managed in archives, registries, data banks or databases ("Databases"). It is also applicable to all use of said data and its automatic management or treatment, making the users responsible for said Database.

Collection of the Data

As provided in the Data Protection Law, the Data must be certain, true and relevant to the purposes for which they were collected. It must also be collected and treated with previous consent of the individual. Moreover, Data must be obtained by means that are not contrary to the Mexican laws, in compliance with the individual guarantees granted by the Mexican constitution and specially the rights of the individual to keep its good name and privacy.

Rights of the Data Owner

Individuals have the right to know the purpose for which the Data is collected as well as the treatment given to the Data. Also, the Data owner should have at his or her sole request access to the said Data contained in the company-managed Database.

The individual should have the opportunity to modify the Data, as well as to revoke its consent to use or treat it. The only requirement to do so is that the individual must identify himself with a valid identification. The person responsible for the Database must comply with said request and inform the individual accordingly within five days as from the date of the request by the individual.

Use of the Data

It is relevant to note that Data, as in the European system, may only be used for the purposes for which the owner of said Data has granted consent. The individual must be notified of any further or different proposed use of the Data in order to obtain his consent. Moreover, the person responsible for the Database should:

- maintain and treat the data as provided by the individual and update it in order for it to be accurate;
- data which are incomplete, inaccurate or were not included by the individual, must be modified in order to be accurate;
- data, which are no longer necessary or relevant for the purpose of the Database, should be cancelled and destroyed.

Protection of the Data and Database

The Law forbids the person responsible for the Database to record any kind of personal data in Databases that do not provide assurance of the integrity and/or security of said data. Moreover, it is necessary that said person, adopts all the technical and organisational measures necessary to avoid non-authorised access to, loss of, or modification of the data. The amendment poses a burden on the Federal Government to put in place a regulation establishing further requirements and minimum conditions of security and organisation, taking in to consideration the technology available, the nature of the data and the risks to which said data may be exposed.

Data must be kept secret and must not be transferred or assigned to another party[1] without previous consent of the individual who owns the data. Also, the individual has the right to know the identity of the assignee, the data assigned and the purpose of the assignment of the Data.

Transfer Data to countries or international entities may only be possible if said country's data protections standards regarding security and protection of databases are at least equivalent to those provided by Mexican legislation. The strict approach to the European regulations on this matter may cause a barrier to the economic relations with countries that follow the North American System.

Current Status of the Data Protection Law

As mentioned previously, the Senate of the Republic has approved the Data Protection Law. The next step, according to the Mexican legislative process, is the revision of the project by the House of Representatives. On September 5, 2002 the project was assigned to a commission that will study it and organise a plenary session for its approval. Later, if the House approves it fully and without modification, the referred project will pass to the President of Mexico for his personal approval and publication. Due to its entailment with the Law of Transparency, which has been in force as from June 13, 2002, it is estimated that the Data Protection Law will finally be approved in the next ordinary session of the House, and enacted later in 2003.

It is expected that the new Data Protection Law will afford individuals wider protection of their data from the misuse and abuse by others. However, the application and legislation related to it is complex and diverse. Nevertheless, in the event that the Data Protection Law is enacted, it will establish strict requirements for companies or individuals that collect personal data from their clients, including data held in Databases (supported by any means), as well as its treatment[2] and use, which will very likely have a negative impact, particularly in the areas of market research and publicity.

1 Other parties may include individuals or companies other than the ones that obtain the information, even if these are affiliates or related in any way to the company.

2 The treatment of data is considered differently from the use of the data itself; it includes the information obtained from operations or systematical procedures to which the data may be subject.

E-Government in Italy: The Use of SMS by Public Utilities

By Avv. Alessandro del Ninno, Information & Communication Technology Department, Studio Legale Tonucci, Rome; e-mail: adelninno@tonucci.it

Introduction

On May 15, 2003 the Italian Data Protection Authority enacted an important regulation (hereinafter: "Regulation") on the correct protocol for the sending of Short Message Services ("SMS") by mobile phones for public utility purposes. Such Regulation adds to the other recent guidance issued by the Italian Data Protection Authority ("IDPA") on March 14, 2003 related to the use of MMS in compliance with the Italian provisions on the protection of personal data (set forth in the Law No. 675/1996 and further modifications and amendments – *see World Data Protection Report, April 2003*).

The IDPA is the first data protection agency in Europe to introduce guidelines for the correct use (*i.e.*, compliant with the protection of privacy) of some of the new TLC services provided by the recent mobile technologies (SMS and MMS). While the rules are not enforced by an Act of law (and therefore do not have a "legislative" value) they can provide some practical guidance for compliance in practice.

The regulation on public utility SMS is the result of a specific inquiry carried out by the IDPA with regard to agreements between public bodies and providers of TLC mobile services aimed at sending shot messages, containing news or information related to activities or tasks pertaining to institutional or public bodies, to mobile phone users. In its inquiry, the IDPA noted that public utility SMS are sent according to different hypothesis and aims:

- In cases of emergency, agreements between public bodies and TLC providers are aimed at sending public utility SMS to subscribers of TLC mobile services who are located in a specific geographical area at a certain time, for example, traffic information on road congestion, road closures *etc.*, in the immediate area. In such cases, SMS are usually sent without prior request from the addressee to receive them.
- In other cases, SMS are sent to inform the addressees about, *e.g.*, levels of air pollution.
- Other initiatives (under consideration only at this stage) are related to informational campaigns organised by central or local administrations with the aim of making citizens aware of certain dates or issues (*e.g.*, World AIDS Day) or with the aim of spreading – by means of SMS sent in collaboration with TLC mobile services providers – information deemed to be of a public utility (cultural happenings, road conditions, fiscal or tax payment terms, validity of documents, *etc.*).

Privacy Implications for Public Utility SMS

The above-mentioned activities imply a processing of personal data related to subscribers of TLC services or holders of rechargeable telephonic cards. The IDPA points out that sometimes the processing relates to the telephone number alone; in other cases it is specifically targeted at a certain subject or categories of interested subjects.

Further, the processing of personal data can only be carried out by either the provider of a TLC service, or by the provider of the TLC service in collaboration with the public body who decides the initiative to be communicated. In both cases, the rules contained in the Italian privacy law No. 675/1996 (and in particular the provisions related to the protection of privacy in the TLC sector, set forth in the Legislative decree 171/998, amending the Law 675/1996) shall apply.

In such cases, the IDPA (which has recently published its annual report on the developments of data protection in Italy for the year 2002) deems it necessary to verify how personal data will be protected when the sending of public utility SMS occurs. Such clarification is needed particularly, if one takes into consideration the invasive nature of the frequent receipt of SMS by a mobile phone user. The receipt, in fact, presupposes the utilisation a) of a datum (*i.e.*, the mobile number) which is generally considered as strictly personal and confidential; and b) of a device (*i.e.*, the mobile phone) by means of which it is possible to reach and contact the user or the subscribers at any time and in any location.

So, the IDPA points out that we are currently facing a situation characterised by a new trend of considering the mobile phone (usually a device utilised by individuals mostly for inter-personal communication) for new and more efficacious (also interactive) kinds of institutional communications.

Beyond privacy implications, the sending of SMS for public utility purposes must also be analysed in light of the discipline introduced by Law No. 150 of June 7, 2000, regulating the information and communication activities carried out by the Public Administration. Amongst others, such law (Article 2) aims at enhancing:

> "any mean of communication suitable for guaranteeing the necessary diffusion of institutional messages, also by means of civic networks, integrated communication initiatives, telematic or multimedia systems".

In any case, Law No. 150/2000 does not provide specific rules regulating the processing or use of personal information by or on behalf of public bodies; on the other hand, it generally provides that the institutional activities for information or communication purposes must comply with the data protection laws (Article 1, para 4, Law No. 150/2000).

In conclusion, the sending of SMS for public utility purposes must be analysed according to a whole set of rules, not ignoring apparently secondary aspects implied

by this issue, such as inconveniencing addressees with an uncontrolled amount of institutional SMS from a growing number of public senders; receipt of delayed messages during anti-social (night) hours; and eventual charge of partial costs (*i.e.*, according to the fees applied by the TLC Operators, in cases of receipt of SMS abroad).

