BNA International

World Data Protection Report

International Information for International Businesses

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

Volume 4, Number 3 March 2004

Articles

Review

Case Report

News

www.bnai.com

BNA International Inc., a subsidiary of The Bureau of National Affairs, Inc., Washington, D.C., U.S.A.

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 £595; Eurozone €950; U.S. and Canada U.S.$995. 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.bnai.com*
ISSN 1473-3579

The restrictions imposed by the Data Protection Directive on organisations transferring personal data out of the European Economic Area have created particular difficulties for multinationals.

Today's trend towards globalisation makes it increasingly common for such organisations to have processes, management-lines, and internal information systems – and so too data transfers – that cross country borders, both inside and outside the EEA. The impact of restrictions on such transfers can be acute. Could the adoption of Binding Corporate Rules be the solution? We are delighted to include an article by Mark Watts, a Partner with technology specialist law firm, Bristows which evaluates the current options for data transfer and provides detailed coverage on Binding Corporate Rules.

In line with other Member States, Ireland has introduced recent amendments to its data protection and communications legislation in respect of direct marketing activity. Rob Corbet of Arthur Cox provides us with an update on p. 7. Alessandro del Ninno (Studio Legale Tonucci) also writes on the latest changes to be made to data protection and e-communication services in Italy under the country's new Privacy Code.

One of the key features in the U.K. Information Commissioner's office Employment Practices Data Protection Code, which deals *inter alia* with monitoring in the workplace, is the so-called "Impact Assessment" (IA). The IA is intended to assist employers in meeting their data privacy obligations in a complex and controversial area. Our article from Simeon Spencer of Morrison & Foerster explains how an employer might carry out an assessment, the justification for doing so and the benefits to be gained.

I hope that you enjoy this issue. We look forward to receiving your comments and suggestions at nicholad@bna.com or on tel. (+44) (0)207 559 4807.

Nichola J. Dawson

We wish to thank the following for their contribution to this issue:
Sally Annereau, Taylor Wessing, London; *Rob Corbet,* Arthur Cox, Dublin; *Linda Farrell,* Bristows, London; *Charles H. Kennedy* and *Trisha Kanan,* Morrison & Foerster LLP, Washington DC and Los Angeles; *Christopher Kuner,* Hunton & Williams, Brussels; *Alessandro del Ninno,* Studio Legale Tonucci, Rome; *Heather Rowe,* Lovells, London; *Mark Watts,* Bristows, London; *Gerrit-Jan Zwenne,* Bird & Bird, The Hague.

Consumer Protection

Case Report

THE NETHERLANDS

Court Supports ISPs' Property Rights over Freedom of Expression

Dutch Supreme Court, March 12, 2004

In the latest legal battle against spam, the Dutch Supreme Court has supported Internet Service Provider XS4ALL, to rule that the property rights of the provider outweigh a direct marketing agency's right of freedom of (commercial) expression, therefore permitting providers to take measures to bar spam.

In his advice to the Court, the Advocate-General pleaded for weighing up the interests on a case-by-case basis:

> "[t]he ISP may prevent third parties from using 'his' facilities if he can advance sufficiently important grounds, and if his decision does not rest upon an unreasonable weighing up of interests".

In its judgment of March 12, 2004 the Supreme Court went one step further to deliver a judgment which gives (almost) absolute priority to the property rights over other rights:

> "[I]f someone, without having the right thereto, makes use of a property to which another holds an exclusive right, and as a result thereof he, as will usually be the case, infringes that exclusive right, he acts unlawfully with respect to that entitled person, except if there is a ground for justification".

In the opinion of the Supreme Court, freedom of expression does not constitute such a ground for justification. Moreover, in the Supreme Court's opinion, the payment of the damage suffered by the ISP cannot be a ground for justification either.

The judgment means that, in theory, providers may prohibit and block all spam, including that which is directed to business e-mail addresses. In practice, however this will be difficult to achieve. A provider will first have to warn a specific spammer, and thereafter claim a prohibition linked to a penalty payment per violation through preliminary relief proceedings. Although it seems likely that the provider will be able to win such proceedings, the ISP may not be inclined to follow such a strategy. This is a costly form of spam prevention, as the law does not provide for damages to cover all the legal costs that will be incurred.

The judgment legitimises the implementation of strict spamfilters by Internet Service Providers but according to some, this is an inadequate solution to the problem. The NLIP, the Dutch branch of the Internet Service Providers' organisation, points out that:

> "[t]aking preventive measures has little effect if the spam prohibition is not really maintained. It is therefore of vital importance that authorities take severe measures if it turns out that undertakings violate the law and send unsolicited mail after all".

The judgment has been criticised, *inter alia* by the Dutch privacy and civil rights organisation, Bits of Freedom, for the far-reaching consequences it could have in terms of the functioning and development of the Internet.

The infrastructure of the Internet has an almost indefinite number of owners. All cables, routers, modems, domain name servers, websites and all other network elements are the exclusive property of different owners. In the reasoning of the Supreme Court, these owners may deny others the use of and/or access to their cables, routers and the like, except when there is a justification for not prohibiting access. This enables them to fight spam, but also to block the conveyance of other unsolicited information, even if this information is not unlawful.

Some writers argue the judgment could imply that a website owner may prohibit another party to have hyperlinks linking to its site. Further, the owner may also prohibit search engines from accessing its site.

In this respect it is rather atypical that the judgment is rendered in favour of Internet Service Provider XS4ALL, which presents itself as a supporter of the freedom of expression.

The judgment is available in Dutch and can be accessed at *www.rechtspraak.nl/uitspraak/frameset.asp?ui_id=58139*

By Gerrit-Jan Zwenne, an advocaat with Bird & Bird, based in The Hague and lecturer at eLaw@Leiden, the Leiden University Centre for Law in the Information Society. The author may be contacted at tel. (+31) 70 353 8803 or at gerrit-jan.zwenne@twobirds.com.

News

UNITED STATES

ISPs Sue Spammers under CAN-SPAM Act

Four leading Internet service providers have brought a series of anti-spam lawsuits against hundreds of defendants, including individuals who are reputed to be among the nation's best known spammers, alleging they sent hundreds of millions of spam e-mails unlawfully. Claims were brought on March 10, 2004.

America Online Inc., EarthLink Inc., Microsoft Corp., and Yahoo! Inc. filed six complaints in federal district courts in California, Georgia, Virginia, and Washington, in the first co-ordinated industry action under the CAN-SPAM Act, which went into effect on January 1, 2004. The ISPs are seeking injunctions and damages, and sued under state and federal law.

Although individuals cannot sue under CAN-SPAM, the law authorises ISPs to seek damages of $100 per e-mail for messages that have false headers and $25 per e-mail for other breaches. The damages ISPs can obtain are capped at $1 million and can be tripled for aggravating factors.

The ISPs united to target some of what they allege to be the worst spammers, but the complaints were individually filed. [*America Online Inc. v. Davis Wolfgang Hawke,* E.D. Va., No.

04-259, *complaint filed* 3/9/04; *America Online Inc. v. John Does 1-40,* E.D. Va., No. 04-260, *complaint filed* 3/9/04; *Microsoft Corp. v. JDO Media Inc.,* W.D. Wash., No. CV04-515P, *complaint filed* 3/9/04; *Earthlink Inc. v. John Does 1-25,* N.D. Ga., No. 04 CV-0667, *complaint filed* 3/9/04; *Yahoo! Inc. v. Eric Head,* N.D. Calif., No. C04-00965, *complaint filed* 3/9/04.]

Alleged Violations

The complaints allege the defendants sent hundreds of millions of bulk spam e-mail messages to subscribers of the four ISPs in violation of CAN-SPAM. For example, the ISPs alleged the defendants used false or misleading "From" lines, sent spam through open proxies that falsified the true sender of the e-mail, used false and misleading subject lines, and failed to provide a physical address and an electronic unsubscribe option.

The defendants were accused of promoting deceptive solicitations for a variety of products, including get-rich-quick schemes, prescription drugs, pornography, instructions for conducting spam campaigns, mortgage loans, university diplomas, and cable descramblers.

Although all the ISPs filed their claims under CAN-SPAM, they also sued under other laws. AOL, which is located in Virginia, sought damages under the Virginia Computer Crimes Act; Microsoft, which is based in Washington, also sued under the Washington Commercial Electronic Mail Act; Earthlink, which is based in Georgia, also alleged breaches of the federal civil RICO Act, the Computer Fraud and Abuse Act, the Lanham Act, as well as violations of Georgia's civil RICO law, the state's Computer Systems Protection Act, and other state law claims; and Yahoo also alleged violations of the Computer Fraud and Abuse Act, the California Computer Criminal Statute (Cal. Penal Code §502), and civil conspiracy.

Anti-Spam Group Reacts

John Mozena, spokesman for the Coalition Against Unsolicited Commercial E-mail (CAUCE), said that CAUCE's opinion, the lawsuits were unlikely to make any real difference to quelling the amount of spam people received and pointed out that this was not the first time that the same ISPs had sued spammers.

CAUCE has worked with states on anti-spam laws which were preempted with the passage of CAN-SPAM. "One problem with CAN-SPAM is we didn't think it set up effective enforcement", he said.

CAUCE would have preferred a federal spam law with enforcement mechanisms that resemble the Telephone Consumer Protection Act, which allows private citizens to sue if they receive junk faxes and provides for $500 in damages for each violation.

According to Mozena, it will take a combination of effective enforcement of spam laws, along with technical solutions, to stem the tide of spam.

CAN-SPAM was signed by the president in December 2004 (see "The U.S. CAN-SPAM Act: An Opt-Out Approach to E-Mail Marketing", *World Data Protection Report*, February 2004). The statute established, for the first time, national standards for sending unsolicited commercial e-mail. Among other things, the law bans deceptive practices, such as "harvesting" e-mail addresses from websites and falsifying header information.

While CAN-SPAM is tough on deceptive spam, critics say it gives a green light to e-mail marketing companies to send large volumes of junk messages. The law permits the transmission of unsolicited commercial e-mail, as long as senders follow certain rules, such as providing a mechanism for consumers to opt out of future messages. Pornographic spam must carry warning labels.

According to San Francisco-based Brightmail Inc., more than 60 percent of Internet e-mail is spam.

AOL Says Law Provides "Necessary Tools"

"With the creation of this anti-spam industry alliance and the implementation of a federal law to litigate effectively against spammers, we are witnessing the impact that this industry-wide attack on spam is having", Microsoft Deputy General Counsel Nancy Anderson said in a statement.

"We've had the opportunity to share investigative best practices and various legal resources and information to ensure that spammers are going to have an increasingly difficult time continuing their deceptive practices with the full force of this industry coming down on them."

AOL Executive Vice President and General Counsel Randall Boe said Congress gave ISPs the necessary tools to pursue spammers with "stiff" penalties, when it passed CAN-SPAM.

Meanwhile, Hypertouch, Inc., a small ISP based in Foster-City, Calif., has accused Boston-based BVWebTies, LLC and Sacramento-based BlueStream Media of sending unwanted e-mail advertisements for Bob Vila's "Home Again Newsletter." That lawsuit, filed on March 4 in a California district court, is said to be the first legal action under CAN-SPAM.

Full Spectrum of Abuses Alleged

The complaints by AOL, EarthLink, Microsoft, and Yahoo, filed in the companies' home states, charge defendants with sending hundreds of millions of bulk spam e-mail messages to customers of the four networks. Charges include sending spam through third-party computers; falsifying "from" lines; and failing to provide a physical address and an electronic unsubscribe option.

AOL and Microsoft filed two complaints, and Yahoo and EarthLink each filed one. Several individuals and companies were named in the lawsuits, and there were more than 100 "John Doe" defendants.

House Judiciary Committee Chairman James Sensenbrenner (R-Wis.) applauded the lawsuits and said he expects the Federal Trade Commission, Department of Justice, and states' attorneys general to bring actions of their own soon.

"The battle against spam will be fought on many fronts and will be won by new technologies, greater consumer awareness, the efforts of ISPs, and legal actions like those today", Sensenbrenner said.

