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 11 November 2004

Articles

Case Reports

News

News

www.bnai.com

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

Publishing Director: Deborah Hicks
Editorial Director: Joel Kolko

Editor: Nichola Dawson
Production Manager: Nitesh Vaghadia

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

Directive 96/9/EC created a database right, intended to encourage and protect the investment in databases. However, due to lack of definition, the Directive has made it difficult to interpret the actual *level* of protection afforded and has meant that cases have been referred to the ECJ for clarification.

Earlier this year, the Advocate General gave her definition of database rights (as reported in the June issue of *WDPR*) and finally, the ECJ has delivered its own long-awaited judgment - interestingly in contrast to that of the Advocate General. The ruling by the ECJ has in effect, restricted the protection afforded to database rights owners. We are pleased to include a detailed commentary by Edward Vickers of Taylor Wessing on page 6, which analyses the ECJ's findings in detail and what this means for anyone producing or exploiting a database.

As readers responsible for transferring personal data out of the European Union will be aware, such transfer is prohibited by the E.U. Data Protection Directive unless the data is being sent to a destination that provides an adequate level of protection for such information ("adequate", as defined by the Directive). As the United States does not fulfil this criterion, the E.U. Commission adopted a special decision in 2000 to permit such data transfers to the U.S. The method, known as "Safe Harbor" is a voluntary scheme that requires recipients of data to comply with a set of principles and is enforced by the Federal Trade Commission. Four years on, the E.U. Commission has conducted a review of its scheme and published a working document assessing the functioning of Safe Harbor - how successful has it been? Our thanks go to Richard Cumbley of Linklaters for his commentary on page 13.

In the Security & Surveillance section this month, we provide the concluding part to Alessandro del Ninno's two-part commentary on the processing of personal data by means of video surveillance devices in Italy, and look at the "U.K. Freedom of Information Act Exemptions and the Public Interest Test" in the Legislation & Guidance section, as explained by Rachel Fetches and Hazel Grant of Bird & Bird.

Case Reports this month examine the latest decision by the ECJ (confirming the E.U. Commission's view) that E.U. data privacy rules do not prevent operators from providing phone bills listing itemised calls, and the U.K. Advertising Standards Authority's latest adjudication regarding e-mail marketing lists.

Nichola J. Dawson

We wish to thank the following for their contribution to this issue:
Astrid Arnold, Lovells, London; *David Clark,* Bird & Bird, London; *Richard Cumbley,* Linklaters, London; *Hazel Grant* and *Rachel Fetches,* Bird & Bird, London; *Robert H. Jackson,* Reed Smith, Washington D.C.; *William Karam, Arlan Gates* and *Robin Rix,* Baker & McKenzie, Toronto; *John W. Kropf,* U.S. Department of State's Office of the Legal Advisor, *Christopher Kuner,* Hunton & Williams, Brussels; *Marie-Claire McCartney,* Hammonds, London; *Charlotte McConnell,* Bristows, London; *Massimiliano Mostardini* and *Debora Stella,* Bird & Bird, Milan; *Alessandro del Ninno,* Studio Legale Tonucci, Rome; *Victoria Sedgwick* and *Ruth Boardman,* Bird & Bird, London; *Edward Vickers,* Taylor Wessing, London.

Consumer Protection

Case Report

UNITED KINGDOM

ASA Adjudication on Explicit Consent Rules for Use of Bought-in Contact Lists

On October 13, 2004 the Advertising Standards Authority ("ASA") upheld a complaint against an online DVD rental company, illustrating just how careful companies are expected to be when they use e-mail marketing lists from a third party provider.

A division of the Peterborough-based Home Entertainment Corporation, *moviechoice.com*, purchased an e-mail marketing list from a liquidated company under a contract which stated that explicit opt-in consent to receive e-mails from third parties had been obtained from the addressees. Unfortunately, this was not the case and when an individual complained that he had consented to receive electronic communications from the liquidated company but not third parties, *moviechoice.com*'s reliance on the contract with the liquidated company was not accepted as a defence, and the ASA upheld the complaint.