Public Utility SMS: A General Classification

According the IDPA's inquiry, public utility SMS can be classified by considering the different modalities for the sending thereof:

(a) Institutional SMS sent by telephonic operators on behalf of public subjects according to emergency situations and using subscribers' personal data, without sending such data to the public subject who has requested the sending of SMS; such cases have to be distinguished from exceptional situations (for example, natural disasters, matters of national security, *etc.*,) in which the public authority adopts compulsory orders making an exception to existing rules;

(b) Institutional SMS sent by providers of telecommunication services, on behalf of the public subject, with the purpose of informing people about cultural event, deadlines, etc.

(c) Institutional SMS sent directly to the public subject without the co-operation of the telecommunications operator, by direct use of the subscribers' personal data retained by the same telephonic operator.

The IDPA Guidelines

In the case of point (a) in the previous paragraph, the telephonic operator who retains the subscribers' personal data (being consequently the "Controller" according to the Italian privacy Law No. 675/1996) carries out and satisfies a public subject's request, and without sending any personal data to the public authority concerned, sends public utility SMS by using the telephonic numbers related to subscribers or to owners of pre-paid telephonic cards, and eventually data related to the location of the mobile phone at a certain time. Other kinds of personal data can be automatically processed according to different situations and on the basis of the purpose of the SMS (for example, birth date for SMS related to addressees included in a certain age bracket; gender for SMS inviting women to undergo mammary screening, *etc.*).

Even if the public authority does not acquire or have disclosed to it personal data identifying data subjects, this does not mean that the related processing is in any case free and allowed. In fact, the current legal framework does not include the telephonic numbers amongst the personal data which can be processed without requiring a prior consent as happens for "data listed or contained in public records, lists, acts or documents knowable by anybody" (see Article 11, Law 675/1996). On the other hand, utilisation of telephonic numbers by telephonic operators must be based on a prior, free and express consent given by the data subject and documented in writing (the consent can also be given orally, as it must be express, but the telephonic operator must eventually prove in writing that an express or verbal consent has been given).

It should also be noted that the regulatory framework and procedure related to the setting up of a General Public Directory (to include mobile phone numbers) is still under way, and the new scenario shall affect the entire process. In any case, the principle of a compulsory prior consent shall also be valid after the introduction of the new General Public Directory.

In case of emergencies and natural disasters, telephonic operators can send public utility SMS and can set aside the request of a prior consent only if the need to comply with a legislative obligation is required, or if a compulsory order is adopted by a public authority for public reasons and according to the laws. In such cases, Law 675/1996 can be derogated. But the IDPA states that the results of its inquiry have pointed out that in several cases the order adopted by the central or local public authority (and the successive request to the telephonic operator for the sending of SMS) was limited to an intervention within an emergency situation, for example verifying a condition of atmospheric pollution and limiting urban traffic, but without adopting orders in compliance with the compulsory emergency requirements provided by the laws.

Even when the public authority has enacted a compulsory and urgent order, according to cases of disasters, emergencies or lodestones, very often nothing has been provided, either directly or indirectly, with regard to exceptional modalities of information to citizens. In such cases, the public authority could eventually wield its power to derogate not only the laws about exceptional events, but also those regarding the processing of personal data by telephonic operators.

On the other hand, a specific provision derogating (for the processing of personal data) the obligation of obtaining prior consent from the data subject must be provided in the compulsory and urgent orders. So, in such cases, the public authority must previously evaluate if:

- the legislative rules providing the power to enact compulsory and urgent orders also gives the public authority the power of derogating to the law related to the processing of personal data; and
- once verified the precondition of a dangerous emergency situation, such situation may or may not be managed by means of ordinary and non exceptional means.

With regard to the other institutional communications or public utility SMS with the purpose of informing people about cultural event, deadlines, *etc.*, being such communications not based on emergency situations as seen above, the IDPA points out that the compulsory principle of achieving the data subject's prior consent cannot be derogated. Independently of the aim

for which the telephonic operators intervene, they must comply with the so-called "proportionality principle" in the processing of personal data set forth in Article 9 of the Italian Law on Privacy No. 675/1996. Accordingly, telephonic operators must employ modalities of communication which prevent the nominative identification of the subscribers. Further, telephonic operators must use personal data processed for the communication (including the information related to the subscribers' location) exclusively for the purpose of sending, and in compliance with the limits and the time strictly necessary to send such SMS. The IDPA also suggests that public utility SMS could be prefaced by a short indication of their purpose (for example, "institutional information", or "public utility SMS"). In this way, SMS's efficacy could be strengthened yet further.

Telephonic operators must previously and adequately inform subscribers or holders of pre-paid telephonic cards about the possibility of receiving public utility SMS, also in cases related to emergency situations (unlike otherwise provided for by law) where the telephonic operator acts on the basis of a public authority's compulsory orders (as explained above). Further, data subjects must be provided with the opportunity to freely express their consent in a specific form (and also to give such consent for some categories of institutional messages but not for others). On these points, the IDPA suggests achieving compliance with the above mentioned qualifications by inserting the related information in the contract stipulated with the user for the subscription of a telephonic service or for the purchasing of a pre-paid telephonic card. On signing the contract, the telephonic operator must promptly inform the interested subject about the purposes and the modalities of the data processing, including the possibility of receiving institutional SMS or SMS of public utility, and the modalities for the data subject to exercise his right for privacy protection. Further, beyond the form containing the contract, the telephonic operators must provide the subscribers – before the sending of SMS – with a separate form including the information and request for consent, which has to be given in writing or orally by means of a specific help desk (but in this case the telephonic operator must also retain written evidence of this verbal consent, for example by keeping its written request to the data subject for processing, or by keeping the information about the consent given by telephone: name of the data subject, date and time of the telephone conversation, *etc.*). In any case, the data subject must be able to exercise his rights easily and freely, even in the case of a previously given consent.

Further, a concrete possibility to exercise the right of refusing (on signing the contract or successively) the receipt of institutional SMS, sent without the request of prior consent, but according to urgent and compulsory orders, must be guaranteed by the telephonic operators to the data subject. In such case, for example, a specific option for refusal should be inserted in the same SMS being sent out. Telephonic operators are only requested to comply with the latest indication if the public subject – for public and urgent aims – has specifically ordered the operator to send SMS based on emergency situations.

With regard to the proposal made by some telephonic operators, with regard to the setting up of specific lists of telephonic numbers related to subjects who have given their consent to the receipt of institutional SMS, the IDPA points out that such hypothesis presupposes that each single telephonic operator had put its clients in the condition of expressing an aware and distinct consent on every possible data processing and on any purpose. The lists shall have to be differentiated and updated according to the categories of messages for whose sending the interested subjects have given their consent.

On the other hand, the eventual setting up by the telephonic operators of specific directories containing telephonic numbers related to subscribers who have not given consent for the receipt of institutional SMS is considered by the IDPA as a licit but merely internal organisational measure, which cannot in any case imply the burden for the interested subjects of enrolling in such lists, or of expressing their dissent.

Direct Sending of SMS by a Public Authority

This case regards the different possibility of the direct sending of institutional SMS by the public subject, using the personal data which it holds. What can happen, is that within the ordinary administrative relationships between public authorities and citizens, the public authority collect personal data directly from data subjects who are interested in being informed about specific things (for example, accessing administrative documents) or in receiving messages, sent by certain public offices, or put at the citizen's disposal online.

In such case, the public subject is also allowed to communicate institutional information by SMS, without requiring a prior consent, but within its institutional tasks and for the sole purposes of answering a specific request made by the data subject. In any case, the public subject shall have to provide the addressee with proper and detailed information with regard to each specific aim for which the SMS is related.

With regard to the above, it is necessary for the processing of any personal data (because of the lack of a prior consent given by the data subject) to be based on a specific task amongst those falling within the public subject's competence. Such task must be clearly indicated to the interested subject, fully explaining the different contexts (for example, by distinguishing the data collecting operations aimed at sending tax information, from the data collecting operations related to the sending of information about cultural events).

Should the public subject – "controller" of the processing as per Law 675/1996 – send institutional SMS, not directly, but by means of external subjects (for example, a specialised company who manages the sending of SMS on behalf of third parties), it shall have to specifically appoint such external subjects to be responsible for the processing.