The Earthlink complaint is available at *www.earthlink.net/about/press/pr_AllianceFAS/EarthLink_CAN_SPAM_Filed_Stamped.pdf*.

Legislation & Guidance

Data Protection and E-Communication Services: New Rules in the Italian Privacy Code

By Avv. Alessandro del Ninno, a Senior Associate in the Information & Communication Technology Department of Studio Legale Tonucci, Rome. The author may be contacted at adelninno@tonucci.it

On January 1, 2004 a renewed legal framework relating to Data Protection in Italy entered into force. Starting from this date, the so-called "Code on Privacy" – adopted by means of the legislative decree of June 30, 2003 No. 196 – shall apply to all processing of personal data.

The Code consolidates all the existing legal provisions so far regulating personal data protection in Italy (and contained in the main Law No. 675/1996, as well as in many sectorial legislative decrees, regulations, Data Protection Authority's deliberations, *etc*.), thus considerably simplifying and harmonising the legal framework at the end of a long transitional period.

The Code is the outcome of a complex exercise that has led to establishing a unique reference text for data protection, tendentially final as to its structure and content. Simplification, harmonisation and effectiveness are the underlying principles with regard to data subjects' rights and the fulfilment of the relevant obligations by data controllers. Furthermore, the enactment of the Code has turned these provisions – laid down in different contexts and through various instruments – into primary legislation, thereby affording a high level of protection to the rights and freedoms at stake. Indeed, the safeguards afforded to all the entities involved have been further enhanced, in accordance with the policy adopted with the enactment of the 1996 Data Protection Act (No. 675/1996). Finally, the Code transposes EC Directive 2002/58 on the protection of personal data within the electronic communications into Italian law.

The Code consists of three parts. Part 1 (sections 1–45) sets out the general principles and obligations that apply to all processing operations, except as provided for in Part 2 with regard to specific categories of processing. In particular, Section 1 explicitly proclaims that everyone has the right to the protection of personal data, a right that was recently reaffirmed by Article 8 of the Charter of Fundamental Rights of the European Union. Section 3 stresses the importance of the data minimisation principle in reducing the amount of personal and identification data, with regard both to information systems and software.

Finally, administrative and judicial remedies, sanctions and the powers and activity of the Supervisory Authority are regulated in Part 3 of the Code (Sections 141–186).

Of note in the new Code are the emphasis and binding force given to codes of conduct and professional practice. This applies both to those codes already adopted as per section 12 of the Code – all annexed to the Code itself – and apply to processing of personal data for historical purposes, for statistical purposes and in the exercise of journalistic activities – and those yet to be adopted in many other sectors (amongst others, the banking and insurance sector; Internet and electronic networks (anticipated at the end of April 2004); video surveillance; direct marketing; labour sector; and private detective investigations). It is expressly set forth that compliance with the provisions of the codes shall be a general prerequisite for the processing of personal data by public and private entities.

The Code also rationalises and develops the rules on the compulsory minimum security measures to be adopted and complied with in the processing of personal data. The related set of rules is contained in Annex B of the Code ("Technical Annex on minimum security measures").

Protection of Personal Data

Title X (articles 121–133) of the Italian Code on Privacy contains the rules about data protection in the field of electronic communication. This set of rules, beyond updating the previous legislative decree No. 171/1998 in light of the latest technological developments, introduces new rules implementing E.U. Directive 2002/58/EC. (Decree No. 171/1998 implemented E.U. Directive 97/66/EC on the protection of privacy in the Telecommunications sector.)

The main points of Title X can be summarised as follow. First of all, for the purposes of the Code:

- "electronic communication" shall mean any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable or identified subscriber, or user receiving the information;
- "call" means a connection established by means of a publicly available telephone service allowing two-way communication in real time;
- "electronic communications network" shall mean transmission systems and switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit-and packet-switched, including Internet) and mobile terrestrial networks, networks used for radio and television broadcasting, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, and cable television networks, irrespective of the type of information conveyed;
- "public communications network" shall mean an electronic communications network used wholly or

mainly for the provision of publicly available electronic communications services;

- "electronic communications service" shall mean a service which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, to the extent that this is provided for in Article 2, letter c) of Directive 2202/21/EC of the European Parliament and of the Council of March 7, 2002;
- "subscriber" shall mean any natural or legal person, body or association who or which is party to a contract with the provider of publicly available electronic communications services for the supply of such services, or is anyhow the recipient of such services by means of pre-paid cards;
- "user" shall mean a natural person using a publicly available electronic communications service for private or business purposes, without necessarily being a subscriber to such service;
- "traffic data" shall mean any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;
- "location data" shall mean any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;
- "value added service" shall mean any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof;
- "electronic mail" shall mean any text, voice, sound or image message sent over a public communications network, which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

Title X (articles 121–133) shall apply to the processing of personal data in connection with the provision of publicly accessible electronic communication services on public communications networks.

One interesting provision is that contained in article 122, which regulates the use of cookies or other means aimed at trailing the browsing activities on the Internet. According to the mentioned provision, it shall be prohibited to use an electronic communication network to gain access to information stored in the terminal equipment of a subscriber or user, to store information or monitor operations performed by a user. Despite this general principle, the Code of conduct on Data Protection and Electronic Networks (the adoption of which is expected at the end of April 2004) shall lay down prerequisites and limitations for a provider of an electronic communication service to use the network in the manner described for specific, legitimate purposes related to technical storage for no longer than is strictly necessary to transmit a communication or provide a specific service as requested by a subscriber or user that has given his/her consent based on prior information as per article 13 of the Code, whereby purposes and duration of the processing shall have to be referred to in detail, clearly and accurately.

With regard to the processing of traffic data, article 123 of the Code provides that such data relating to subscribers and users that are processed by the provider of a public communications network, or publicly available electronic communications service, shall be erased or made anonymous when they are no longer necessary for the purpose of transmitting the electronic communication.

Nevertheless, providers shall be allowed to process traffic data that are strictly necessary for subscriber billing and interconnection payments for a period (not in excess of six months) in order to provide evidence in case the bill is challenged or payment is to be pursued. This is subject to such additional retention as may be specifically necessary on account of a claim also lodged with judicial authorities.

Further, for the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process traffic data to the extent and for the duration necessary for such services or marketing, on condition that the subscriber or user to whom the data relate has given his/her consent (and such consent may be withdrawn at any time).

Another interesting provision is that set forth in article 126 with regard to the so-called location data (for example: the location services provided by the latest generation mobile phones).

Location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, may only be processed when they are made anonymous, or with the prior consent of the users or subscribers, which may be withdrawn at any time, to the extent and for the duration necessary for the provision of a value added service (*i.e.*, the location service).

The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service.

Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber shall continue to have the possibility, using a simple means and free of charge, of requesting to temporarily refuse the processing of such data for each connection to the network or for each transmission of a communication.

Rules on Unsolicited Communications

Article 130 of the Italian Code on Privacy provides important rules relating to unsolicited communications.

The use of automated calling systems without human intervention for the purposes of direct marketing or sending advertising materials, or else for carrying out market surveys or interactive business communication shall only be allowed with the subscriber's consent. This applies to electronic communications performed by e-mail, facsimile, MMS or SMS-type messages or other means for the purposes referred to therein. Further communications for the purposes referred to therein as performed by different means shall be allowed in

pursuance of articles 23 and 24 (which contains the general rules about the need of prior consent and the cases of derogation).

Where a data controller uses, for direct marketing of his/her own products or services, electronic contact details for electronic mail supplied by a data subject in the context of the sale of a product or service, said data controller may fail to request the data subject's consent, on condition that the services are similar to those that have been the subject of the sale and the data subject, after being adequately informed, does not object to said use either initially or in connection with subsequent communications. The data subject shall be informed of the possibility to object to the processing at any time, using simple means and free of charge, both at the time of collecting the data and when sending any further communications.

In any event, the practice of sending communications for marketing or promotional purposes, by disguising or concealing the identity of the sender, or without a valid address to which the data subject may send a request to exercise all his/her rights as per article 7 of the Code shall be prohibited.

It has to be noted that, amongst others, the breach of the rules provided by articles 123 (Traffic Data), 126 (Location Data) and 130 (Unsolicited communications) constitutes an "unlawful data processing" (article 167 of the Code) which is punishable by imprisonment of between six and eighteen months. If the offence involves data communication or dissemination, it is punishable by imprisonment of between six and twenty-four months, unless the offence is more serious.

Latest Developments

The 2003 EC law (L. of October 31, 2003 n. 306), article 12, provides additional rules to definitively complete the implementation of the EC Directive 2002/58/EC, by providing the enforcement (by April 2004) of a specific legislative decree aimed at introducing into the Code:

- specific rules about the need for prior consent (required in writing for sensitive data) for the processing of personal data within General Public Directories (both hard copy and electronic) if the processing is not strictly linked to the research of a subscriber;
- provisions for implementing articles 5, 6, 8 (paragraphs 1-4) and 9 of E.U. Directive 2002/58/EC; and
- additional provisions on data retention (which must be limited).

With regard to the last point, it should be noted that in the meantime an important decree has been adopted with regard to the data retention discipline for justice purposes; the law decree of December 24, 2003 n. 254 (published in the Italian Official Journal of December 29, 2003 n. 300).

Articles 3 and 4 in the final text of the decree, which was adopted on February 18, 2004, introduce the obligation for TLC operators to keep personal data related to telephonic traffic (e-mail and Internet data are excluded) up to 24 months. Prior to the amendment, article 132 of the Code provided a unique time limit of 30 months for the retention of telephone traffic data. An additional data retention period of a further 24 months is provided exclusively to carry out requests of judiciary authorities linked to criminal investigations.

Direct Marketing Developments in Ireland

By Rob Corbet, a Senior Associate with Arthur Cox, Dublin. The author may be contacted on tel. (+353) 1 618 0566 or at rob.corbet@arthurcox.com

Recent amendments to Irish data protection and communications legislation have introduced a new regulatory regime in respect of direct marketing activity in Ireland. Over the past year, a confusing series of statutory instruments and amendments to primary legislation have increased the regulatory burden on all Irish organisations wishing to communicate directly with customers and potential customers. In this article, some of the main recent developments are considered in chronological order of enactment.

E-Commerce Regulations 2003

With effect from February 24, 2003, the EC (Directive 2000/31/EC) Regulations 2003 implemented the Electronic Commerce Directive (2000/31/EC). These Regulations introduced prior information requirements on all service providers who offer any electronic services at the individual request of the customer and thus apply to most online service providers. In addition, Regulations 8 and 9 oblige such service providers to clearly identify commercial communications as such and to include contact details with each communication. In addition, online service providers must offer a clear choice to customers at the point of data capture regarding unsolicited commercial communications. Most online traders are affected by these Regulations and their data capture pages and procedures are required to be designed accordingly.

Data Protection (Amendment) Act, 2003

The Data Protection (Amendment) Act, 2003 updates the Data Protection Act 1988 with effect from July 1, 2003. The purpose of this amending legislation is to finally implement in full the Data Protection Directive (95/46/EC) in Ireland. The official title of the amended data protection legislation is the Data Protection Acts 1988 and 2003 ("DPA").

Section 2(7) of the DPA has always provided data subjects with the right to be deleted from direct marketing databases upon request. However, the DPA now goes further. Under Section 2(8) of the DPA, data controllers who anticipate that personal data will be processed for the purposes of direct marketing must inform the data subjects that they may object, free of charge and at any time, to being included in a direct marketing database. Read in isolation, Section 2(8) implies that provided the data controller informs the data subject that he intends to use the data for direct marketing purposes, a simple "opt-out" box at the point of data capture would suffice to permit such marketing.

Privacy in Telecoms Regulations 2003

However, this interpretation of Section 2(8) of the DPA does not survive the enactment of the EC (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations, 2003. These Regulations came into effect on November 6, 2003 and implement Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.

These Regulations affect direct marketing activity in a number of respects, primarily in Regulations 13 and 14 which deal with unsolicited communications and reflect the "anti-spam" provisions in the underlying Directive.