The Complaint

moviechoice.com advertised free DVD rental in an e-mail entitled "30 days FREE DVD rental!". The e-mail stated:

> 1 – SELECT Choose your DVDs from over 18,000 titles …
> 2 – RECEIVE Receive your DVDs by First Class post …
> 3 – WATCH Enjoy your DVDs for as long as you like …
> 4 – RETURN Return free of charge and we'll send you the next one …

The complainant, a Cambridgeshire resident, objected that:

- *moviechoice.com* had not obtained his explicit consent to send him commercial e-mails because although he had consented to receive e-mails from the liquidated company he had not given his consent to the liquidated company to pass on his details to third parties; and
- the e-mail did not give him the opportunity to opt-out of receiving further commercial e-mails from *moviechoice.com*.

In relation to the second point, *moviechoice.com* maintained that it was their standard practice to include an *unsubscribe* facility in their e-mails but admitted that on this occasion that facility had been mistakenly omitted. They stated that this error had now been corrected. The ASA accepted this but upheld the complaint and cautioned *moviechoice.com* to make certain that it was included in future.

The explicit consent issue was dealt with as follows.

The Defence

moviechoice.com provided the ASA with a copy of the contract it had negotiated with the liquidators of the company whose customer e-mail addresses it had purchased. The contract stated that:

> … [*moviechoice.com*] has agreed to buy a customer list … that contains approximately 216,000 email addresses representing all of the active customers (*i.e.*, customers who have made at least one purchase from the Seller within the period of 12 months immediately preceding the date of this Agreement) known to the Liquidators who have given opt-in consent (which has not been withdrawn and is still current at the date of this Agreement) to receive electronic communications from third parties …

The contract had even included the following declarations from the partners in the liquidated company:

> I confirm that the customer database … comprises a list of e-mail addresses of former customers of the company all of whom, to the best of my knowledge and belief, have agreed to receive electronic communications from third parties …

moviechoice.com assured the ASA that their decision to buy the e-mail database had been based on this contractual undertaking that the liquidated company's customers had given opt-in consent to receiving e-mail marketing from third parties, which they had specifically included in the contract to ensure their compliance with the relevant legislation.

The ASA's Decision

The ASA acknowledged that *moviechoice.com* had bought the customer database in good faith and that the contract stated clearly that the customers had given opt-in consent to receiving e-mails from third parties. However, the ASA observed that *moviechoice.com* had not adduced any evidence to show that the complainant (or for that matter any of the other customers of the liquidated company whose e-mail addresses it had bought) had given explicit consent to the liquidated company to pass on their details to third parties. The ASA said that it was the responsibility of any third party purchasing a marketing list to ensure that the first instance permission-holder from whom they are buying the list had been given explicit consent by its customers to pass on their details to third parties. The third party marketer should also be able to provide the ASA with evidence of this explicit opt-in consent upon request.

The ASA therefore accepted the complainant's contention ("contention" because there is no hint in the adjudication that the complainant had any evidence of *not* having provided explicit consent) that he had not given the liquidated company consent to pass on his details to third parties and upheld his complaint that *moviechoice.com* had sent him a commercial marketing e-mail without having obtained his explicit consent.

The specific sections of the CAP Code which *moviechoice.com* was held to have breached are sections 43.4c and 43.5, which provide that:

> **43.4c** The explicit consent of consumers is required before …sending marketing communications by e-mail or to mobile devices, save that marketers may send unsolicited

marketing about their similar products to those whose details they have obtained in the course of, or in negotiations for, a sale. They should, however, tell them they may opt-out of future marketing both when they collect the data and on each occasion they send out marketing communications and should give them a simple means to do so. Explicit consent is not required when marketing business products to corporate subscribers (see 1.3j), including to their named employees

43.5 If after collection it is decided to use personal information for a purpose significantly different from that originally communicated, marketers should first get the explicit consent of consumers. Significantly different purposes include:

(a) the disclosure of personal information to third parties for direct marketing purposes

(b) the use or disclosure of personal information for any purpose substantially different from that which consumers could reasonably have foreseen and to which they might have objected.

The ASA instructed *moviechoice.com* to acquire evidence-based explicit consent before sending commercial e-mails in future.

What Does this Mean in Practice?

moviechoice.com was not fined or penalised directly (though the instruction to acquire evidence of explicit opt-in consent for third party marketing means that *moviechoice.com* is presumably prevented from using any of the approximately 216,000 other customer addresses it had bought from the now defunct company). It is important to note that this was dealt with as a breach of the CAP Code, not as a breach of the Privacy and Electronic Communications Regulations 2003.