In conclusion, the IDPA's intervention has provided some important practical rules with regard to the development of e-government services in Italy, a country which at European level is one of the most advanced in this sector.

News

ESTONIA

Legislation Amended in Line With E.U. Norms

The Riigikogu (parliament) passed the Personal Data Protection Act on February 12, 2003.

The Act brings protections for personal data into compliance with the data protection rules applicable in the European Union, in particular with Directive 95/46/EC of October 24, 1995.

The new Act does not prescribe substantial changes in the principles laid down in the former Act, but elaborates its wording and terms.

The Act enters into force on October 1, 2003. The former Act of 1996 becomes ineffective from the same date.

By Raino Paron, Raidla & Partners, Tallinn; e-mail: raino.paron@raidla.ee

EUROPEAN UNION

Commission Reports on the Data Protection Directive

BRUSSELS—Although all but one European Union Member State has now implemented the European Union's 1995 data privacy directive, wide differences in national laws and how they are implemented make it difficult for companies to operate Europe-wide data processing systems and thus take advantage of the benefits of the internal market.

These are the conclusions of the European Commission's "First Report on the Implementation of the Data Protection Directive". The report, which was published on May 16, 2003 comes a year and a half later than originally planned, due to Member States' slowness in transposing the directive into national law. While the E.U. executive said it would be "premature" to propose amending the law at this point, it does lay out a work plan aimed at narrowing divergences among national measures and bolstering enforcement.

> "I am pleased that most businesses seem to appreciate that the directive has made it easier to move data around and that maintaining the free movement of data depends on their meeting their data protection obligations", said E.U. Internal Market Commissioner Frits Bolkestein. "But E.U. law can only work if Member States implement it on time, so I deplore the long delays in many Member States."

He called on France, the only E.U. country that has not yet implemented the directive, to rectify the situation urgently.

Eliminate Differences

The main impetus behind the European Directive on Data Protection (95/46) was to eliminate differences in the way Member States approached the issue of data privacy. Since its adoption, the proclamation of the European Union's Charter of Fundamental Rights by the European Parliament, the Council of Ministers and the Commission in December 2000 has given added emphasis to the privacy dimension of the directive.

Findings in the report were based to a large extent on a broad consultation begun in 2002, in which all stakeholders –governments, institutions, businesses and consumer organisations, companies and citizens – were invited to express their views (see *World Data Protection Report, July 2002*). The Commission received nearly 10,000 responses to an online questionnaire in addition to 80 written contributions, mainly from businesses.

Implementation of the directive has been slow, with only four Member States passing national laws by the October 1998 deadline E.U. governments themselves established in adopting the directive. In December 1999, the Commission took France, Germany, Ireland, Luxembourg and the Netherlands to the European Court of Justice for failure to comply.

Germany and Netherlands, along with Belgium, implemented the directive in 2001, and Luxembourg in 2002 after a court ruling against it. Ireland only recently passed legislation (*see World Data Protection Report, May 2003*) though has not yet formally notified the Commission. That leaves only France, which has still not yet amended its 1978 data protection rules to comply with the directive.

Unauthorised Data Transfers?

Among countries that have already updated their legislation, there are still large differences in both the laws and the ways in which they are applied in practice. One area in which there are still wide discrepancies and where enforcement is lacking is in the transfer of data outside the European Union. The report notes that although national authorities are supposed to notify the Commission when they authorise such transfers, the Commission has received only a very limited number of notifications.

> "This suggests that many unauthorised and possibly illegal transfers are being made to destinations or recipients not guaranteeing adequate protection", the report says.

There are also wide differences in the notification companies are required to make when using the data of private citizens. In their comments to the Commission,

the European Privacy Officers Forum and the E.U. Committee of the American Chamber of Commerce said that this leads to difficulties for multinational companies operating on a pan-European level.

In order to narrow differences in national legislation and enforcement of the rules, the Commission laid down an action plan which it intends to review in 2005, at which time it will decide whether it is necessary to make proposals for amending the directive.

Among other things, the action plan calls on the Commission to:

- hold bilateral meetings with Member States to discuss ways to bring national laws fully in line with the requirements of the directive, as well as discussions with the 10 new countries set to join the European Union in 2004;
- co-operate closely with data protection authorities and Member States to collect information about implementation, identify areas where there are gaps and seek to fill those gaps as quickly as possible; and
- simplify the requirements for international transfers.

Voluntary Codes, Self-Regulation Urged

But there is more to data protection than legislation. In the report, the Commission also urged business sectors and interest groups to come forward with voluntary codes, arguing that self-regulation, and codes of conduct in particular, should play an important role in the future development of data protection both within the European Union and elsewhere.

In order to raise awareness about data protection, the Commission plans to launch a "Eurobarometer survey", similar to the online questionnaire it conducted in 2002. Some of the findings of the 2002 survey were as follows: 44.9 percent of respondents consider the level of protection a minimum; 81 percent thought the level of awareness about data protection was insufficient, bad or very bad, while only 10.3 percent thought it was sufficient. A little more than 3 percent thought it was good or very good.

Data controllers also had a very negative view of citizens' awareness, with 30 percent calling it insufficient and only 2.95 percent saying it was very good. Data protection rules have a high acceptance among businesses, with 69.1 percent of data controllers considering data protection requirements essential while only 2.64 percent regard them as completely unnecessary.

A large majority of the data controllers that responded to the questionnaire – 62.1 percent – did not consider that responding to individuals' requests for access to their personal data required a large effort for their organisation. Most of the data controllers either did not have figures available or received fewer than 10 requests for all of 2001.

The Commission has urged Member States to devote more resources in raising awareness, in particular via the budgets of the national supervisory authorities.

The report, a technical analysis of implementation in E.U. Member States and the results of the online survey, can be found online at the Internet at *http://europa.eu.int/comm/internal_market/privacy/lawreport_en.htm*.

See also "95/46: The Case for Proper Reform", World Data Protection Report, December 2002.

INTERNATIONAL

Proliferation of Data Privacy Laws Challenges Multinationals

A new survey by global law firm White & Case examining cross-border data transfer laws in 22 major jurisdictions shows a growing proliferation of data privacy laws throughout the world. This proves problematic for multinational corporations with operations or markets in multiple jurisdictions since sharing electronic data between jurisdictions often raises different issues depending where the data came from and was sent to. It can get very difficult to know what information can legally be sent where, and it's vital for companies to know what they must do to protect themselves and their data.

To illustrate the challenge, if a company needed to move data without the data subject's consent between Spain and Australia to protect that individual's vital economic interests, one generally could send it from Australia, but not Spain. If the company needed to transfer the same data due to a legal claim, one could send it from Spain, but not Australia. Still other jurisdictions in the survey, such as South Korea, generally forbid the data to be transferred for either reason.

In all, the survey covers eight jurisdictions in Europe: France, Germany, Hungary, Italy, Poland, Russia, Spain and the United Kingdom; seven in the Asia-Pacific region: Australia, China, Hong Kong, Japan, Malaysia, South Korea and Thailand; and seven in North America: Canada, Mexico and the United States, as well as the Canadian provinces of Ontario and Quebec and the U.S. states of California and New York. These four prominent non-sovereign jurisdictions were included because they have been particularly active in the privacy law area.

The research found that 11 of the surveyed jurisdictions treat cross-border data transfers differently from those moved only within their domestic borders, and five more jurisdictions have laws proposed or pending that would affect cross-border data transfers differently from transfers within their borders. In particular, 12 of the jurisdictions impose restrictions of various kinds on moving personal data across borders, and five others would do so under proposed or pending new laws. Of the nations surveyed, only China, Japan and the United States permit such data transfers generally unimpeded.

Even the most routine cross-border transfers can cause problems for businesses. Multinationals often ex-

perience the full burdens and inconsistencies of the privacy regime, even in relation to transfers of often quite run-of-the mill data, such as sharing business contact information among its own business units.

For example, Mark Powell, an information technology attorney and expert in European competition law in White & Case's Brussels office, recently observed that while

> "E.U. Member States accept in theory the Data Protection Directive, there is still … confusion about how the directive is interpreted by the individual Member States, with some nations going beyond the directive guidelines to severely limit the sharing of any personal data outside the home country, while others interpret the requirements more liberally".