In summary, the Regulations adopt an "opt in" obligation for all electronic-based direct marketing to individuals whilst the "opt out" option remains possible for telephone-based direct marketing to individuals, all direct marketing to non-individuals and all direct marketing to existing customers.

With regard to electronic forms of direct marketing, unsolicited direct marketing e-mails and SMS are generally prohibited unless the individual recipient has previously notified the sender that he/she consents for the time being to such communications being sent, *i.e.*, has "opted in" to receiving commercial e-mails or SMS messages.

However, it is permissible to send direct marketing communications by e-mail or SMS message where:

- the e-mail address has been obtained in the course of a sale or negotiations for the sale of a product or service;
- the marketing is in respect of the marketer's similar products and services; and
- the recipient has been given, and continues to be given, a simple means of refusing use of his or her details in this way.

This is in effect a soft "opt-in" exemption in the context of an existing customer relationship. The scope of the terms "in the course of a sale or negotiations" and "similar products and services" are not defined and their interpretation will have important ramifications for marketers.

Any person who fails to comply with the relevant provisions of these "anti-spam" provisions shall be guilty of an offence and the sending of each unsolicited communication or making of each unsolicited call constitutes a separate offence. An offence may be brought and prosecuted by the Data Protection Commissioner.

Where a person is convicted of an offence under the Regulations the court may order any data material which appears to be connected with the offence to be forfeited or destroyed. It should be further noted that in the context of a claim for damages under the Regulations, it is a defence for a person to establish that he, she or it has taken all reasonable care to comply with the requirement concerned.

A further interesting development is the legislative recognition of the National Directory Database which has been established by the Communications Regulator, *ComReg*, in conjunction with the telecommunications operator *eircom*. Regulation 13 obliges all direct marketers to consult the National Directory Database prior to making unsolicited calls to individuals and companies. The National Directory Database affords certain rights to individuals and companies to centrally "opt out" of receiving unsolicited communications.

Conclusion

It is regrettable that there has been such a multi-layered legislative approach to the regulation of direct marketing. As can be seen from the above, a compliant direct marketer is now required to consult with several different laws, most of which have only come into effect in the past year or so, before any direct marketing campaign can be lawfully conducted.

The recent laws therefore present significant practical problems for existing direct marketing databases which have been created prior to the introduction of the new laws. While there are various remedies available under the these new laws to the Data Protection Commissioner, the Director of Consumer Affairs and to the individual recipients of unwanted mail, it remains to be seen how they will be enforced in practice. The Data Protection Commissioner for one is reported to have already acted against distributors of unsolicited SMS messages.

In any event, for any party wishing to create a database of existing or potential customers for the purpose of future marketing, now would be a good time to review the processes and procedures surrounding how contact details are captured and used.

News

AUSTRALIA

ACA Moves to Protect Customer Directory Data

The Australian Communications Authority (ACA), the government regulator of telecommunications and radiocommunications, has announced that it is taking to steps to guarantee increased protection for personal information provided by customers to telecommunications companies.

In a discussion paper, "Who's Got Your Number? Regulating the Use of Telecommunications Customer Information", released by the ACA on March 18, the communications authority has proposed new measures designed to prevent unauthorised commercial use of personal data, including direct marketing.

The proposed measures are built around a mandatory standard governing the use of customer information when it is made available for directories and other approved uses. The standard could include obtaining a customer's consent before disclosing his or her personal information, restricting access to customer information to specific entities, and more tightly specifying how the information can be used.

Under existing regulations, the personal details of telecommunications customers are collected and stored in the Integrated Public Number Database (IPND) – an industry-wide database of all listed and unlisted telephone numbers – and databases used for telephone number directories.

Data in the IPND is protected under the Telecommunications Act. It can only be used for approved purposes including the operation of the 000 emergency call service, investigations by

  WDPR ISSN 1473-3579

law enforcement and national security agencies, providing directory assistance and producing telephone directories.

But according to Acting ACA Chairman Dr Bob Horton, there is evidence that customers' information is being collected by public number directory producers and collated with data drawn from other sources to create consumer "profiles".

> "Current use of telecommunications customer data appears to go beyond what is allowed under existing legislation," Dr Horton said. "In fact, our investigations indicate that databases are being created and maintained based on information provided by customers to their telecommunications service providers.
>
> "These databases are then sold to other companies for direct marketing and other commercial activities.
>
> "In the ACA's opinion, this is not only a breach of existing law but also outside what customers providing personal information expect to happen".

Dr Horton said many telecommunications customers were not specifically warned about all the possible uses and disclosure of their personal information when they provided it to their telecommunications company.

The ACA is calling for submissions on the proposed regulatory options from interested individuals, groups and industry bodies. Submissions close on April 30, 2004. The discussion paper is on the ACA website at *www.aca.gov.au/aca_home/issues_for_comment/Whos_Got_Your_Number*.

EUROPEAN UNION

Parliament Endorses Cappato Report on Review of Data Protection Directive

On March 9, 2003, the European Parliament adopted by an overwhelming majority (439 votes in favour, 39 against and 28 abstentions) Marco Cappato's report on Data Protection Directive 95/46/EC. In particular, the report is highly critical of the failure of some Member States to meet the October 31, 2003 implementation deadline and regrets differences in application at national level.

The report also reaffirms that transfers of personal data to third country authorities without consent, such as in the case of the U.S. authorities accessing transatlantic air passenger data, is a serious infringement of E.U. data protection law. The report, dated February 24, 2004, is available on the European Parliament's website, at: *www2.europarl.eu.int/omk/sipade2?L=EN&OBJID=69010&LEVEL=3&MODE=SIP&NAV=X&LSTDOC=N*

The adopted text will be posted shortly on the same website.

By Christopher Kuner, Hunton & Williams, Brussels.

Submissions by Authors: The editors of *World Data Protection Report* invite readers to submit for publication articles reporting on or analysing legal and regulatory developments around the world. Prospective authors should contact Nichola Dawson at nicholad@bna.com or tel. (+44) (0)20 5559 4807; fax. (+44) (0)20 5559 4880.

Personal Data

Transferring Personal Data from the E.U.: Are Binding Corporate Rules the Answer?

By Dr Mark Watts, a Partner at technology specialist law firm, Bristows. Prior to joining Bristows in 2003, Mark was IBM's Global Privacy Attorney. The author may be contacted at Mark.Watts@Bristows.com

The restrictions imposed by Article 25 of the Data Protection Directive (95/46/EC) on organisations transferring personal data out of the European Economic Area are not new. Indeed, few, if any, data protection issues have attracted as much attention as those presented by Article 25. The provisions of Article 25 need not be set out again here; suffice to say, even nearly ten years after its restrictions first appeared, transferring personal data out of the EEA is not a straightforward matter; far from it.

The organisations most affected by Article 25 are probably the multinationals. Today's trend towards globalisation makes it increasingly common for multinationals to have processes, management-lines, and internal information systems – and so too data transfers – that cross country borders, both inside and outside the EEA. The impact of restrictions on such transfers can be acute, as potentially they represent powerful limitations on the deployment of internal technological solutions, restrictions on the cost savings that can result from reducing duplication between standalone-country IT systems and restrictions on pan-global (or "dotted") management lines. Most multinationals understand and appreciate the importance of safeguarding individuals' personal data overseas yet desire a simple but robust, effective but low-formality solution to the problem, something that enables lawful transfers of personal data but also fits the complexity of their corporate structures.

Methods for Transferring Personal Data Overseas

Until recently, a multinational seeking to transfer personal data around the world, broadly speaking, had three options available to it, namely, acquiring the fully-informed and freely&#30;given consent of everyone about whom it transferred personal data, implementing a network of contractual arrangements between its various country legal entities, or, in respect of transfers to the United States (only), entering the E.U.-U.S. Safe Harbor. No one "solution" is perfect. (Please note that whilst there are other exceptions under the Directive that allow personal data to be transferred, these are generally considered to be far too narrow in scope to meet the day-to-day needs of a typical multinational).

Individual Consent

With regard to a solution based on individual consent – the most popular solution according to some industry surveys – the drawbacks are significant. "Business-to-business" multinationals, for example, are likely to acquire personal data about thousands of individuals, such as business "contacts" and yet not deal with the individuals directly, so preventing their consent being obtained or requiring it to be collected only "indirectly" via the individual's colleagues or his employer, which is unlikely to be effective. In relation to personal data a multinational processes about its employees, consent is also problematic. Depending on the nature and scope of the consent sought, some employees – perhaps many – may refuse their consent. The multinational must then either ignore their refusal of consent and transfer their data anyway, a risky strategy, or provide an alternative means of processing that does not involve transferring their data out of the EEA – expensive or perhaps impracticable. And even if everyone consented, much has been made of the validity of consent from an existing (as opposed to a prospective) employee. It is argued that an employee who is asked to consent to the transfer of his personnel record to, for example, the United States is unlikely to refuse. In these circumstances is consent really "freely-given"? Also, to be valid, shouldn't consent be capable of being withdrawn? A consent-based solution seems to be the one least favoured by Data Protection Regulators too, as unlike other solutions, it does not require data protection measures to be applied in the destination country, nor does it require continuing liability for the multinational in respect of the personal data transferred.

Model Contracts

A contractual solution also has its problems. A multinational may implement a contractual solution using its own terms but if it does so then it must conduct a "Tour of Europe" to acquire (hopefully) the authorisation of each of the various EEA Data Protection Authorities. Alternatively, to avoid this exercise, a multinational may adopt the European Commission Model Contracts. The Model Contracts have not proved popular with industry and much has been said about their content - the onerous level of detail required, and the vagaries of certain key terms such as "factually disappeared", but the main difficulty arises not from the contents of the agreements but the sheer numbers and complexity involved in implementing a comprehensive contractual solution. Take, for example, a multinational with 200 companies worldwide, each based in a different country, each sharing personal data with its counterparts on a regular and frequent basis, perhaps via shared IT infrastructure. Contractual arrangements should be put in place between each and every pair of companies sharing data. The number of contracts required soon becomes unwieldy – 19,900 here. And whilst legal devices can be used to minimise the number of bits of paper actually signed to support this "web" of contracts, the administrative headache for a multinational implementing such a solution should not be underestimated. And at some point in the future, the multinational is bound to acquire another company, requiring the web to be updated.

  WDPR ISSN 1473-3579

Safe Harbor

What of the E.U.-U.S. Safe Harbor? Viewed in terms of formality alone, the E.U.-U.S. Safe Harbor is perhaps the most attractive of the solutions available, although it is, of course, only available in respect of transfers of personal data to the United States. It also excludes certain important categories of personal data, such as that processed within the financial services sector. Moreover, many multinationals, particularly those with a US-based parent, have been put off joining for fear of increased scrutiny of their parent company by the US Federal Trade Commission. Also, being a politically "negotiated" document, many of the Safe Harbor Principles (and accompanying FAQs) include language that arose out of political comprise rather than a quest for legal certainty and clarity. Different interpretations are possible. Whilst the number of multinationals signed up to Safe Harbor continues to increase, progress must be described as slow and steady, largely for the reasons outlined.

All of these options fall short of providing a real and workable solution for a multinational struggling to do the right thing.

Binding Corporate Rules

So it was with the aim of overcoming many of these difficulties and simplifying life for multinationals that the Article 29 Data Protection Working Party (the body set up under the Data Protection Directive, comprising representatives from each of the Member State Data Protection Authorities) adopted a paper on June 3, 2003, discussing another means of "Adducing Adequate Safeguards" under Article 26(2), which has become known as "Binding Corporate Rules". Binding Corporate Rules refers to the sorts of internal codes of conduct, policies, directives and the like that many multinationals use for internal governance on matters such as the handling of confidential information, conducting business ethically and other similarly important corporate affairs. Conceptually, such policies, directives, codes and similar unilateral undertakings can be thought of as internal "law" within the multinational. Can such documents deliver "adequate safeguards" under Article 26(2)? In principle, yes, according to the Working Party Paper, subject to meeting certain stringent requirements.