However, its reputation has not been improved by the adverse publicity and the response to that segment of its marketing campaign which was based on the liquidated company's customer list may have been poor, since it is likely that the complainant was not the only recipient who had not provided explicit opt-in consent.

More broadly, this ruling makes it very clear that the ultimate responsibility for ensuring that explicit opt-in consent has been obtained lies absolutely with the marketer, and this means that marketers buying in address lists of contacts to whom they wish to market can no longer accept the word of list brokers at face value. A paper trail to prove consent is required, and list warranties – though commercially essential - are clearly not enough. A list purchaser should probably seek examples of the wording that was used to obtain the consent, and great caution should be exercised with entities who are unlikely to be able to make good on the contractual warranties they have provided.

Finally, and uncontroversially, marketers should always ensure that an *unsubscribe* facility is included in their marketing e-mails.

By David Clark, Bird & Bird, London. The author may be contacted at David.Clark@twobirds.com

E-Commerce

E-Contracting in Italy

By Massimiliano Mostardini and Debora Stella, Bird & Bird, Milan. The authors may be contacted at +39 02 3035 6000 or massimiliano.mostardini@twobirds.com, debora.stella@twobirds.com

The execution of contracts through electronic devices represents a current issue that offers new marketing opportunities. This article looks at how this might be achieved by means of SMS and MMS, taking into consideration the applicable law and the possible technical limits of this type of operation.

Applicable Law

If it is in the interest of a service or goods provider to enter into supply or service agreements through electronic means under Italian laws, this should be evaluated against the relevant applicable legislation and, in particular, the Italian legislation on distance selling (Legislative Decree May 22, 1999, n. 185, which enforced the E.U. Directive 97/7/CE), the legislation on e-commerce (Legislative Decree April 9, 2003, n. 70, implementing the E.U. Directive 2000/31/EC) and the legislation on data protection (Legislative Decree June 30, 2003 n. 196, implementing in particular, E.U. Directive 95/46/CE and E.U. Directive 2002/58/CE).

Data Protection Issues

Pursuant to Article 130 of the Italian data protection law before any commercial proposal is sent via electronic means, and in particular via SMS or MMS, the informed consent of the recipient must be obtained. This implies that the recipient should have also received from either the provider of the goods or services or the direct marketer, information required by the Italian data protection law to be given in relation to data processing.

Contractual Issues

Pursuant to the legislation on distance selling and e-commerce, in addition to the information concerning the data processing, the provider (or the direct marketer) is required at the same time to provide the consumer with a clear communication highlighting, *inter alia*:

- that the communication is a commercial communication;

  WDPR ISSN 1473-3579

- the subject on behalf of whom the commercial communication is done; and
- that the recipient may refuse at any time any further commercial communication.

In additional to the above information which has to be given to the recipient, before execution of the contract with the consumer, the provider (or the direct marketer) has to provide the consumer/recipient with the following essential information:

- the identity and address of the provider (or the direct marketer);
- the main features of the good/service;
- the price of the good/service, including applicable taxes;
- the payment and modalities for the supply of the service or of the delivery of the goods;
- the termination right or exclusion of the termination right;
- the cost of communication between the provider and the consumer if different from the ordinary tariffs;
- the duration of the offer;
- the minimum duration of the contract; and
- the address at which to notify claims related to the good/service.

This information, as well as the contract terms and conditions, must be provided or made available to the recipient in a way which allows the recipient to store and reproduce it (the so-called "durable means" requirement).

The information requirements set out above are mandatory and neither the provider (or the direct marketer) nor the consumer can agree on any exemption or derogation therefrom.

Contracts Executed by Means of SMS and MMS Messages

In addition to the above, it should be noted that the execution of contracts by means of SMS and MMS messages raises some technical problems related to the full compliance of such operations with the requirements of law.

Technical Issues: Complete Information and Durable Mean

It is clear that compliance with the requirements for complete information on data processing and on the content of the contractual proposal may result in difficulties when the contract between the provider (or the direct marketer) and the consumer/recipient is restricted to electronic means such as SMS or MMS, which for their own feature consist in short/small files.