The E.U. Data Protection Directive allows the transfer of data between E.U. states and to other nations that have an "adequate level of protection". However, there is a question about what an "adequate level" of protection means for non-Member States and how that can be demonstrated. This is one of the key components currently being discussed before the European Union and must be ironed out before the requirements can be applied broadly.

By contrast, most countries in Asia and the Pacific Rim currently impose less restrictions when it comes to the transfer of cross-border data. The primary exceptions are Australia and South Korea. Australia has adopted similar restrictions as those laid down by the European Union, while South Korea has extremely strict requirements in that an individual must grant a company explicit consent in order for that company to transfer personal data across borders.

Kim Rooney, a White & Case partner in Hong Kong, has noted that of all the jurisdictions surveyed, South Korea seems to have the toughest restrictions when it comes to cross-border transfer issues. She recently stated:

> "South Korea not only requires prior positive consent from the individual data subject to transfer data outside the country, but even with such consent prohibits the overseas transfer of critical information, such as high-technology developed in South Korea, altogether. This could cause additional problems as South Korea continues to grow in importance as a key economic market".

The White & Case survey was released in Spring 2003, in conjunction with the Third Annual White & Case Global Privacy Symposium, linking speakers and guests at the Firm's offices in Brussels, London, New York and Washington. The survey was inaugurated in 2002, to supplement last year's Global Privacy Symposium, and to our knowledge it is still the only publicly available in-depth survey of privacy laws in the world's major jurisdictions as they affect international businesses.

Key findings of the survey include the following:

- Most jurisdictions surveyed treat cross-border information flows differently than they do data exchanges within their domestic jurisdiction. The United States, including New York and California, Canada (at the federal level), China, and Japan are the key exceptions. In addition, France, Malaysia, Mexico, Thailand and Ontario are considering proposals that would impose different requirements on cross-border and internal transfers.
- Twelve jurisdictions restrict data flows across borders, and four, Malaysia, Mexico, Thailand and Ontario, currently are considering proposals to do so. Hong Kong has passed restrictions on data flow across borders, but the new legislation has not yet been put into operation. Those without such restrictions are China, Japan, the United States, and the two U.S. states in the survey, California and New York.
- The European Union's Data Protection Directive has become a benchmark by which many jurisdictions measure the adequacy of their data-transfer controls. The Directive permits transfer of data to non-E.U. jurisdictions where the receiving jurisdictions provide an "adequate level" of privacy protection. Indeed, the Eastern European countries seeking to join the European Union are in some cases already bringing their laws into compliance with the Directive.
- Of the 12 jurisdictions that have restrictions on cross-border transfers, and the five either pending or considering them, all would permit transfers with the consent of the data subject. Most require "opt in" consent, in which the data subject must affirmatively give consent. Australia, the United Kingdom and Quebec permit "opt out" consent, in which the data subject must affirmatively withdraw consent in order to prevent data from being transferred outside the jurisdiction.

For multinationals that transport data across borders, the survey findings underscore the need to be mindful of some key points. First, multinationals should consult counsel knowledgeable about cross-border transfer laws in the particular jurisdictions where their companies do business to ensure they are in compliance with current laws and to plan accordingly as new laws emerge. Secondly, companies need to review their current data privacy polices and determine if they are being implemented properly. Thirdly, companies should consider undertaking a privacy audit to determine how their data transfer and other privacy-related policies and practices compare with the laws and rules of the jurisdictions in which they collect information. Though the growing number of privacy laws around the world can be a major challenge for multinationals, foresight and preparation can help keep the headaches of compliance under control.

A full copy of the 2003 White & Case Global Data Protection Survey is available online at *www.whitecase.com/*.

By Robert L. Raskopf, White & Case LLP.

Robert L. Raskopf *chairs White & Case's E-Commerce, Media and Technology Group. He regularly counsels multinational clients concerning compliance with the growing global privacy data requirements. He also litigates cases in which personal and professional privacy, sensitive business information and law enforcement interests are weighed against common law and First Amendment rights to information.*

NEW ZEALAND

New Telecommunications Information Privacy Code Released

Following 18 months of public and industry consultation, the New Zealand Privacy Commissioner has issued the Telecommunications Information Privacy Code 2003, pursuant to the Privacy Act 1993.

The code affects telecommunications agencies in their handling of personal information about customers and users of telecommunications services. The code covers, for example, telephone companies, the publishers of telephone directories, Internet service providers, mobile telephone retailers and many call centres.

The code is intended to help individuals and the telecommunications industry alike. Some of the benefits to individuals will include, for example:

- cementing-in existing good practices (for example, ensuring that subscribers need not pay to keep their details from being published in the telephone book as was formerly the case);
- requiring "blocking" options to be available free of charge when caller ID is offered with agencies to take steps to make subscribers and users aware of these options;
- prohibiting the use of traffic data gained from interconnection for unauthorised direct marketing;
- requiring internal complaints handling processes which meet certain minimum standards;
- prohibiting the inclusion of personal details in a reverse search facility without individual consent;
- providing more control to subscribers as to the way in which names and addresses appear in the telephone book (this last requirement being delayed until 2005 to provide a lead-in for changes to telephone directories).

The major telephone companies spent considerable effort developing a draft code some years ago and a number of its elements have been carried forward into the issued code. Benefits for telecommunications agencies might be counted as including:

- the establishment of a set of rules which have been tailored to the terminology and circumstances of telecommunications;
- the conferral of new discretions upon telecommunications agencies in relation to the collection, use and disclosure of personal information through the inclusion of special exceptions not found in the Privacy Act (for example, allowing for the disclosure of information for the purposes of preventing or investigating an action or threat that may compromise network or service security or integrity or to assist a foreign law enforcement authority in the prevention, detection, investigation and prosecution of a breach of a foreign telecommunications law).

There are a host of privacy issues in respect of telecommunications and the code does not seek to address them all. Many such issues will continue to be addressed under the more general information privacy principles in the Privacy Act. For example, the code does not cover ordinary businesses in respect of their use of the telephone or e-mail.

The code does however, provide a solid base from which additional telecommunications privacy issues (for example, retention of traffic data; monitoring of employees' telephone calls and e-mails; telemarketing and the use of location data) can be addressed in future amendments.

UNITED KINGDOM

E-Government Progress Hampered by Data Protection Laws

E-government progress is in danger of being held back by the current legal quagmire of data protection and freedom of information law, according to a new survey by Headstar (*www.headstar.com*).

Around a third of public sector respondents to the survey said that the Data Protection Act 1998 – which is intended to safeguard personal information – was preventing them from "joining up" and putting services online when this involved the sharing of data between departments or agencies. Furthermore, a quarter foresaw difficulties fulfilling their obligations under the Freedom of Information (FOI) Act 2000 and FOI (Scotland) – which oblige them to disclose information to the public when asked, unless exempted by other laws.

More worryingly, however, respondents seemed to feel that the obligations imposed by the two acts could clash with each other. Said one, "some of the information we are required to make available under the Freedom of Information Act would require the gathering of data which seems to contravene parts of the Data Protection Act". The Lord Chancellor's Department is due to publish advice on resolving legal problems relating to information management later in 2003.

Headstar's full survey was published in May 2003 in "E-Government Outlook 2003–04: Key Steps to Successful Services" which provides a round-up and analysis of events over the last year in the U.K. e-government sector. Details of how to order a copy of the report are available online at: *www.headstar.com/ outlook*

UKauthority.com – a news and information service for local e-government

The Next Great Trans-Atlantic Voyage: E.U. Laws Protecting HR Data Arrive on America's Shores (Part I)

By S. Atkins, P. L. Gordon and S. J. Wenner of Littler Mendelson, in collaboration with G. Clayton, Founder and Chairman of the Privacy Council

Introduction

Globalisation! The much-ballyhooed war cry of American business during the past decade could soon become a double-edged sword for United States businesses with employees in the European Union. The European Union's fifteen[1] Member States have slowly commenced enforcement of, or will soon begin to enforce, unprecedented privacy-based restrictions on the "export" to the United States of "personal data" concerning E.U. residents. These new barriers, raised in consequence of the European Union's Data Protection Directive (the "E.U. Directive"), affect far more than the well-publicised transfers of customer information generated by businesses engaging in e-commerce. Virtually every transfer of human resources data from operations, affiliates, or subsidiaries in the European Union to U.S headquarters or business units – even a transfer of basic personnel information such as an employee's name, work address, and work telephone number – is subject to these restrictions and triggers broad obligations.