Much of the content required of Binding Corporate Rules is as would be expected. The Working Party Paper reaffirms that the "usual" data protection principles need to be included, much as under EEA data protection legislation, the E.U.-U.S. Safe Harbor and the E.U. Controller-Controller Model Contract. More detail and explanation may be required to ensure compliance under Binding Corporate Rules, however, particularly by parts of the multinational that operate in countries without a data protection law or culture. The principles should be tailor-made so that they practically and realistically fit with the processing activities that the multinational actually carries out.

Perhaps most importantly though, the Binding Corporate Rules must be binding both "inside and out", referring to the requirement that the multinational must be bound both *in practice* (compliance) and *in law* (legal enforceability). They must deliver a real and ensured legal effect throughout the multinational.

Here, binding "in practice" or compliance means that all companies of the multinational, as well as their employees, feel compelled to comply with the Binding Corporate Rules; that is, they must respect this internal "law". The Working Party Paper does not stipulate how multinationals should guarantee compliance but states more generally that the binding nature of the rules must be clear and good enough to be able to guarantee compliance with the rules outside the EEA. A multinational must be able to demonstrate, for example, that the rules are known, understood and effectively applied wherever they apply by employees who have received appropriate training. Disciplinary measures should be in place for non-compliance. Executive-management must be involved to oversee and ensure compliance.

As with other every other transborder dataflow solution (except consent), auditing compliance has an important role to play. Binding Corporate Rules must provide for self (*i.e.*, internal) audit and/or external supervision by accredited auditors on a regular basis with the results being directly reported at board level. The Data Protection Authorities may become involved in this aspect too, as part of a broader commitment by the multinational to co-operate with the Data Protection Authorities.

The Working Party Paper also recognises that even with fully enforceable legal rights, as described below, litigation can be disproportionately expensive and burdensome for an individual, particularly if it has to be conducted overseas. Multinationals are encouraged to incorporate other means of compliant handling, and the use of alternative dispute resolution mechanisms is promoted.

As well as being binding internally, Binding Corporate Rules must be binding "outside", that is, legally enforceable between the multinational and the outside world – the outside world being the EEA's Data Protection Authorities and the individuals about whom data is processed. A Data Protection Authority should be able to achieve legal enforceability of its rights and powers under the Binding Corporate Rules fairly simply, for example, via the process of granting an authorisation under Article 26(2) (and its national law equivalent). It will require an unambiguous undertaking that the multinational as a whole and each of the companies within it will abide by the "advice" of the Data Protection Authority. Some multinationals have expressed concern about the meaning of "advice" in this context. For example, the same language is used under the E.U.-U.S. Safe Harbor, where it can include a requirement to compensate individuals affected. The Working Party Paper also states that such advice may be made public.

For the individuals about whom personal data is processed, legal enforceability requires them to become "third party beneficiaries" via some means, either by the legal affect of the Binding Corporate Rules themselves (where possible) or the Binding Corporate Rules in combination with other contractual arrangements within the multinational. Individuals must be able to enforce compliance both by lodging a complaint before the competent Data Protection Authority and/or by commencing legal proceedings before a competent court.

The remedies available to an individual under Binding Corporate Rules should be broadly the same as under the E.U. Controller-Controller Model Contract. Giving individuals such broad legal rights is regarded as undesirable by some multinationals. They argue that provided sufficiently high levels of internal compliance are achieved, together with a commitment to co-operate with the Data Protection Authorities, there should be no need for legal enforcement

measures quite so far reaching. But legal enforceability is clearly an area to which the Working Party attaches great importance, and, in fairness, it always has. See, for example, the very similar remarks it made about "appropriate redress" in its 1997 paper, "First Orientations on Transfers of Personal Data to Third Countries". Giving individuals the right to seek judicial remedies is justified in two ways in the Working Party Paper. Firstly, because even the firm commitment required from multinationals to co-operate with the Data Protection Authorities cannot guarantee 100 percent compliance and the individuals concerned may not always agree with the views of the Data Protection Authority. Secondly, because the views of the Data Protection Authorities may vary from country to country and none of them are able to award damages as a remedy; only courts can do that. Given these remarks, it's hard to see how Binding Corporate Rules that don't provide individuals with judicial remedies could now be approved by an EEA Data Protection Authority. This is frustrating for many multinationals, particularly bearing in mind that, as the Working Party Paper acknowledges, the laws of some EEA countries do not enable third party beneficiary rights to be created by unilateral undertakings. In other words, the legal theories required for Binding Corporate Rules acceptable to the Working Party may not exist in some EEA countries. Certainly it's hard to think of a single, broadly effective legal theory that will invariably work everywhere. A patchwork of legal theories tailored to various country laws seems more likely. Possibilities discussed include theories based on unfair trade practices, the law of trusts, the law of misrepresentation and misleading advertisement, employment and consumer protection laws. From a legal point of view, finding an effective means of giving third party beneficiary rights unilaterally across the EEA is probably the biggest obstacle to the widespread adoption of the Binding Corporate Rules approach.

The Working Party Paper also deals with some of the "structural" issues unique to multinationals. It recognises them as mutating groups of entities whose members and practices change from time to time and acknowledges that updates to both the Binding Corporate Rules themselves and the list of entities to whom they apply will need to be made over time. Updates are allowed under a Binding Corporate Rules solution (without the multinational having to reapply for a new authorisation) under the following conditions:

- no transfer of personal data is made to a new group member until it is effectively bound by the rules and can deliver compliance;
- a fully updated list of members is maintained by the multinational along with a record of any updates to the rules, which should be made available to individuals or Data Protection Authorities upon their request;
- changes to the list of members and/or the rules are reported annually to the relevant Data Protection Authority, together with a brief explanation of the reason for the change.

For larger multinationals, even maintaining such a length list may be problematic, although it should be far easier than continually updating a contractual solution.

The Working Party Paper recognises that even if EEA-based individuals are provided with legally enforceable rights against, say, a multinational's Venezuelan company, in practice, exercising such rights is likely to be prohibitively complicated and/or expensive for the individual. It recommends that the E.U. headquarters (if an E.U.-owned multinational) or an E.U. member of the multinational with delegated data protection responsibilities should accept responsibility for the acts of all other companies of the multinational outside the EEA. This would include, where appropriate, making a commitment to pay compensation for any damages resulting from the relevant violation anywhere outside the EEA. Intriguing, and not present in either the Model Contracts or the E.U.-U.S. Safe Harbor, is the requirement that the burden of proof falls on the E.U. headquarters or delegate in such circumstances to establish that the individual's loss was *not* a result of the multinational's company overseas. In its initial request for an authorisation of the Binding Corporate Rules under Article 26(2), the multinational must include evidence that the EU headquarters (or its E.U. delegate, as the case may be) has sufficient assets within the EEA to cover payment of compensation for breaches of the Binding Corporate Rules, or that it has taken measures to ensure that it would be able to meet such claims, such as, for example, taking out appropriate insurance.

The possibility of relying on Binding Corporate Rules and avoiding many of the drawbacks associated with other approaches, has been met with excitement by data protection practitioners and warmly welcomed *in principle* by many multinationals, ABN&#30;Amro, Citigroup, Daimler Chrysler and Philips to name but a few. Several are already a long way down the road towards developing and implementing a Binding Corporate Rules solution. Concerns remain, however, that the approach may still be to formalistic and that many of provisions required are too onerous or simply "too difficult", particularly in terms of the legal rights to be provided to individuals.

Previous reference was made as to how multinationals wishing to use a contractual solution other than the E.U. model contracts must currently conduct a "Tour of Europe" seeking authorisations from each of the various EEA Data Protection Authorities. This is a time consuming exercise that often leads to variations in the "adequate safeguards" adduced in the various EEA countries. Data Protection Authorities have differing views on certain issues. The Working Party Paper acknowledges these difficulties and refers to a co-ordinated procedure that it hopes to give further guidance on in the future. Certainly, increased co-operation between the Data Protection Authorities would be a good thing, along with a procedure that enables multinationals to deal with one rather than all of the EEA Data Protection Authorities. Perhaps most ideal would be if a process of mutual recognition between the Data Protection Authorities were to develop, whereby an authorisation granted by one Data Protection Authority would be recognised by those of all other EEA countries. Formal timescales for responses by the Data Protection Authorities would also be welcomed, although in reality they may face too many resource shortages to be in a position to make such commitments.

There is still some work to be done before Binding Corporate Rules can be regarded as the simple but robust, effective but low-formality means of safeguarding individuals' personal data overseas it needs to become. The early signs are promising however. Many multinationals are adopting the approach. Some have already had local "approvals" and are in discussions with Data Protection Authorities across the EEA. It is to be hoped that, finally, after so many years, a realistic and "multinational friendly" approach to Article 25 of the Data Protection Directive will be available before too much longer.

The Transfer of Personal Data Regarding Airline Passengers from the E.U to the U.S.

By Heather Rowe, a Partner with Lovells, London.

On January 29, 2004, a Working Party established under the E.U. Data Protection Directive (95/46/EC) produced its opinion number 2/2004 "on the adequate protection of personal data contained in the personal records of air passengers to be transferred to the United States' Bureau of Customs and Border Protection (USCBP)". The Working Party is an independent European advisory body on data protection issues that provides opinions to the European Commission on data protection matters. Passenger Name Record or "PNR" data contain information regarding those passengers on flights to, from and through the United States.

This whole area has been a matter for contention and a regulatory concern for airlines for many months. Airlines were caught between two very different regimes – the legitimate aims of the United States, in the wake of September 11, to combat terrorists and the extensive E.U. data protection laws, designed to protect the individual.

Background

In light of the events of September 11, the United States adopted a number of laws and regulations requiring airlines flying into the United States to transfer to the U.S. administration, personal data relating to passengers (and crew members) flying to and from the United States. For example, airlines were obliged under the legislation to provide the USCBP with electronic access to passenger data contained in the "passenger name record" (PNR) for such flights. Non-compliance could lead to heavy fines for the airlines or even a loss of landing rights, as well as causing delays to their passengers landing in the United States.

The Working Party has already delivered opinions in October 2002 and June 2003 looking at the decisions that were taking place in the United States and the European Union and the dialogue that had taken place, particularly regarding commitments from the U.S. on the conditions for processing PNR which, in June 2003, was still a cause of concern for the Working Party. For example, there were issues surrounding the transfers; the principle of proportionality as regards what data were transferred, as well as when transfers must take place and how long the data would be held. Other considerations focused on the processing of sensitive data and concerns that there should be strict controls on further transfers to other U.S. government or foreign authorities, together with some sort of guarantees for the subject data's individual rights.

The current position is that on January 12, 2004, the Working Party received a European Commission Communication to the Council and to the Parliament entitled "transfers of passenger name records (PNR) data: the need for global approach"; as well as updated versions of undertakings from the U.S. authorities of the same date. Prompted by those documents, the Working Party has produced a new opinion, given the results of further negotiations. Clearly, the dichotomy was trying to balance the steps needed in the fight against terrorism, a necessary and valuable element of democratic society, whilst at the same time respecting the fundamental rights and freedoms of individuals, including their right to privacy, a right which is highly developed in the European Union. In particular, the way that private data is collected for commercial purposes and held in airline databases and is to be communicated to a public authority by access to such system has no precedent in the European Union.

Proposals for Legal Acts to be Adopted

The European Commission's Communication expresses the view that a sound legal basis for transferring PNR to the U.S. authorities should take the form of a European Commission decision under Article 25, paragraph 6 of the Directive, combined with an international agreement authorising the airlines to treat U.S. requirements as legal requirements in the European Union. The agreement would also bind U.S. airlines to treat the U.S. requirements as legal requirements in the European Union and commit the United States to granting reciprocity and ensuring "due process" for E.U. residents. Article 25(6) provides:

> "The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiation referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals".

The Working Party, in the absence of documents yet to be drafted, was not in a position to adopt an opinion with regard to the possible content of such an agreement, but pointed out that the mechanism under Article 25, paragraph 6, by its nature refers to the adequacy of protection for personal data after they have been transferred to a third country and so far they have typically dealt with transfers to private sector organisations in third countries. This is the first time in which the transfer takes place because of a *legal obligation* from a *third country* which requires operators in the European Union to transfer data to a public authority *outside* the European Union in a way which does not conform with the E.U. Data Protection Directive (95/46/EC).