In addition, and assuming that complete information to the consumer/recipient is feasible via SMS or MMS, it should be noted that the provider (or the direct marketer) is also required to provide the consumer, before (or at the time of) execution of the contract, with information concerning the contract *in writing or on a "durable mean"*: the provider will have to manage with the additional hindrance relating to the consumer's right to obtain all the above information on a durable means which is usually unavailable to the major handsets (without GPRS or "blue tooth" devices).

Therefore, technical reasons (connected to the possibility of having all necessary information displayed and readable by the consumer, as well as properly amended by the latter, if required) will likely bar this innovative marketing operation, for the time being at least.

Vexatious Clauses

Another practical issue to consider in relation to execution of contracts via SMS – and within the limit of their validity in the case of the consumer – is the explicit and specific acceptance by the recipient of the so called "vexation clauses" (*e.g.*, clauses providing for the limitation of liability, the withdrawal, *etc*.)[1] included in the providers standard terms and conditions of the service/supply.

According to Italian law, these types of clauses are null and void unless specifically accepted in writing by the party adhering to them (*i.e.,* the consumer/recipient[2]). It is also evident that, in the absence of specific electronic means ensuring the validity of a written declaration from the recipient via SMS/MMS, the contract would not be properly executed since the vexation clauses could not be duly accepted by the recipient via SMS or MMS messages.

In the light of the foregoing, and assuming that the provider would not easily be able to provide all the aforementioned information via a simple SMS or MMS message, it will be necessary at least to direct the recipient/consumer to a website displaying all the information, as well as the terms and conditions of the service/supply in a readily printable format.

1 According to section 1341 of the Italian Civil Code, the "standard conditions prepared by one of the parties are effective as to the other, if at the time of formation of the contract the latter knew of them or should have known them by using the ordinary diligence". These clauses refer to limitations on liability, the power of withdrawing from the contract, or of suspending its performance, or which impose time limits involving forfeitures on the other party, limitations on the power to raise defences, restrictions on contractual freedom in relations with third parties, tacit extension or renewal of the contract, arbitration clauses, or derogations from the competence of courts, *etc*.

2 Please consider that according to section 1469-bis of the Italian civil Code some clauses (*e.g.*, those listed under section 1469-bis which implemented the E.U. Directive 93/13) are null and void notwithstanding the consumer agreed to them.

Intellectual Property

The ECJ Restricts Protection Afforded to Database Rights Owners

By Edward Vickers, Taylor Wessing, London. The author may be contacted by e-mail at: e.vickers@taylorwessing.com

The European Court of Justice ("ECJ") has handed down its decision in four linked cases,[1] concerning two types of sport-related database – a database of football fixtures and a database of horse races and related runners and riders. The first three cases concerned the database of football fixtures (and dealt with much the same issues) and the fourth concerned the database of horse races (and dealt with different issues). (*See also*, "Database Rights Defined: The Advocate General's Opinion", *WDPR* (June 2004)).

The decision is particularly important for anyone responsible for creating, maintaining or exploiting a database, as it relates to the extent that the database can be protected against unauthorised use or reproduction by someone else. In other words, the decision is relevant to the ability to obtain revenue (and a return on the investment involved in creating a database) by licensing the use of the database, or of data from the database.

What is a "Database"?

In 1996, an EC Directive[2] was published, the aim of which was to harmonise across all of the countries in the European Union the extent to which intellectual property rights existed in databases and, therefore, the extent to which databases were protected against unauthorised copying or exploitation. Before the directive, the way in which intellectual property rights applied to databases was different from country to country. In particular, some countries protected databases using copyright, while others did not (or did not do so to the same extent). This caused potential difficulties with the exploitation of a database on a pan-European basis.

The directive defines a database like this:

> "…a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means".

How are Databases Protected under the Directive?

The directive sets up two ways in which a database can be protected. First, some databases will qualify for protection as copyright works. Secondly, there is a special "database right" which protects databases in some cases even if they do not qualify for copyright protection.

Copyright Protection of a Database

In order to be protected by copyright, a given database has to be one which:

> "…by reason of the selection or arrangement of its contents, constitutes the author's own intellectual creation".