Given the imminent enforcement of European laws regulating the transfer of data from the European Union to the United States, in-house counsel and human resources professionals at U.S. corporations with employees in the European Union must assess, if they have not done so already, whether, and how, to put their company's information-handling practices in line with the European Union's data protection standards. Compliance will require many corporations to radically change how they collect, store, use, transfer and disclose – *i.e.*, "process" – their human resources data. This is because what many human resources professionals in the United States would consider to be "business-as-usual" data handling practices are patently illegal under data protection laws in Europe where privacy is considered a fundamental human right. That, in turn, places both the European transferor and the U.S. transferee at risk.

It is reasonable for members of the legal and human resources departments to ask why they should prevail upon their companies' business units to commit scarce capital, time, and attention to an effort that might appear quixotic in the context of the United States business culture. The answer: non-compliance with European data protection laws is a smoldering ember which, if left unattended, could suddenly engulf your company in a conflagration of bad publicity, civil lawsuits, government enforcement actions, loss of important data, and internal recriminations.

While the European enforcement record remains relatively undeveloped at this early stage, authorities in E.U. Member States have been authorised to levy corporate fines ranging from small amounts per offence to close to $600,000 per offence (in Spain).[2] Not only are some corporate employees financially at risk, but they and their employers could also face criminal prosecution (in Italy[3] and in the United Kingdom,[4] for example), with convictions for particularly egregious violations resulting in imprisonment. Perhaps even worse for the corporation, an offending business could be barred from eligibility to receive and use personal data coming from Europe, and could be ordered to destroy any such data that it acquired unlawfully. Finally, the bad publicity associated with these enforcement actions could seriously tarnish a corporation's hard-earned public image. Put simply, no U.S. corporation can afford to ignore the European Union's data protection regime.

This paper will address the practical impact of the E.U. Directive on human resources management at U.S. companies with European operations. We will also explain the three most practical options that in-house counsel and human resources professionals should consider as they develop strategies to help guide their business through uncharted terrain. In the end, this paper should equip the reader with a basic understanding of how the data protection laws now directly applicable to their corporation's European operations will demand new approaches to the collection, storage, use, and disclosure of human resources data at U.S headquarters as well as in Europe, and the options for addressing this change.

How the E.U. Directive Affects Your Human Resources Functions

The Basic Principles of the E.U. Directive

The E.U. Directive, which was enacted in 1995, required the 15 E.U. Member States to implement national data protection laws by 1998. The Directive established minimum standards for these national laws. However, the Directive's standards are broadly written, leaving room for interpretation and interstitial legislation by each Member State to fit its own social and political culture and its national experience.

As a result, strong common threads will be seen running through the data protection laws of all E.U. Member States, but there are also important distinctions from country to country. United States in-house counsel and human resources professionals advising a company with employees in, for example, the United Kingdom, Belgium, and Spain must be prepared to encounter three separate, but related, sets of data protection laws

administered in those nations by different administrators and through differing procedures.

To communicate effectively with European counterparts and European data protection authorities, human resources professionals in the United States and their legal advisors must become familiar with the Directive's data protection lexicon. The key terms most foreign to U.S. notions of privacy law are defined below:

- *personal data*: any information relating to an identified or identifiable natural person;
- *sensitive personal data*: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health, or sex life;
- *data subject*: the natural person to whom personal data relates;
- *processing of personal data*: any operation, or set of operations, performed on personal data, whether or not by automated means (such as collection, recording, organisation, storage, transfer, alteration, retrieval, use, or disclosure);
- *data controller*: the person or entity who alone, or jointly with others, determines how, and for what purpose, personal data will be processed;
- *data protection authority*: the national regulatory agency responsible for ensuring that data collectors comply with national data protection laws.

The E.U. Directive requires enactment of national laws throughout the European Union that establish strict limits on the processing of personal data, impose significant obligations on the data controller vis-à-vis the data subject, and confer substantial rights on the data subject vis-à-vis the data controller. As applied to the employment context, the Directive's chief principles guiding the application of data protection laws include the following:

- *Legitimacy*: the employer (the "data controller") may process an employee's (the "data subject's") personal data only (a) with the employee's prior consent; (b) as necessary to perform the employment contract; or (c) to the extent necessary to comply with legal obligations.
- *Notice*: before processing personal data, the employer must inform the employee of the personal data being collected, how and why the personal data has been or will be processed, to whom the data has been or will be disclosed, and whether the data will be exported outside the European Union or to a country which does not provide "adequate" protection.
- *Proportionality*: the employer may process data for the purpose disclosed to the employees, or for a compatible purpose, but in all events the personal data, which are processed must be the minimum necessary to carry out that purpose. It would violate the "minimum necessary" requirement, for example, to require a job applicant to provide the European equivalent of a social security number if that number will not be used in connection with the hiring process.
- *Access*: the employer must (a) grant each employee's reasonable request for access to the personal data it maintains; (b) provide each employee with the opportunity to correct, erase, or block further processing or transfers of inaccurate, outdated, or incomplete data; and (c) notify any third party to whom inaccurate, outdated, or incomplete data has been disclosed of any additions or corrections made in response.
- *Security*: the employer must protect the data from unauthorised access and disclosure.
- *Training*: the employer must train employees, as appropriate, in applicable data protection requirements.

The precise application of these abstract concepts to the day-to-day human resources functions of a business enterprise employing dozens, or thousands, of employees is a complex matter still being debated at the European Union's highest levels and refined at the national level. What is clear, however, is that the national laws implementing the Directive's broad principles will apply to and generally limit the collection, storage, transfer, use, and disclosure of a wide range of human resources data which, in the United States, would be considered freely subject to use and disclosure wholly at the discretion of the employer.[5] For example, national data protection laws of E.U. members will govern, for employees residing in that state, the processing of resumes, job applications, sickness and leave records, performance evaluations, and even employee contact information within the organisation.

While compliance with the national data protection laws implementing the E.U. Directive most likely will fall primarily within the purview of your European counterparts and advisors, the E.U. Directive, nonetheless, demands that you understand what your company must do to comply with those laws and how the data protection authorities where your company has European operations are administering and enforcing those laws. These matters cannot simply be left on the other side of the Atlantic because, as noted above, European data protection authorities have the power not only to levy substantial fines on violators, but also to block transfers of personal data from your European operations. Furthermore, the national laws will govern how data may be processed in Europe before it is transferred to the United States, and thus will determine whether certain data may be transferred at all. And finally, under certain circumstances (described below), your U.S. organisation may have to pledge to co-operate with the data protection authority of each E.U. member from whose country data is exported. These authorities and the laws they administer matter to U.S. corporations doing business in Europe.

The Extra-Territorial Reach of the E.U. Directive

Central to the E.U. Directive is a general prohibition against the "export" of personal data to any country not providing privacy protections deemed adequate under

E.U. standards. The national data protection authority can easily enforce this prohibition because under the E.U. Directive, the national laws of each Member State must require that a data controller seek and obtain approval from the national data protection authority before "exporting" personal data to a non-E.U. country. Circumventing E.U. data protection authorities could have the severe administrative, financial, and even criminal repercussions described above.

Proud as Americans are of their legal system, the European Union has determined that the laws of the United States do not adequately protect personal data. Consequently, when your European counterparts or advisors apply to the appropriate national data protection authority for approval to send even the most basic human resources data to the United States home office, they will bear the burden of demonstrating that one of the exceptions to the general prohibition against exporting human resources data to the United States applies. We discuss below the principal exceptions to the prohibition of data transfers from the European Union to the United States.

Options for Maintaining the Flow of Data

The current regulatory regime offers three principal options for the management of human resources data by United States corporations with employees in an E.U. Member State:

- re-direct transborder data flows to avoid national data protections authorities;
- certify compliance with the "Safe Harbor Principles" negotiated by the U.S. Department of Commerce; or
- provide contractual guarantees of adequate privacy protection.