The Working Party opinion reviews what sort of protections are available, under the revised proposals, and in particular takes the view that any Commission

decision approving such transfers should not rest merely on "undertakings" of administrative agencies in the United States, but on officially published commitments which would be "fully binding" on the U.S. side. At the present, the proposed U.S. undertakings will not be legally binding and, indeed, there is wording at the end of them that states that the undertakings "do not create or confer any right or benefit on any person or party, private or public" which is not helpful in terms of swaying the Working Party's decision.

Certainly, there are aspects to the revised proposals which the Working Party approved of, including the introduction of a "sunset clause", giving the package a life of three and a half years to be implemented, as well as purpose limitation – *i.e.*, that the United States had indicated what the purposes were for which PNR data would be used (although it was still somewhat vague). In addition, the Working Party approved that the PNR data is limited to a list of 34 data elements, with various elements previously included now excluded, although there was still little progress on what the list of data elements to be transmitted would be. Indeed, the revised U.S. list still contained 20 elements that the Working Party had previously considered disproportionate and problematic.

It is clear that the Working Party was, however, still exercised by how the United States proposed to treat "sensitive" personal data. Under the E.U. Data Protection Directive, sensitive personal data is described in Article 8, paragraph 1, and refers to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life.

In particular, there still seemed to be scope for certain "free" text fields to be included in PNR data which could include sensitive personal data. Observations on meal preferences or special health requirements would be sensitive, as could a reference to someone as being "clergy". Such data should be deleted, in the view of the Working Party, before transfer.

Other Observations of the Working Party

The Working Party noted that there were some other improvements in the revised proposals, for example in relation to the length of time data would be held. The United States originally said that all data would be held for seven years, but this had been reduced to three and a half years (broadly) although this was still longer than the Working Party had indicated a preference for, being "weeks or months", but was an improvement on the seven years originally proposed by the United States.

As regards the timing of data transfers, the previous opinion of the Working Party recommended that the U.S. Bureau of Customs and Border Protection (CPB) should receive data on specific flights no earlier than 48 hours before the flight departs and that thereafter, that data should be updated once. The revised versions of undertakings from the United States still grant U.S. authorities access 72 hours prior to departure and a maximum of three updates, which the Working Party finds regrettable.

The previous undertakings from the United States were vague about the precise identity of other public bodies who might be entitled to receive the data, stating that there might be onward transfers on a case by case basis, conditional upon the recipient giving undertakings no less favourable than those provided to the European Commission by the United States. However, no comprehensive list of possible authorities has yet been provided and the Working Party remains concerned about the breadth of these provisions.

As regards the rights of the data subject, the Working Party have emphasised that clear information should be provided to the data subject about use of their data; certain rights of access by third parties should be restricted; individuals should have an ability to be able to have their data rectified; and some form of redress should be provided to E.U. residents for considering complaints about use of their data has not been properly dealt with. Not all of those issues have been resolved in the new proposals, and the Working Party is concerned that there is no truly independent redress mechanism.

A welcome development is that there will be review by experts from Member States and the CBP of the implementation of the undertakings and the Working Party expressed the view that they hoped that such reviews would be conducted with the necessary level of openness and transparency.

The Working Party noted that recent experience showed that a new element has to be taken into consideration looking at this area, namely that PNR data collected by CBP are matched in the United States with lists of persons searched. These processing operations had led to the cancellation of flights from the European Union at the last minute, although information subsequently provided revealed that those cancellations were mistakes or cases of unclear data relating to terrorism suspects. The Working Party considered that further initiatives should take place to prevent such consequences in the future.

Conclusion

The Working Party noted the progress made in the U.S./E.U. dialogue concerning passenger PNR data, particularly the proposed January 2004 undertakings from the U.S. administration. It is clear, however, that whilst they are "pleased to record some improvements over the previous version of such undertakings …", their comments also indicate that they are not wholly satisfied with the arrangements:

> "in the Working Party's view the progress made does not allow a favourable adequacy finding to be achieved".

Before being able to say the situation was favourable, the Working Party indicated it would wish there to be progress on various matters such as the uses to be made of passenger data; the fact that no sensitive data should be transmitted; that data subject's rights should be enhanced; that the commitments from the U.S. side should be legally binding; and that onward transfers of passenger PNR data to other government or foreign authorities should be strictly limited.

  WDPR ISSN 1473-3579

Once Confidential, Always Confidential? Personal Data under the U.K. Data Protection Act

By Linda Farrell, Bristows; e-mail: Linda.Farrell@bristows.com

Documents relating to the employment process are frequently produced in the expectation that they will be kept confidential, *e.g.*, statements taken in the course of an investigation into alleged harassment or test results of a promotion or redundancy selection procedure. However, there are circumstances when the veil of confidentiality can be pierced.

Under the Data Protection Act 1998 (DPA), individuals have the right, on payment of a fee, to make a written request for access to data held about them. This is known as a "subject access request".

Service of a subject access request may be the first port of call for someone seeking disclosure of information about them, as press coverage is generating increasing awareness of this procedure. For example, it was used by a City high-flyer to seek information supporting his claim that his career had been ruined by inaccurate information posted by a financial institution on an anti-fraud database.

However, employers who receive a subject access request will often face the dilemma that compliance with the request will necessarily result in disclosure of information about another individual (*e.g.*, identifying a complainant). Under the DPA, the employer is not obliged to comply with the request unless the other individual consents, or it is reasonable in all the circumstances to disclose the information without consent (taking account of any duty of confidentiality owed to the other individual and any express refusal of consent).

When is it "reasonable in all the circumstances" to disclose data about another individual? This issue arose for consideration by the Court of Appeal in the case of *Durant v. Financial Services Authority* [2003] EWCA Civ 1746. In that case the Court noted that there is a real tension in the obligation that the Act imposes on data controllers to respect the right of privacy of others whose names may figure in the personal data of any individual. For example, data may identify another individual as the source of the information. In such cases, both the data subject and the source of the information about him may have their own (and contradictory) interests to protect. The data subject may have a legitimate interest in finding out what has been said about him, and by whom, in order to enable him to correct any inaccurate information given or opinions expressed. However, the other individual may have a justifiable interest in preserving the confidential basis upon which he supplied the information or expressed the opinion.

The Court said that a two-stage process should be adopted to ensure that there is a balancing act between this potential conflict of interests. First, it should be determined whether the information about another individual is necessarily part of the personal data that the data subject has requested. Secondly, if the information does form an integral part of the personal data, then it will depend on all the circumstances whether it would be reasonable to disclose to a data subject the name of that other individual.

The Court also stated that the provisions appear to create a presumption or starting point that the information relating to the other individual, including his identity, should not be disclosed without his consent. It made it clear that this presumption can be rebutted if the data controller considers that it is reasonable "in all the circumstances" to disclose it without such consent.

Due to the complexity of the DPA route, the most likely procedure where tribunal proceedings are on foot is an application for a disclosure order.

In *Knight v. DSS [2002] IRLR 249*, a tribunal ordered disclosure to itself (but not to the disabled applicant, Mr Knight, or his representatives) of marked test papers in connection with a job for which Mr Knight had unsuccessfully applied.

On appeal, the DSS argued that the documents were confidential and that, if they were required to disclose them, the test would have to be re-written at substantial cost. However, the EAT held that confidentiality in itself is not a basis for refusing disclosure of relevant documentation and that, whilst cost is a material consideration, it should not deprive the applicant of disclosure, particularly as this particular test had been in use for many years.

This case can be contrasted with *Asda Stores Limited v. Thomson [2002] IRLR 245*, in which three managers, who had been summarily dismissed for alleged supply of illegal drugs at company events, sought disclosure of witness statements made by other employees in the course of their employer's investigations. Asda resisted the application on the grounds that a promise of confidentiality had been given to the authors of the statements (due to a fear of reprisals) and that disclosure of the statements and their authors' identities was not necessary for a fair disposal of the unfair dismissal claims.

In allowing an appeal against an order by the tribunal for blanket disclosure, the EAT held that the tribunal had failed properly to exercise its discretion. It emphasised that the tribunal ought to have exercised its power to order disclosure of documents in an anonymised or redacted form in order to conceal the witnesses' identities. It noted, however, that it may be proper to exclude a statement altogether if concealment of the witness's identity is impossible.

In Summary

The following key points should be considered in relation to personal data:

- particular care should be taken with subject access requests where personal data of an individual other than the maker of the request is involved;
- confidentiality *per se* is not a reason for a tribunal to refuse a disclosure order and more wide-ranging disclosure may be granted in discrimination cases, provided that the documents are relevant.
- tribunals may, however, refuse disclosure of confidential documents where the identity of other employees or job applicants cannot be concealed.

A previous version of this article was published in Personnel Today (24.2.04).

Security & Surveillance

Assessing the Impact of Workplace Monitoring in the United Kingdom

By Simeon Spencer, a Solicitor with Morrison & Foerster MNP. The author may be contacted at sspencer@mofo.com.

The Information Commissioner's office has published the third section of its Employment Practices Data Protection Code, dealing with monitoring in the workplace. One of the key features of the code is the so-called "Impact Assessment" (IA) which is aimed at assisting employers to meet their data privacy obligations in this complex and controversial area. The Code expressly recognises the need to,

> "strike a balance between a worker's legitimate right to respect for … private life and an employer's legitimate need to run its business" and so the impact assessment is the tool for achieving this.

Although a Code is not "law" and so not legally binding in itself, nevertheless the Courts are charged with the duty to take it into account when determining relevant issues under data privacy law. The Code is therefore a useful yardstick for compliance, providing essential benchmarks and pointers for an employer to navigate through what can be a bewildering array of regulation in this relatively new area of concern. The central message to all employers who are carrying out monitoring activities or who are contemplating doing so is that they should embrace the positive recommendations and guidance in the Code, making the process of achieving compliance more manageable and so less of a burden than is really necessary.

In essence, the IA is the process by which an employer arrives at the correct and justified decision as to whether monitoring in a given context is appropriate. The assessment process enables the employer to examine which type of monitoring is most appropriate to adopt, and to ensure that any adverse impact on the worker is properly balanced by the benefits to the employer and/or others.

The Commissioner's monitoring code states that an IA will involve identifying the purpose(s) behind monitoring and its benefits, any adverse impact that may arise, consideration of any alternatives, taking into account the obligations that arise from monitoring, and judgment as to whether monitoring is justified.

Scope of the Impact Assessment

The IA should cover existing and future monitoring, and for ongoing or one-off monitoring activities. Since facts and circumstances change over time, assessments should be used to achieve justified monitoring in the first place and then also to review that justification periodically.

The forms of possible monitoring potentially caught by the Data Protection Act are wide and varied and can include information gathered through point of sales terminals, CCTV footage, randomly opened e-mails, website logs, telephone recordings, or credit reference agency information, drugs and alcohol testing (see Part 4 of the Code).

Carrying out an Impact Assessment

The guiding aim is to achieve balance between adverse impact (*i.e.*, intrusion and/or damage) on workers and the employer's business benefit. The Code highlights some of the considerations that should be made when assessing adverse impact:

- Intrusion into private lives of workers and others. It is important to remember that "expectation of privacy" may extend to the workplace.
- The state of knowledge of workers and others about monitoring and their ability to limit its use.
- To what extent sensitive information captured by the monitoring process will be seen beyond a need-to-know basis?
- The impact on mutual trust and confidence.
- The impact on extraneous relationships, for example, with trade unions and representatives.
- Impact on those with professional secrecy obligations (for example, doctors or solicitors).
- Any oppressive or demeaning effects as a result of monitoring.

Employers should broadly consider the expectation of privacy amongst the workforce. What culture or atmosphere has either been created or does the employer wish to create? What sort of culture does the employer's industry normally engender? In this regard, it is essential that employers always give fair consideration to whether alternatives can be utilised both in terms of the methods used for monitoring and any alternatives to monitoring that could be used. The code suggests that employers should consider a number of issues. For example, could established or new methods of supervision, effective training and/or clear communication from managers – rather than electronic or other systematic monitoring – deliver acceptable results? Could targeted monitoring on specific incidents replace continuous monitoring? Employers could also consider limiting monitoring to specific complaints or other suspicion of wrongdoing.