Note that the "intellectual creation" factor relates to the *selection* or the *arrangement* of the contents, *not* to the *creation* of the contents. So, for example, if a lot of creativity goes into the creation of the contents of the database (*i.e.*, of the data that populates the database), but the data is arranged in a very simple way, then the database as a whole will not qualify for copyright protection (although that may not stop the individual items of content being protected by copyright).

Take the example of a list of names and addresses. This may well be a database. However, there is not much "intellectual creation" involved in arranging the names in alphabetical order so this type of database may not qualify for copyright protection.

To take an opposing example, you might have a database composed of relatively simple items of data but where the data is selected and arranged in a special way so as to make the whole collection particularly original in terms of its organisation. If the data that has been selected, or the way it is arranged, do constitute an original "intellectual creation" by the author of the database, then the database will be protected by copyright. This may, in many cases, be quite difficult to show, so copyright protection may be difficult to claim for many types of database.

So, what happens (for example) where the data in a database is selected and arranged in a straightforward way? Is there any protection for the database in that case?

Database Right

This is where the special right – "database right" – comes in. Database right will exist in a database where, when looked at in terms of quantity or quality, there has been a substantial investment in the:

- obtaining;
- verification; or
- presentation;
- of the contents of the database.

Just because someone has spent a lot of time, effort and money obtaining, checking or presenting the data in a database, does not mean that the way that the data has been selected or arranged is original or clever enough to qualify as an "intellectual creation". It is possible therefore, to have database right where copyright does not exist in a database.

There have been a number of difficulties in interpreting exactly how database right works in practice, and it was with some of these difficulties that the decision of the European Court of Justice was concerned. That decision is likely to have some

  WDPR ISSN 1473-3579

far-reaching effects on the extent to which database right can be used to protect certain types of database. In order to explain why, we need to look at each of the two groups of cases in turn.

Football Fixtures

The basic facts of this set of cases were as follows:

- Each of the Football Leagues in England and Scotland contracted with a company, Football Fixtures Limited, to handle the exploitation of each of their fixture lists outside the United Kingdom via a licensing scheme. Football Fixtures was given the right to represent the holders of the intellectual property rights in the fixture lists (*i.e.*, the Football League).
- Three companies in (respectively) Finland, Sweden and Greece used the Football League fixture lists without a licence for the purposes of their gambling business. Each of them was sued for infringement of (among other things) the Football League's database rights in its database of football fixtures.
- The various national courts in Finland, Sweden and Greece all raised questions which they referred to the European Court of Justice regarding the interpretation of the rules governing database rights as they applied to a database of football fixtures. The European Court of Justice dealt with all three cases at once and made a number of interesting points.

Is the List of Football Fixtures a "Database"?

The first question the ECJ looked at was whether or not the list of football fixtures was a database in the first place. On that question, it said:

- It was the intention of the directive to give the term "database" a wide scope, without getting into complicated considerations (for example, of a technical nature) in order to try to define it. The directive said that it covered the legal protection of databases "in any form". The directive covered non-electronic as well as electronic databases.
- The fact that the data or information in the database relate to a sporting activity did not stop the database from being recognised as such under the directive.
- In order for something to be a database, it must fulfil the following criteria:
  - It must be a collection of "independent" materials – that is, materials which can be separated from one another without their informative, literary, artistic, musical or other value being affected.
  - The independent materials making up the collection must be systematically or methodically arranged and individually accessible in one way or another. It is not necessary for the systematic or methodical arrangement to be physically apparent.
  - The collection should be contained in a fixed base of some sort and include technical means (such as a process driven by software), or some other means, such as an index, a table of contents, or a particular plan or method of classification, to allow the retrieval of any independent material contained within the collection.
- The date and the time of and the identity of the two teams playing in home and away matches count as "independent materials". Although the main interest of a football league lies in the overall result of the various matches, it is still the case that the data concerning the date, the time and the identity of the teams in a particular match have an independent value in that they provide interested third parties with relevant information.
- The collection, in the form of a fixture list, of the dates, times and names of teams in the various football matches involved systematic or methodical arrangement and individual accessibility of the constituent materials of the collection. The fact that lots are drawn to decide the pairing of the teams does not make a difference.
- As a result, a fixture list for a football league such as in this case constituted a database within the meaning of the directive.

To What Extent did Database Right Protect a List of Football Fixtures?