Deciding which option best suits your organisation will depend upon a host of factors, including the data-processing methods of your European operations, the structure of your company's human resources management, the flow of human resources information within your organisation, and the enforcement perspective of the applicable national data protection authority. We provide a brief overview of each option to assist you in developing strategies to navigate through the new regulatory environment.

Option One: Redirecting Transborder Data Flows

Those United States corporations with employees in Europe having decentralised human resources management may be able to avoid the direct effect of the E.U. Directive on their United States operations altogether by processing human resources data related to E.U. residents only within the European Union. By way of illustration, a United States company with employees in Amsterdam, Brussels, and London could centralise all human resources functions for those employees in Brussels. By taking the United States headquarters out of the human resources data flow, the corporation would avoid the need to adjust its privacy practices in the United States to meet European standards.

In reality, few U.S. corporations with employees in Europe could take advantage of this option. Because national data protection laws apply to personal data related to all E.U. residents, regardless of nationality, all human resources data related to United States citizens working in the corporation's European facilities would have to remain in Europe. United States executives would have to travel to Europe to participate in employment decisions requiring their review of performance evaluations of an employee in a European facility. As a third example, the corporation could not transfer to the United States any human resources information related to a European employee temporarily transferred to the United States.

In each of these situations, the United States corporation, in theory, could seek approval for each specific data transfer on an as-needed basis by demonstrating to the national data protection authority the applicability of one of the exceptions to the general prohibition against personal data exports to the United States. However, reliance upon these exceptions most likely would be both impractical and risky in view of the consequences.[6]

As one exception, the E.U. Directive permits E.U. Member States to allow transborder data flows to a third country not providing adequate privacy protections, like the United States, where the data subject consents to the data transfer.

However, that consent, to be effective, must be "freely given." In the employment context, consent can be freely given only if:

- the employee receives prior notice of the purpose for the data transfer; and
- the denial, or subsequent withdrawal, of consent would have no negative ramifications for the data subject.

Thus, an employee would have unfettered power to veto a data transfer intended to permit United States executives to consider his demotion or discharge. Aside from this practical obstacle to relying upon consent, E.U. authorities responsible for interpreting the E.U. Directive have specifically warned employers not to rely upon employee consent when seeking permission to transfer human resources data to a third country lacking adequate privacy protections, both because of the ease with which consent can be revoked and because of the strict standards applied. Furthermore, in some E.U. Member States, such as Belgium, there are categories of data that employees may not consent to having transferred outside the European Union. Any such consent is deemed void, thus leaving that transfer unprotected. In other E.U. countries, such as Germany and Austria, individual employees cannot consent on their own behalf; rather, the consent must be obtained through the employee, and some councils have taken the position that employees cannot freely consent to the export of their personal data to the United States under any circumstances.

The E.U. Directive also permits Member States to allow data transfers to an "inadequate" third country where the transfer:

- is necessary to perform a contract between the data controller and the data subject;
- is necessary to perform a contract between the data controller and a third party for the data subject's benefit; or
- is legally required.

These exceptions would cover, for example, the transmission of payroll information about a U.S. citizen employed in Frankfurt to permit U.S. headquarters to cut a paycheck, to pay insurance premiums on the employee's behalf, and to report to the Internal Revenue Service. However, the administrative delay inherent in first determining which exception applies and then in obtaining approval from national data protection authorities on a transfer-by-transfer basis could be extremely disruptive of such routine functions.

Option Two: Certifying Compliance with the Safe Harbor Principles

Given the importance of the trade relationships between Member States and the United States, government officials on both sides of the Atlantic labored to develop a framework, which would permit a more regularised flow of personal data between E.U. Member States and the United States than would be permitted by reliance solely upon the narrow exceptions described above. The end product of these efforts is a set of privacy protections known as the Safe Harbor Principles. National data protection authorities in the Member States will approve the export of personal data concerning E.U. residents to any United States business which properly certifies its compliance with the Safe Harbor Principles. In-house counsel and human resources professionals considering the Safe Harbor option must understand that there are burdens associated with the benefits of administrative regularity and predictability so that the decision whether to join the Safe Harbor must be thoroughly analysed.

Not surprisingly, the Safe Harbor Principles mirror many of the core principles embedded into the E.U. Directive and, therefore, may be as foreign to United States professionals addressing workplace privacy issues as the terms "data controller" and "data protection authority." The key terms and broad outlines of the Safe Harbor Principles, as applied to the employment context, are described below:

- *Notice*: employers must clearly and promptly advise employees of the purposes for the anticipated use and disclosure of each category of personal data collected, the types of third parties to whom the information will be disclosed, and the procedure for lodging complaints concerning alleged violations of the Safe Harbor Principles.
- *Choice*: for "sensitive" personal information (defined above), the employer must obtain the employee's affirmative consent before disclosing the information to a third party or using the information for a purpose which is incompatible with the purposes for which the employer told the employee the information had been collected. For all other personal information, the employer must give the employee the opportunity to "opt out" of the use or disclosure.
- *Onward transfer process*: the employer must comply with the notice and consent requirements described above before disclosing personal data to a non-agent. The employer may disclose personal data to an agent without notice or consent if the agent provides adequate privacy safeguards, for example, by the agent's own certification to the Safe Harbor Principles or by the agent's contractual agreement to abide by those principles.
- *Security*: the employer must take reasonable precautions to protect personal data from loss, misuse, unauthorised access and disclosure, alteration, and destruction.
- *Data integrity*: the employer must take reasonable steps to ensure that the data is relevant to its intended use, and is accurate, complete, and current.
- *Access*: upon request, the employer must disclose to the requesting employee personal information collected from or about that employee in an E.U. Member State and processed in the United States after transmission from Europe. The employer also must provide the employee with the opportunity to correct, amend, or delete inaccurate information. The employer must notify third parties to whom the data has been disclosed of the inaccuracies.
- *Enforcement*: the employer, through an identified corporate representative, must certify annually to the Department of Commerce that (a) it has implemented policies to enforce the Safe Harbor Principles; (b) it has trained its employees in those policies; (c) it provides an internal complaint procedure for resolving complaints of non-compliance; (d) it periodically audits compliance; and (e) it will co-operate with E.U. authorities investigating complaints of non-compliance and will comply with any recommended remedial action.

Potential Burdens of Safe Harbor Certification

While in theory a corporation is required to apply the Safe Harbor Principles only to personal data received from an E.U. Member State, it would be difficult, in practice, to justify to a company's workforce the much greater privacy rights conferred upon employees residing in Europe, particularly if those employees are United States citizens. Moreover, it may become impracticable to quarantine the personal data to which the Principles must be applied from that which is generated in the United States or elsewhere outside the European Union, risking confusion between "protected" and "unprotected" data. Thus, as a practical matter, compliance with the Safe Harbor Principles may require a complete overhaul of your company's information-handling practices for your entire workforce.

An increased compliance burden is not the only potential cost of certifying to the Safe Harbor Principles. Although certification is purely voluntary, once a corporation certifies compliance to the Department of Commerce, the organisation's failure to live up to that representation in connection with human resources data could result in the company facing litigation in Europe. As noted above (see, "Enforcement"), a company that certifies to the Safe Harbor Principles must agree to comply with any remedy imposed by European data protection authorities empowered to resolve employee complaints that a U.S. employer has violated the Safe Harbor Principles.[7]

Moreover, the Federal Trade Commission could seek administrative penalties for what would be deemed an unfair trade practice (and, in egregious cases, the FTC could request in addition that the company be criminally prosecuted for making false representations to the United States government.) Indeed, FTC Chairman Tim Muris announced in his first major public statement that, under his stewardship, the FTC will emphasise enforcement of existing privacy laws and, in particular, the Safe Harbor Principles. The FTC will not necessarily wait for a referral from European authorities. In the FTC's view, the agency has the power to prosecute domestic complaints of Safe Harbor violations without European authorities first attempting to resolve the complaint.