Employers must consider their broader data protection obligations when deciding what monitoring activities they are going to carry out. For example, whether and how workers are notified of monitoring activities, how the information collected is secured and handled, as well as the implications of subject access rights to the information gathered. These are all wider obligations under the Data Protection Act.

Justification

Justification is really the drawing together of the employer's considerations and conclusions in respect of adverse impact and benefits. Justification can involve a consideration of areas such as the benefits of monitoring, alternative methods, fairness to individuals, limiting intrusion, or recognising that significant intrusion into private lives will not be justified unless the business is at real risk of serious damage.

"Supporting Guidance" to the monitoring code, published by the Information Commissioner, will help employers to assess how intrusive certain types of monitoring will be. The guidance uses a sliding scale approach to indicate what level of intrusiveness is proportionate to the degree of privacy an employee will normally expect with regard to their communications. Purely business communications, for example, are least likely to cause damage or distress, and involve a disproportionate infringement of privacy. Communications that contain both business and private information (often including HR communications), the guidance makes clear that the approach to monitoring must vary according to the specific circumstances but that those who are involved in this must understand the proper procedures and be fully trained before they are allowed to perform monitoring. For purely personal communications, the risks posed need to be managed very carefully indeed. The Code uses the example of access to pornographic websites to explain that even personal usage may need to be monitored for specific and valid reasons. The guidance makes it clear that monitoring to check for abuse of this sort may be reasonable, but must always be no more than is necessary to achieve the purpose of the monitoring. Even a total ban on personal communication may not justify monitoring the content of personal communications.

The Code does not cite business "benefits" as a separate area of consideration for the IA, but the employer would be well advised to give separate consideration to this, as it is fundamental to the question of justification. The greater the benefit *e.g.*, averting damage to the business or serious health and safety issues – the greater the likely weight of justification against adverse impact. An example of this would be in the tricky area of drug and alcohol testing. Where the employer is seeking to impose a systematic regime of drug and/or alcohol testing the business benefits needs to be overwhelming and will probably only be result in justification if there is a real health and safety dimension to take into consideration.

Should Assessments be Written or Oral?

Although the code states that an impact assessment does not have to be written down and could be merely an oral assessment, in the modern world of employment rights any employer would be well advised to commit their assessments to written form at all stages, including the initial consideration stage.

Any non-documented process or procedure that affects workers' rights will have a tendency to be viewed with suspicion, both by the workers affected by it and by the courts or employment tribunals involved in disputes.

The prudent employer will also retain copies of documentation received at the input stage – for example, relevant policies, reports on incidents, and any information gathered from existing monitoring not yet covered by an impact assessment. Other information could include: minutes of meetings held with individuals along with any collective consultations; written records of opinions from interested parties; and reports detailing assessment findings, conclusions that have been drawn and any actions to be taken.

Wider Considerations

The code sets out some five "core principles" to encapsulate the general approach that employers should take towards monitoring at work.

- It will usually be intrusive to monitor your workers.
- Workers have legitimate expectations that they can keep their personnel lives private and that they are also entitled to a degree of privacy in the work environment.
- If employers wish to monitor their workers, they should be clear about the purpose and satisfied that the particular monitoring arrangement is justified by real benefits that will be delivered.
- Workers should be aware of the nature, extent and reasons for any monitoring, unless (exceptionally) covert monitoring is justified.
- In any event, workers' awareness will influence their expectations.

The Benefits of Conducting an Impact Assessment

Employers may justifiably question the worth of an IA when confronted with the requirement to conduct a time-consuming exercise in respect of monitoring activity they have conceivably been carrying out for some considerable time, or which they consider essential to their business.

It is perhaps not convincing enough to merely say that the Information Commissioner has recommended it and so compliance with the Data Protection Act is more likely as a result. However, the benefits of carrying out IAs potentially stretch beyond straight privacy law compliance. IAs and the process of carrying them out can produce tangible benefits for businesses.

- Employers who carry out IAs in an open and transparent manner will engender trust and confidence in the workforce. A contented and trusting workforce is generally a more productive workforce.
- Not all monitoring will be necessary or legitimate in all contexts. IAs assist employers in making the right decision as to whether to monitor in a given context before tackling the decision of how to monitor and to what degree.
- Compliance through properly conducted IAs will help to avoid legal actions being brought by workers. Legal action against employers may be wider than just actions for breach of the Data Protection Act itself and may include such employment actions as unfair dismissal or workplace discrimination. If legal actions are brought, information in support of the employer will be more persuasive in a court or employment tribunal if it has been properly gathered through monitoring conducted on the strength of an IA.

- Ensuring a measured and targeted approach to monitoring will result in responses being directed properly to the objective in hand and not wasted on wider monitoring that is unnecessary.
- IA provide a solid foundation of legitimacy in monitoring that allows employers to acquire the information necessary to deal with "problematic" issues in the workplace.
- The Code is formulated with the E.U. Data Protection Directive in mind. Carrying out proper IA will mean that employers are also likely to be complying with much of the laws of other jurisdictions. A health warning applies to this though since employers should be aware that several jurisdictions view monitoring at work very differently indeed.
- IA can help compliance with laws and regulations that impinge upon monitoring at work – for example, employment statutory rights, such as unfair dismissal and discrimination, and also other statutes such as the Regulation of Investigatory Powers Act and the Human Rights Act.
- The results of IA will inform the employer on the right policy and procedures for monitoring. They can also assist in the formulation and application of related policies and procedures, such as e-mail and Internet use, disciplinary and performance, or equal opportunities.
- The working environment can be an underestimated key to success and productivity. IA will assist an employer in striking the right balance between workers' freedom and the need to ensure that operations are controlled.
- Carrying out an IA will assist in raising awareness, not only of those involved in the process, but those who are affected by the outcomes. They will be given a greater awareness of data protection and privacy issues in the workplace and the importance of personal data privacy, both internally and externally.

Additional Issues

The following points are some further steps and considerations, some of which arise out of the Code, that employers may take into account when carrying out IA and deciding what monitoring to carry out in the workplace:

- Employers may consider carrying out a "general" IA aimed at determining whether monitoring is appropriate in the workplace at all followed by a more focused IA for each of the monitoring activities proposed, to establish the justification and the depth of monitoring that is appropriate.
- Employers should always identify who within the organisation has the power to authorise monitoring.
- The person with authority should be well-educated in the wider implications of monitoring, as well as the employer's obligations under the Data Protection Act.
- Carry out IA both on present monitoring and any planned monitoring.
- Ensure that any other policy which either impacts upon monitoring at work, or is affected by it, is taken into consideration when carrying out IA and that the results of IA are made clear in the relevant policies.
- Where specific IA have been properly carried out, this should assist employers in setting out specific and separate policies in each of the areas considered.
- Update workers of any changes in monitoring activity.
- When carrying out IA, give full consideration to those who will have access to the personal data collected and ensure security measures and confidentiality requirements are in place.
- Ensure those who are going to be responsible for carrying out monitoring understand their role and the limits of what they are doing, or are required to do – for example, IT personnel.
- Ensure the dissemination of data obtained through monitoring activities is on a strictly need-to-know basis.
- If outside agencies are to be used to carry out monitoring activities, employers should factor into the IA the lack of control that will come as a result. Employers should ensure that proper controls are exerted over the outside agency's activities. A contract should be put in place requiring proper security measures and ensuring that the outside agency does not gather information beyond that requested by the employer.
- An employer can also use the process of carrying out a general and then focused IA to inform itself of the wider training and education needs of the workforce and management involved to ensure best practice and "buy-in" from those affected.
- Carrying out IA will also throw up lateral thinking about ways to avoid or minimise monitoring and intrusion – for example, creating workplace "Internet cafes" for private web surfing or setting up separate phone lines for personal calls.

Conclusion

Respect for private life is a basic human right enshrined in the European Convention on Human Rights and is the rationale behind data privacy in the Data Protection Act 1998. The right to respect for private life is not relinquished at the factory gates or in the lift to the office. Working environments akin to the Orwellian dystopia is hardly on the agenda of the average employer. Equally, most employers are appreciative of the productive benefits of a contented workforce. Yet, varied forms of monitoring are now commonplace and the received wisdom is that monitoring is an integral aspect of business success. Productivity lost through excessive surfing of the net and wider liabilities created by inappropriate use of technology by workers are, amongst many others, legitimate concerns for any employer. Castigated and applauded in equal measures by each side of the industrial divide, the Code truly seeks to balance out the inherent tension between Orwellian intrusiveness and the business imperative that lies behind all monitoring.

It is fair to say that monitoring in the workplace presents to employers a particularly controversial and complex area of data privacy law, with real potential for challenge from workers in a number of liability areas. However, it is also the case that the employer who has taken the time to acquaint itself with the IA process and has made the effort to carry out impact assessments, will have little to fear from the wider liabilities that can flow from monitoring that is improperly carried out and ill-justified.

Surveillance of Workplace Communications: U.S. Employer Rights

By Charles H. Kennedy and Trisha Kanan. Charles H. Kennedy is a Partner in the Washington, DC office of Morrison & Foerster LLP. Trisha Kanan is an Associate in the Los Angeles, California office of Morrison & Foerster LLP. Mr. Kennedy can be reached at ckennedy@mofo.com; Ms Kanan can be reached at tkanan@mofo.com

U.S. law gives employees few protections against employer surveillance of their workplace communications. Even without express employee consent, U.S. employers generally may listen to workplace telephone conversations, read messages sent to and from corporate e-mail accounts, and record and disclose the contents of employee communications. Employees that bring legal challenges to these practices rarely succeed in U.S. courts. The recent decision of the U.S. Third Circuit Court of Appeals in *Fraser v. Nationwide Mutual Insurance Company*, 352 F.3d 107 (3d Cir. 2003), which upholds an employer's reading of an employee's electronic mail ("e-mail") messages, typifies the obstacles that complaining employees face under U.S. law.

Background to the *Fraser* Decision: The Electronic Communications Privacy Act

In the United States, monitoring of employee communications is governed primarily by the Electronic Communications Privacy Act of 1986 ("ECPA"), 18 U.S.C. § 2510 *et seq*.[1]The ECPA is divided broadly into restrictions on two kinds of activity:

- interceptions, which are acquisitions of communications in real time (*e.g.,* while the parties to a conversation are speaking or while an e-mail is in process of transmission); and
- unauthorised access to communications after they have been placed in electronic storage.

The interception and access-to-stored-communications restrictions often are referred to, respectively, as Title I and Title II of the ECPA.

Taken together, these prohibitions apply to most kinds of electronic surveillance, including listening to and recording wireline and wireless telephone calls, reading e-mail, and use of hidden microphones to eavesdrop on oral conversations. The ECPA applies to wire, oral and electronic communications, and the statute defines each of these categories in highly technical terms. At the risk of some over-simplification, wire communications contain the human voice, in analog or digital form, and may be carried over wireline or wireless facilities. 18 U.S.C. § 2510(1). Oral communications generally are ordinary, acoustically-transmitted human conversations that occur under conditions disclosing a reasonable expectation that those conversations will not be intercepted. 18 U.S.C. § 2510(2). Electronic communications may be wireline or wireless and include, but are not limited to, e-mail and other online communications. 18 U.S.C. § 2510(12). Both governmental and private parties are subject to ECPA restrictions.

Unlike the counterpart regulations in many European jurisdictions, the ECPA is not comprehensive. A careful reading of the ECPA, including the definitions of key terms and the statute's numerous exceptions, discloses ample scope for monitoring and recording of communications. A complete discussion of the gaps in the statute's coverage is beyond the scope of this article, but those statutory provisions with particular value to employers are worth noting.

Activities That Are Not Classified as Interceptions

When an employer is accused of violating an employee's rights under the ECPA, the employer's legal position is improved if the challenged action can be classified as access to a stored communication rather than an interception. The ECPA's prohibitions against interceptions, which involve the acquisition of the contents of a communication with the aid of an electronic, mechanical or other device, are more stringent than the prohibitions against unlawful access to stored communications. "Intercept" for purposes of the ECPA is "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device". 18 U.S.C. § 2510(4). For example, as we discuss further below, courts have found that an employer that provides a communication service to its employees may read those communications, when in storage on the employer's system, for any purpose. Real-time *interceptions* of employee communications, however, may be unlawful unless they come within specific statutory exceptions.

The distinction between real-time interception of a communication, and access to that same communication in storage, is complicated by the technology of electronic communications in the digital era. E-mail systems, in particular, combine transmission and storage functions in ways that might not have been fully anticipated when the ECPA was written, and plaintiffs have tried to persuade the courts that intermediate or temporary storage of an e-mail by the service provider should not convert the acquisition of that message from an interception to a mere acquisition of a stored communication.

An early example of this issue was the case of *Steve Jackson Games, Inc. v. United States Secret Service ("Steve Jackson Games")*, 36 F.3d 457 (5th Cir. 1994), superseded by statute as stated in *Konop v. Hawaiian Airlines, Inc*., 302 F.3d 868 (9th Cir. 2002). In that case, the U.S. Secret Service had seized, pursuant to a search warrant, a Steve Jackson Games server that contained 162 e-mail messages that had not been opened by their intended recipients. Steve Jackson Games, Inc. was a publisher of role-playing games that operated an electronic bulletin board system which offered its customers the ability to send and receive e-mail. Among other claims,

Steve Jackson Games alleged that the e-mails, although stored in the server, had been intercepted for purposes of the ECPA because the government had acquired the e-mails prior to delivery and prevented their delivery. The district court rejected this argument on the ground that under the ECPA, an act of interception must be "contemporaneous with the [communication's] transmission". *Steve Jackson Games,* supra*,* 36 F.3d at 460-461. On appeal, the Court of Appeals also rejected the plaintiff's interception claim, but on the ground that the definition of "electronic communication" in the ECPA – unlike that statute's definition of "wire communication" – did not include an electronic communication while in electronic storage. Accordingly, by definition, acquisition of an electronic communication while in electronic storage could not be an interception of that communication.[2]

Subsequent decisions have confirmed the difficulty of challenging the seizure of a stored communication as an interception. Notably, in *Konop v. Hawaiian Airlines, Inc.,* 302 F.3d 868, 872 (9th Cir. 2002), *cert. denied*, 537 U.S. 1193 (2003)*,* the U.S. Court of Appeals for the Ninth Circuit reviewed the case of Konop, an airline pilot who "maintained a website where he posted bulletins critical of his employer, its officers, and the incumbent union …. " An officer of Konop's employer, using other employees' names, gained access to the website and read Konop's critical postings. Among other claims, Konop alleged that his employer's activity violated the ECPA interception and access-to-stored communications provisions. The district court granted summary judgment for the employer on both claims, and Konop appealed.

On the interception claim, the Court of Appeals, following the rationale of *Steve Jackson Games,* concluded that, "for a website such as Konop's to be 'intercepted' in violation of the [ECPA], it must be acquired during transmission, not while it is in electronic storage". *Konop*, supra, 302 F.2d at 878. Accordingly, the Court of Appeals upheld the district court's grant of summary judgment for the employer on that claim.[3]

Not all employer efforts to monitor employees' communications, however, will fall outside the "interception" category. Where an employer listens in on or records an employee's telephone conversation, or otherwise acquires the contents of an employee communication that has not been placed in electronic storage, those actions will be characterised as interceptions under the ECPA. Even where an employer's actions fall within the "interception" category, however, certain exceptions to liability may be available to the employer. The principal exceptions are discussed below.

Permitted Interceptions: The Business Extension Exception

One important gap in the ECPA's interception restrictions is known popularly as the "business extension" exception. Specifically, a call is not intercepted for purposes of the ECPA if the device by which the contents of a conversation are acquired is,

> "any telephone or telegraph instrument, equipment or facility, or any component thereof … furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business".

18 U.S.C. § 2510(5)(a). This language is generally interpreted to mean that an employer acting in the ordinary course of its business, and using an extension telephone or other device provided by the telephone company or other communications service provider, may listen to – and perhaps even record – employee conversations that take place on the employer's business premises.

However, the business extension exception is not absolute. Notably, not every recording or interception device an employer might use will qualify as a permitted telephone "instrument, equipment or facility" under the business extension exception.

As a general rule, employers are more likely to qualify for the exception if they monitor employee communications by means of extension telephones or other equipment normally provided by telephone companies, rather than specialised surveillance and recording equipment. In *Williams v. Poulos*, 11 F.3d 271, 280-281 (1st Cir. 1993), for example, the First Circuit Court of Appeals found that alligator clips placed on a telephone line on the employer's premises were not devices of the kind contemplated by the business extension exception. Similarly, in *Deal v. Spears*, 980 F.2d 1153, 1158 (8th Cir. 1992), the Eighth Circuit Court of Appeals found that a recording device connected to the employer's extension telephone did not qualify for the exception. However, in *Epps v. St. Mary's Hospital, Inc*., 802 F.2d 412, 415 (11th Cir. 1986), the Eleventh Circuit Court of Appeals held that an employer's use of a double-reeled tape recorder, attached to an ambulance dispatch console on which emergency telephone calls were terminated, qualified under the exception.

Employers relying on the business extension exception must also demonstrate that their use of interception or recording equipment was "in the ordinary course of its business". 18 U.S.C. § 2510(5)(a). In interpreting this language, the courts distinguish employees' business calls, which may be extensively monitored if necessary to serve the employer's business purpose, and personal calls, which ordinarily may be monitored only to the extent necessary to ascertain that those calls are, in fact, personal. See *Watkins v. L.M. Berry & Co*., 704 F.2d 577, 581 (11th Cir. 1983). In *Ali v. Douglas Cable Communications*, 929 F. Supp. 1362, 1373 (D. Kan. 1996), for example, the district court found that an employer that listened in extensively on its sales representatives' business conversations in order to "monitor [representatives] in the use of proper skills and to assist the [representatives] with difficult customers" acted in the ordinary course of business within the exception. In *Deal v. Spears,* supra, 980 F.2d at 1158, however, the Eighth Circuit Court of Appeals found that an employer's interest in preventing use of its telephones for personal calls might justify limited monitoring, but did not support "record[ing] twenty-two hours of calls" and listening to all of them. Similarly, in *United States v. Harpel*, 493 F.2d 346, 351

(10th Cir. 1974), the Tenth Circuit Court of Appeals found "as a matter of law that a telephone extension used without authorization or consent to surreptitiously record a private telephone conversation is not used in the ordinary course of business".

Permitted Interceptions: The "One Party Consent" Exception

Unlike the statutes of some of the states, the ECPA permits a communication to be intercepted so long as "one of the parties to the communication has given prior consent to such interception". 18 U.S.C. § 2511(2)(d). Accordingly, under federal law, an employee's consent to the employer's interception of a communication, even where the consent of the other party to that communication is lacking, may immunise the employer from liability. This exception, where available, has obvious advantages over the business extension exception. Notably, where the employee's consent to interception has been obtained, the employer need not prove that the device it used to make the interception was of the kind ordinarily provided by the telephone company. Also, the one party consent exception does not require proof that the interception was in the ordinary course of the employer's business.

In order to take advantage of an employee's consent to interception of his or her communications, however, the employer should make the employee's consent to interception an express condition of employment, and should state that policy clearly in employee handbooks and other corporate communications as appropriate. Courts have denied employer claims of employee consent where the policy had been not been stated with sufficient clarity. In *Williams v. Poulos*, supra, 11 F.3d at 281, for example, the First Circuit Court of Appeals rejected an employer's consent defense on the ground that the employee was not "informed (1) of the manner – i.e., the intercepting and recording of telephone conversations – in which this monitoring was conducted; and (2) that he himself would be subjected to such monitoring". Similarly, in *Deal v. Spears*, supra, 980 F.2d at 1157, the Eighth Circuit Court of Appeals rejected a defense based upon consent when the employee was not informed "that [the employer was] monitoring the phone, but only [that the employer] *might* do so … ".(emphasis added).

Permitted Interceptions: Protection of the Employer's Rights or Property

Interceptions of employee communications also are permitted where the employer is the "provider of a wire or electronic communication service" over which the communications are transmitted, and interception is "a necessary incident to the rendition of [the] service or to the protection of the rights or property" of the employer. 18 U.S.C. § 2511(2)(a)(i). This exception is especially useful where an employee is suspected of communicating trade secrets or other proprietary information of the employers, or is engaging in other activities that harm the employer's business interests.[4] Where those circumstances apply, an interception may be permitted even where the business extension or one-party consent exceptions are unavailable.

Employer Access to Stored Employee Communications

As noted earlier, the ECPA provisions concerning access to stored communications are more lenient, as applied to employers that provide communications capabilities to their employees, than the interception provisions. Specifically, the stored communication provisions expressly do not apply to "conduct authorized . . . by the person or entity providing a wire or electronic communications service". 18 U.S.C. § 2701(c)(1). For example, in *Bohach v. City of Reno*, 932 F. Supp. 1232, 1236 (D. Nev. 1996), the court found that the plaintiffs' employer, the City of Reno, Nevada, was the "provider" of an electronic communications service used by the employees. Accordingly, both the City and its employees were permitted to "do as they wish[ed] when it [came] to accessing communications in electronic storage" on that service.

To the extent employee communications are stored on the employer's server, therefore, the employer may read those communications regardless of whether they were acquired through use of a business extension, or whether any party to the original communication consented to such access, or whether such access is necessary in order to provide the service or protect the employer's rights or property.

The *Fraser* Decision

The most recent appellate decision concerning employer access to employee communications involves Richard Fraser, an independent insurance agent for Nationwide Mutual Insurance Company ("Nationwide") until he was fired in September 1998 for disloyalty. See *Fraser v. Nationwide Mutual Insurance Company*, 352 F.3d 107 (3d Cir. 2003), affirming in part and remanding in part, 135 F. Supp. 2d 623 (E.D. Pa. 2001). About a month before his termination, the company learned that Fraser had drafted letters to two competing companies expressing dissatisfaction with Nationwide and seeking to determine whether the competitors would be interested in acquiring certain of his policyholders. After learning about these letters, Nationwide became concerned that Fraser might be revealing company secrets to its competitors. In an effort to determine whether Fraser had actually sent letters to any of its competitors, Nationwide searched its main file server for any e-mails to or from Fraser that showed improper behaviour. The e-mail search confirmed Fraser's disloyalty, and his contract with the company was terminated.

Unwilling to accept his termination, Fraser brought suit against Nationwide alleging various claims, including violation of his privacy rights under the ECPA and a parallel state statute. Fraser claimed that the company's actions in accessing his e-mail without his permission violated the interception provisions of ECPA Title I. He also claimed that the company's search of his e-mail violated Title II of the ECPA, which creates liability for accessing, without authorisation, electronic communications in electronic storage. The district court disagreed, and granted summary judgment in favour of Nationwide. Fraser appealed.

Fraser Court Finds No "Interception" of Employee's E-Mail

The primary issue in Fraser's Title I claim was whether Nationwide had "intercepted" an electronic communication when it accessed Fraser's e-mail in storage. The district court had found that the company's actions did not constitute an unlawful "interception," but reached that conclusion under a questionable interpretation of the law that would, if accepted by other courts, have limited the ability of employers to argue that certain acquisitions of stored e-mail are not interceptions. Specifically, the district court took the view, rejected by the Court of Appeals in *Steve Jackson Games,* that access to a stored message that has not yet been retrieved by its recipient is an interception under the ECPA. On this view, because Fraser's e-mail message was accessed from the employer's server after it had been delivered, the employer's action in reading that e-mail was not an interception. *Fraser*, supra, 135 F. Supp. 2d at 635.

Although the district court ruled for the employer on the interception issue, acceptance of its rationale by other courts would harm the interests of employers. According to the district court's reasoning, had Konop's employer retrieved the e-mail after it was sent, but *before* the intended recipient had opened it, the employer would have "intercepted" the communication rather than gained access to a stored communication. On this rationale, employers would be protected from interception claims only if they accessed messages that happened to have been delivered before the act of access occurred.