The Potential Benefits of Certification

On the other hand, there are definite benefits to certification beyond ensuring the predictability of data transfers – itself a huge benefit. Companies certifying compliance with the Safe Harbor may earn a reputation for being privacy-friendly employers among highly prized technical employees, providing a competitive advantage when labor markets tighten. Companies on the Commerce Department's publicly available Safe Harbor list may also burnish their reputation for trustworthiness with online consumers and with the media. Finally, a growing number of countries, including Canada, Switzerland, Japan, Hungary, New Zealand, and Australia, are implementing data protection regimes modeled on the E.U. Directive, in part to ensure that the companies within their borders maintain their own flows of data from the European Union. Certifying compliance with the Safe Harbor most likely would go a long way towards putting your company in compliance with the data protection laws in these countries. Finally, certification to the Safe Harbor Principles can only enhance the reputation of the certifying company in European jurisdictions where its reputation will be important – those where it has a corporate presence or markets its products.

Option Three: Contractual Data Protection Safeguards

The Safe Harbor is not the only option available to those U.S. corporations with employees in an E.U. Member State for which redirecting transborder data flows is not a practical solution. At least where a European facility, affiliate, or subsidiary is organised as a separate entity, the United States company can agree by contract to provide privacy protections for data transfers from Europe that the national data protection authority would deem adequate. For some corporations, these data transfer contracts may be preferable to certifying compliance with the Safe Harbor Principles. For corporations in the banking and telecommunications sectors, which are specifically excluded from the Safe Harbor, agreement to "data transfer contracts" presently may be the only feasible alternative for obtaining quick and routine approval of data transfers to the United States.[8]

To facilitate the use of data transfer contracts, the European Union has developed a standard contract for exports of personal data to countries, like the United States, which do not provide adequate privacy safeguards under E.U. standards. The contract requires the parties to identify the categories of personal data to be transferred; the data subject or categories of data subjects to which that personal data relates; the reason that the data transfer is necessary; and the persons or categories of persons to whom the data importer intends to disclose the imported data. Under these contracts, the data importer agrees that when it processes the transferred data, it will abide by data protection provisions similar to the Safe Harbor Principles. In addition, the contract confers on the data subject the right to enforce the contract's privacy provisions against both the data importer and the data exporter through mediation, arbitration, or litigation (at the data subject's discretion) in the location of the data exporter and subject to that state's laws.[8]

Advantages of the Standard Contractual Provisions

There are two principal advantages to using a data transfer contract instead of certifying to the Safe Harbor Principles. First, the limited scope of a contract may permit the U.S. corporation to avoid the expense and administrative burden of a complete overhaul of its information handling processes to comply with the Safe Harbor Principles. Under the contract option, the corporation must provide expanded privacy protections only for the specific data which are the subject of the contract and the company is not required to conduct periodic compliance audits, engage in routine training, or promulgate an entire set of privacy policies, all of which are contemplated when agreeing to the Safe Harbor Principles. Second, the contract option reduces litigation risks because no corporate executive is required to make a public representation concerning the corporation's privacy practices and because the enhanced data protection obligations are limited to the personal data transmitted pursuant to the contract.

Significantly, the corporation can obtain the benefits of the contract option without necessarily foregoing the predictability of data transfers through certification to the Safe Harbor Principles. National data protection authorities are required to permit data transfers made pursuant to the standard contractual provisions except where those authorities have reason to believe that the data importer has not, or will not, comply with the contract's data protection requirements. Thus, predictability is virtually assured. In addition, the contract is standard

for all E.U. Member States so that a corporation can use the same contract to transfer the same type of personal data relating to its employees in any E.U. Member State.

Disadvantages of the Standard Contractual Provisions

The narrow scope of the data transfer contract has its disadvantages as well. A U.S. corporation, which imports personal data about its customers, or a wide variety of human resources data about its employees, may be required to execute an unwieldy number of contracts to cover the entire spectrum of data categories. In addition, the contracts could hamstring a company that may wish to use the imported data for an unanticipated purpose. By its own terms, the standard contract permits the data importer to use the imported data only for the purpose specified in the contract when the transfer was made. Thus, use for another purpose would place the data importer in breach of contract.

The data subject has the unilateral right to choose whether to mediate a data protection dispute or to bring a civil action in the courts of the Member State in which the data exporter is established. If the data subject and data importer both agree, they also can refer the dispute to arbitration if the data importer is in a country, such as the United States, that has ratified the New York Convention on enforcement of arbitration awards.

However, regardless of the forum selected (mediation/litigation) or agreed to (arbitration), the Standard Contract Clause commits the parties to resolve disputes according to the data protection laws of the data exporter's country. The right of data subjects to choose unilaterally to litigate in the data exporter's courts means that by signing the standard contract in order to receive a data transfer from a source in a Member State, the data importer has subjected itself to the laws and the courts of a Member State. By contrast, U.S. companies certifying to the Safe Harbor are subject to remedial action in Europe for an alleged privacy violation in the United States only if the alleged privacy violation involved human resources data.

1 The present number of members is certain to grow in this decade as nations, many formerly in the Eastern Bloc, who were unable to satisfy the rigorous admission standards earlier, vie for admission.
2 See Organic Law of December 13, 1999 on the Protection of Personal Data, Art. 44(4)(a).
3 See Act No. 675 of 31.12.1996 (consolidated), Chapter VII, Article 35.
4 See, e.g., Data Protection Act 1998, ch. 2, §§21m 47(1).
5 There are exceptions to this proposition at the state level in jurisdictions such as California, which recognise a state constitutional right to privacy that has been held to be applicable to private employment relationships. This is a distinct minority view in the United States, however. More states, e.g., New York, are at the opposite end of the spectrum, essentially recognising only a very limited right of privacy in the commercial context.
6 In addition, the notion that a U.S. company's human resources organisation could avoid contact with personal data from the European Union completely is even less reasonable when it is realised that any personal data, including data developed for *inter alia* sales and marketing purposes, could trigger application of the E.U. data protection mandates for the data transferred.
7 The situation is different if the company's violation of the Safe Harbor Principles relates to its handling of customer data, as opposed to human resources data. In such circumstances, the U.S. company would be subject to sanction only in the U.S. Thus, one of the major advantages of certifying to the Safe Harbor Principles with respect to the processing of customer data is not present when considering whether to certify with respect to the processing of human resources data. A U.S. company may elect to certify with respect to one category of data, but not the other.
8 As of this writing, Safe Harbor protection for financial services and telecommunications companies is under active consideration.
9 The standard contract can be found at *http://europa.eu.int/comm/internal_market/en/dataprot/news/1539en.pdf*.

Scott J. Wenner *and* ***Philip L. Gordon*** *are Members of Littler Mendelson in the firm's New York and Denver offices, respectively. Mr. Wenner may be contacted by telephone or e-mail at: 212.583.2664; swenner@littler.com and Mr. Gordon may be contacted as follows: tel: 303.575.5858; pgordon@littler.com. Shanti Atkins, an attorney, is Littler Mendelson's Allied Business Manager in San Francisco, and can be reached at: tel: 415 677 3140; satkins@littler.com. Gary E. Clayton is Founder and Chairman of the Privacy Council. He may be contacted on tel: 972 997 4044; or at: gclayton@ privacycouncil.com*

The second part of this article will appear in the July issue of World Data Protection Report.

SECURITY & SURVEILLANCE

Case Report

AUSTRIA

■ STATE MUST PAY FOR SURVEILLANCE EQUIPMENT

Austrian Constitutional Court, February 27, 2003

A court in Austria has ruled that it is unconstitutional to compel telecommunication operators ("TO"s) to implement wiretapping equipment at their own expense. In a decision of February 27, 2003 the Austrian Constitutional Court (*Verfassungsgerichtshof, VfGH*) annulled a provision of the Telecommunications Act (*Telekommunikationsgesetz, TKG*) whereby the burden of expenses for wire tapping equipment was imposed on the telecommunication operators.

Since 1997, section 87 TKG requires TOs to install wire tapping equipment. This provision authorises law enforcement authorities to obtain traffic data from a TO. It provides that TOs are "obligated to co-operate to the necessary extent in the surveillance of telecommunication". They are required to make available all equipment needed for the surveillance of a specific telecom-

munication to the prosecuting authorities. All data recorded by such equipment may be released to prosecuting authorities merely on the basis of a court decision pursuant to the Austrian Criminal Procedure Code (section 149a *et seq*).

The Ministry for Traffic, Innovation and Technology recently issued an ordinance in 2001, which specifies the obligations under section 89 TKG, the Surveillance Ordinance (*Überwachungsverordnung, ÜVO*).

Under section 3 ÜVO, the TOs must provide for different surveillance installations within their networks. In particular, they are obligated to furnish the following data upon a court's request:

- the recording of calls from and to the subscriber line under surveillance;
- the number of the subscriber line under surveillance;
- the numbers dialled from the subscriber line under surveillance, even when a call is not completed;
- any incomplete numbers dialled from the subscriber line under surveillance, where an attempted call is prematurely terminated;
- the numbers of subscriber lines from which the subscriber line under surveillance is dialled, even when a call cannot be completed;
- in the case of mobile-telephone lines under surveillance, the cells carrying the call under surveillance;
- the beginning of the call or attempted call with date and time;
- the termination of the call or attempted call with date and time and the duration of the call.

In addition, starting from 2005, TOs have to comply with the European Standard ES 201 671 Version 2.1.1 of the European Telecommunications Standardisation Institute (section 4, para 1, subpara 4 ÜVO).

Section 89 TKG provides for a right of the TOs to be reimbursed for the pertinent cost of a single wiretapping. The reimbursement excludes, however, the cost of the necessary surveillance equipment and its installation.

Six major Austrian (fixed and mobile) telephone operators challenged the legality of this provision before the VfGH. They argued that it infringed their fundamental rights to protection of property and to equality of treatment. Costing several million Euros, the obligation to install the required surveillance equipment imposed upon the TOs a financial burden that was not outweighed by any private benefit linked to it but was solely in the public interest for the prosecution of criminal activities. Furthermore, this financial burden was likely to increase in the future since the TOs were compelled to update the surveillance equipment in line with technological development.

In its decision, the VfGH affirmed the state's power to commit private persons or entities (such as TOs) to perform public tasks or to co-operate in such. Therefore, the co-operation obligations provided for by the TKG and the ÜVO as such are in line with the Austrian constitution.

However, the Court also held that the co-operation obligations imposed upon the TOs must comply with the principle of proportionality provided for in the Austrian constitution. This principle requires that the costs of the TOs be balanced with circumstances creating a special legal and economic relation between the TOs and its (monitored) customers. Such circumstances comprise the calculability of the expenses, the economic burden and the interest of the company in the required services and a possible endangerment created by the operation of the company's business.

Since the law, by simply shifting all expenses to the TOs, lacked any observation of this duty of balancing, it violated the principle of proportionality. The Court found that it is not justified to impose such obligations on the TOs regardless of the nature and scope of the TOs' obligations to co-operate, and regardless of the content and extent of the wire tapping involved. Therefore, "the financial burden of the telecommunication operators and the preparation of copious devices is only justified in case of special circumstances and after a conducted balancing of interests" (VfGH judgment, p. 43). Mere budgetary constraints of the state, however, cannot constitute a reasonable basis for the imposition of the duty to bear all costs of such an activity of public interest.

As a consequence, the Austrian government has to amend section 89 TKG by the end of 2003, taking into account the principle of proportionality. By such amendment, the TOs will probably be entitled to reimbursement of the cost incurred by the installation of the surveillance equipment required under the TKG and the ÜVO.

By Martin Brodey and Florian Oppitz, Dorda Brugger & Jordis.

EUROPEAN UNION

ECHR RULES ON BREACH OF PRIVACY BY USE OF CCTV IMAGES

Peck v. The United Kingdom

In the recent case of *Peck v. The United Kingdom (Application no. 44647/98)*, the European Court of Human Rights held that the disclosure by Brentwood Council of images of Mr Peck constituted a serious interference with his right to respect for private life, and the disclosure was not proportionate to the legitimate aims pursued by the Council.

In 1995 images of Mr Peck walking down Brentwood High Street were captured by Brentwood Council's CCTV cameras without his knowledge. At the time Mr Peck was suffering from depression and attempted suicide (although the event was not captured on CCTV). Mr Peck was carrying a knife and the police were alerted, although Mr Peck was never charged. Later in 1995 the Council disclosed still photographs and

footage from their CCTV system to various local newspapers, Anglia TV and BBC's "Crime Beat" programme to publicise the success of the Council's CCTV cameras. In each case Mr Peck's image was either not masked or masked inappropriately, and as a consequence he was recognised by his friends, neighbours and colleagues.

Although at the time Mr Peck was in a public street, the Court held he was not participating in a public event and was not a public figure, and in addition he had never been charged with a criminal offence. The Court held that the Council's actions were disproportionate and an unjustified interference with Mr Peck's private life, and as a result a violation of Article 8 of the European Convention on Human Rights. The Court found that the Council should have pursued other options, for example discovering Mr Peck's identity and obtaining his consent, or the Council could have effectively disguised Mr Peck's identity, or taken better care to ensure that the media properly disguised Mr Peck's identity, for example, by having a written contract regarding the disclosure.

Although Mr Peck had complained to the Broadcasting Standards Commission, the Independent Television Commission and the Press Complaints Commission (two of which upheld his complaint) and applied for judicial review, at the time the European Convention of Human Rights had not been implemented in the United Kingdom and therefore the Court held that he had not been able to obtain an appropriate national remedy. The Court found that the threshold for judicial review was too high for Mr Peck to obtain an effective remedy. As a result the Court awarded Mr Peck EUR11,800 for distress and embarrassment, and EUR18, 075 to cover the costs of both domestic and European proceedings.

The case highlights that CCTV footage must be treated with care and in particular attention should be paid to individuals' right to privacy following the implementation of the European Convention of Human Rights, and the Data Protection Act 1998, in relation to how CCTV footage is captured, retained and used.

CCTV footage is personal data for the purposes of the Data Protection Act 1998 and the recording, use and disclosure of such footage must be in accordance with the provisions of the Act. The Information Commissioner has approved a Code of Practice in relation to the use of CCTV cameras, and although there are a number of exceptions to the application of the Code (including CCTV used by employers to monitor their employees which falls under the Employment Practices Data Protection Code, or the use of personal security equipment in private homes, and surveillance activities covered by the Regulation of Investigatory Powers Act), the Code does have useful guidance on the capturing and processing of CCTV images to ensure compliance with the Data Protection Act 1998.

By John Armstrong and Lisa Benjamin, CMS Cameron McKenna; tel: +44 (0) 20 7367 2701; e-mail: john.armstrong@cmck.com; or lisa.benjamin@cmck.com

News

UNITED KINGDOM

Part 3 of Employee Monitoring Code Published

After a delay of over two years, the Information Commissioner has today finally published Part 3 of The Employment Practices Data Protection Code on the controversial issue of monitoring employees at work (including their use of e-mail, the Internet and telephone calls).

The Code does not create new law, rather it sets out the Information Commissioner's recommendations as to how the existing legal requirements of the Data Protection Act ("the Act") can be met in the context of the employer/employee relationship. However, businesses must consider the contents of the Code carefully as it contains benchmarks which can be cited by the Commissioner in any enforcement action that it takes against an employer in relation to its processing of employees' personal data.

The following points in the Code are of particular significance:

- Any adverse impact of monitoring on employees must be justified by the benefits to the employer and others. This is best achieved by carrying out an "impact assessment" which is designed to help employers judge whether a monitoring arrangement is a proportionate response to the problem it seeks to address.
- Monitoring is usually intrusive and employees have "legitimate expectations that they can keep their personal lives private". The key message for employers is that monitoring should only be carried out where there is a clear, justified purpose, and employees must be fully informed of the reasons and circumstances under which they may be monitored.
- Covert monitoring (where an employee does not know he or she is being monitored) can only be carried out in "exceptional circumstances", where there are grounds for suspecting criminal activity or equivalent malpractice and where notification would hinder the prevention or detection of the activity.

The courts and employment tribunals are also likely to take the Code seriously. Recent cases (such as the Naomi Campbell privacy case) indicate that the courts are already guided by the Commissioner's views.

The Code is available from the "Guidance & other publications" page of the Information Commissioner's website at *www.dataprotection.gov.uk*.

By Gary Brooks, Solicitor, Berwin Leighton Paisner, London; e-mail: gary.brooks@blplaw.com