On appeal, the Third Circuit affirmed that there was no interception, but did so without endorsing the district court's idiosyncratic reading of the ECPA. Expressly endorsing the reasoning of *Steve Jackson Games,* the Third Circuit agreed that an "intercept" under the ECPA cannot be accomplished by acquisition of messages in electronic storage. Because the company did not monitor the messages in real time as they were transmitted, the Third Circuit found here, as the Fifth Circuit had found in *Steve Jackson Games*, that Nationwide did not "intercept" Fraser's e-mails. Accordingly, Nationwide's search did not violate Title I of the ECPA. Consistent with the *Steve Jackson Games* rationale, the court did not suggest that the result would have been different if the employer had retrieved Fraser's e-mail before it was delivered.

Fraser Court Finds No Violation of ECPA Title II

Fraser also alleged that Nationwide violated Title II of the ECPA when it retrieved, without authorisation, Fraser's e-mail from electronic storage on the company's server. The district court rejected this argument, and relied in doing so on its own interpretation of the ECPA's definition of "electronic storage". According to the ECPA, electronic storage includes any "temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication . . . for purposes of backup protection of such communication". 18 U.S.C. § 2510(17). In the district court's view, the definition's reference to "temporary, intermediate storage" must mean storage of a message before it has been retrieved by the addressee, and the reference to "backup protection" must mean temporary storage that "protects the communication in the event the system crashes before transmission is complete". *Fraser, supra,* 135 F. Supp. 2d at 636. Applying this gloss on the statutory definition, the district court found that because the e-mail in question was neither in "temporary, intermediate storage" nor in "backup" storage, it was not unlawfully acquired from electronic storage for purposes of Title II of the ECPA.[5]

On appeal, the Third Circuit expressed appropriate scepticism about the district court's reading of the "electronic storage" definition, then affirmed the district court's decision on different grounds. Specifically, the court relied on the holding in *Bohach v. City of Reno*, supra, 932 F. Supp. at 1236-1237 to find that Nationwide's search of Fraser's e-mail fell within the service provider exception to Title II. Under this exception, a provider of an electronic communications service may access communications in electronic storage on its system without violating the ECPA. As noted earlier, in *Bohach*, the court held that the Reno police department could retrieve pager text messages stored on the police department's computer system because the department is the provider of the service and "service providers [may] do as they wish when it comes to accessing communications in electronic storage". Because Fraser's e-mails were stored on a system administered by Nationwide, the Third Circuit held that the company's search likewise fell within the provider exception.[6] Accordingly, Nationwide's search did not violate Title II of the ECPA.

Conclusion

The *Fraser* decision demonstrates the continuing disadvantages faced by U.S. employees who challenge their employers' workplace surveillance practices. Against this background, the best advice an American attorney can give an employee client is to assume that none of his or her workplace communications is private.

1 In addition to the ECPA, monitoring of employee emails is also governed by the electronic surveillance laws in each of the individual states in which the employer does business, or with which employees are likely to have online contact. In assessing their rights to engage in, or challenge, any particular surveillance activity under U.S. law, employers and employees should consult applicable state privacy laws, including state wiretap/eavesdropping statutes and common-law causes of action such as invasion of privacy. Detailed discussion of these state law theories is beyond the scope of this article.

2 The USA PATRIOT Act, enacted several years after the *Steve Jackson Games* decision, erased this distinction between wire and electronic communications by amending the definition of "wire communication" to exclude such communications in electronic storage. Pub. L. No. 107-56, §209, 115 Stat. 272, 283 (2001).

3 See also *United States v. Steiger*, 318 F.3d 1039, 1048-49 (11th Cir. 2003), cert. denied, 123 S. Ct. 2120 (2003); *Wesley College v. Pitts*, 974 F. Supp. 375, 384-385 (D. Del. 1997), summarily aff'd, 172 F.3d 861 (3d Cir. 1998).

4 See, e.g., *United States. v. Mullins*, 992 F.2d 1472 (9th Cir. 1993), cert. denied, 510 U.S. 994 (1993); *United States v. McLaren*, 957 F. Supp. 215 (M.D. Fla. 1997); *United States v. Christman*, 375 F. Supp. 1354 (N.D. Cal. 1974).

5 The district court's argument, in *Fraser*, that post-transmission storage of email is not "electronic storage" under the ECPA was recently rejected by the Ninth Circuit Court of Appeals in *Theofel v. Farey-Jones*, 2004 U.S. App. LEXIS 2555 (9th Cir. February 17, 2004), amending 2003 U.S. App. LEXIS 26896 (9th Cir. 2003).

6 But see *Fischer v. Mt. Olive Lutheran Church*, Inc., 207 F. Supp. 2d 914, 924-926 (W.D. Wis. 2002) (holding that plaintiff's Hotmail e-mail was protected by Title II of the ECPA because it was in "electronic storage" on a third-party, web-based server).

News

EUROPEAN UNION

Parliament Members Object to EC Proposal for Biometric Passports

The United States and the European Union look set to conflict over the use of biometric passports as members of the European Parliament have raised objections to a European Commission proposal to require mandatory facial images and the option to use fingerprints.

At a European Parliament hearing, European Parliament member Graham Watson said the Commission proposal "raises more questions than answers". Watson, who heads the Liberal Democratic party, added that "proposals to include biometric identifiers in visas and passports raise serious questions of privacy, reliability, and cost. It is far from clear that these are outweighed by the potential security benefits.

"We need to know who will have access to this data and what for", Watson said. "We must ensure that adequate safeguards are in place, and that doubts about reliability are addressed. We have to weigh the high public costs of this technology against the value and greater security that it delivers."

Based on recent European Commission proposals, E.U. passports will require a facial image but the addition of fingerprints will be left up to individual E.U. Member States. The new passports, containing a chip with biometric data, would be issued from 2005. A database containing the photos of all E.U. passport applicants also will be set up.

Justice and Home Affairs Commissioner Antonio Vitorino defended the Commission proposal and said it struck a balance between protecting data privacy and ensuring national security needs in the fight against terrorism.

Meeting with U.S. Officials in May

Vitorino said he will meet with U.S. officials in May in order to convince them to delay the October 26, 2004 deadline for implementation of biometric passports. According to U.S. law, any arriving foreign citizen must have biometric data in his or her passport. If not, the person cannot enter without a visa. Currently all E.U. citizens except those from Greece can enter the United States without a visa.

Meanwhile, a U.S. embassy official said the chances of granting the European Union a delay in enforcing the new law were slight.

"The change of the October deadline would require a vote from the United States Congress as it would require a change in the legislation", said the U.S. official, who spoke on the condition of anonymity.

Based on the mood of many members of the European Parliament, it is unlikely that the required E.U. legislation will be in place anytime soon.

More Debate Needed

Ole Sorensen, the European Parliamentarian who will steer the Commission proposal through the Committee for Civil Liberties before it reaches a vote in the General Assembly, said there needed to be much more debate on the issue.

"A key element of this fight involves protecting the fundamental values which form the basis of our democratic societies", Sorensen said. "Before embarking on such far-reaching and unprecedented legislation, we need a thorough debate on all the possible ramifications. The current proposals on the use of biometrics could be a step towards systematic and centralised storage of sensitive personal data." Such a step would obviously go beyond what is required.

"It would be premature to adopt this legislation until our concerns about privacy, reliability and cost have been addressed", Sorensen continued. "It should certainly not enter into force without reciprocal obligations on U.S. visitors to Europe."

The Commission proposal was also heavily criticised by Statewatch, a non-governmental organisation dedicated to protecting civil liberties.

"There are no plans, or political will, to make data protection effective in protecting the right to privacy or to guard against the misuse and abuse of the data", said Statewatch official Tony Bunyan. "The rationale for the measure is another response to September 11 and the war on terrorism. It has little to do with combating terrorism and a lot to do with the demands of the law enforcement agencies for the surveillance of everyone's movements."

A member of the European Biometrics Forum dismissed the fears outlined by MEPs and said the E.U. data protection law would ensure there were no abuses of the biometric data.

Vitorino said that while the European Parliament does not have veto power over the Commission proposal it would be political difficult to approve the legislation without its consent.

E.U. heads of state and government already pronounced their approval of biometric passports when it called for them at a summit in June of 2003.

Review

BOOKS

Data Protection Strategy – Implementing Data Protection Compliance

By Richard Morgan IT Consultant and Ruth Boardman, Partner, Bird and Bird.

Published by Thomson Sweet & Maxwell 2003. ISBN 0421 838302

Review by Sally Annereau, Data Protection Analyst, Taylor Wessing, London.

Data Protection and privacy law is to an extent, still seen by many as the preserve of a small community of specialist data protection compliance practitioners, engaging in esoteric discussions about different concepts of privacy, human rights and data handling standards.

The real world however, is different. In practice, finance directors or IT managers who are employed by a business that has never previously considered data protection, may one day find themselves "allocated" responsibility for data protection compliance. In short, this means undertaking the long and thankless task of checking what responsibilities the business has and ensuring appropriate procedures are in place.

The Data Protection Act 1998 is complicated and was described by the Court of Appeal law in the case of *Naomi Campbell v. Mirror Group Newspapers Limited* ("MGN") as a "cumbersome and inelegant piece of legislation" [*Naomi Campbell v. MGN Limited* [2002] EWCA Civ No:1373, October 14, 2002]. The compliance practitioner is not offered easy to follow practical rules but is instead faced with a number of loosely defined principles with potentially far-reaching scope, that are bounded by complex sets of processing pre-conditions, exemptions and special arrangements for different categories of data processing. All in all, the requirements and how to achieve them are far from clear.

For these new and possibly reluctant entrants to the data protection arena, help is now at hand in the form of "Data Protection Strategy – Implementing Data Protection Compliance". The book offers re-assurance to the reader by guiding them through a number of process-driven stages designed to help them put a compliance strategy in place within their business, whilst at the same time learning why, in data protection terms, different actions are important.

As a first step in this process, the reader is given some basic background information on data protection. Importantly, the authors then go straight into explaining the consequences of getting things wrong by setting out the different types of criminal offences, sanctions and other legal actions that can be taken against the business, its officers and in certain cases, employees. Understanding what can happen when things go wrong is often the first point the reader will need to impress upon his management and the board in order to make sure he has their backing, and budget, to make a proper job of undertaking an audit and implementing the audit's findings. Therefore, the sequence of topics in the book reflects real-world practice and requirements.

The authors then move on to consider the process of preparing for and undertaking the audit. The authors rightly point out that this process is best undertaken by independent auditors and to some extent, the auditing chapter is presented on the basis that this is the chosen route. If for reasons of budget, the reader finds that he has to carry out the audit exercise himself, he may need to seek more practical advice on how to draw up audit questionnaires or conduct audit interviews than is provided in the book. However, the chapter does include a useful critique of the Information Commissioner's audit manual and tips as to how this could best be used.

The chapters that follow are structured towards applying the findings of the audit into compliance procedures for different areas such as fair collection notices, contracts when working with data processors, matters for employment contracts and e-mail/Internet monitoring policies. There is a helpful chapter on the various issues a data protection officer may need to consider when liasing with different departments in the company, such as human resources, marketing and IT. Finally, the book contains some helpful precedent materials covering a number of the important source documents the reader will need.

Although the basic premise behind the book is refreshingly simple and different, the structure designed to deliver this concept has had to be quite complex, with the authors making wide use of different forms of cross referencing sections, tables, precedents and explanatory text. This may make the book appear overly formal to the novice non-lawyer. However, non-specialists should not be put off from investing in what is a very practical resource, as in all other respects the content is easy to read and informative. The book maintains a good balance between practicality and process and will get beginners off to a flying start, whilst retaining sufficient depth for practitioners to grow into the subject as their knowledge and experience increases.

Sally Annereau is a Data Protection Analyst in Taylor Wessing's Data Protection and Privacy Group. She may be contacted at s.annereau@taylorwessing.com

   ISSN 1473-3579