Having established that the list of football fixtures was a database within the meaning of the directive, the ECJ next had to decide whether or not the database qualified for protection under database right. In relation to that point, it had the following to say:

- Database right only applies to databases that meet specific criteria, that is, it only applies to databases in relation to which there has been (qualitatively and/or quantitatively) a substantial investment in the *obtaining*, *verification* or *presentation* of the contents of the database.

The criterion of *substantial investment* in the *obtaining* of the content of the database refers to the resources used to *find* existing independent materials and to *collect* them in the database, and *not* to the resources used for the *creation* of those independent materials.

In other words, no matter how much investment went into the creation of the materials that are included in the database, it is not that investment that is relevant. *Obtaining* the content of the database does not include *creating* that content. What is important is the amount of investment that goes into *collecting* the materials (once they have been created) and *arranging* them in the database. The resources used in creating the material that is to be included in the database *cannot* be taken into account in assessing whether or not the investment in the creation of the database was substantial.

- Investment in the *verification* of the contents of a database refers to the resources used:
  - to ensure the reliability of the information contained in the database; and
  - to monitor the accuracy of the materials collected when the database was created and during its operation.
- Investment in the *presentation* of the contents of the database refers to the resources used:
  - to arrange the materials contained in the database (in a systematic or methodical way); and

- to organise the database so that the materials are individually accessible.

- *Investment* may involve human, financial or technical resources. It has to be substantial in terms of *quantity* or *quality*. So, for example, it must involve a sufficient quantity of money or time or a lot of intellectual effort.
- It does not matter if the person who creates the database is also the person who creates the materials that are contained in the database, provided that as well as any investment in the creation of the material, there is also a substantial investment in obtaining, verifying or presenting the materials. As mentioned, the investment in creating the materials in the first place does not count in deciding whether or not there has been sufficient investment to allow the database to be protected by database right.
- In arranging the football league fixtures, the various Football Leagues invested time and effort in establishing the dates and times of and home and away teams playing in the various matches. However, this investment relates to the creation of the data contained in the database (*i.e.*, it involves the creation of the data relating to each match in the various leagues). Therefore, this investment cannot count in deciding whether or not database right protects the database of football fixtures.
- Finding and collecting the data making up a football fixture list does not require any particular effort on the part of the Football League. Putting together the football fixture list thus does not require any investment over and above that required for the creation of the data contained in that list in the first place. Likewise, no particular effort is required to monitor the accuracy of the data on league matches when the list is made up. The verification of the accuracy of the contents of fixture lists during the season only involves adapting some of the lists to take account of any postponement of a match. This does not amount to substantial investment. Lastly, there is no particular effort involved in presenting a football fixture list once the fixtures have been decided upon, so that does not require substantial investment either.
- As a result, because all of the investment in producing a football fixture list goes into the creation of the data to go into the list, rather than the assembling of the data into a list, the checking of the list or the presentation of the list, database right does not protect a football fixture list.

Before going on to consider the conclusions to be drawn from these cases, it is worth turning to the horse racing case, as it reinforces certain aspects of the decision in the football fixtures cases.

BHB v. William Hill

This case involved some of the same issues as the football fixture cases. There was an additional issue, which was the extent to which people were allowed to re-use contents of the database before they infringed the database right.

What Database Right Prevents

If database right exists, then the owner of the database right has a right to control:

- *extraction*; and/or
- *re-utilisation*;

of *all or a substantial part of the content* of that database. When deciding whether a *substantial part* has been extracted or re-used, this must be considered both in terms of *quantity* (how much of the data been used as against the whole) and in terms of *quality* (how valuable is the data that has been used as against the whole).

For these purposes:

- *extraction* means the permanent or temporary transfer of all or a substantial part of the contents of the database to another medium by any means or in any form; and
- *re-utilisation* means any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by online or other forms of transmission.

In addition to that, *repeated* and *systematic* extraction and/or re-utilisation of *insubstantial* parts of the contents of the database so as to:

- conflict with a normal exploitation of the database; or
- unreasonably prejudice the legitimate interests of the maker of the database;

is also controlled by the owner of the database right.

The Facts in *BHB v. William Hill*

The basic facts were as follows:

- The case concerned the British Horseracing Board, which manages the horse racing industry in the United Kingdom. It compiles and maintains a database that contains a lot of information supplied by horse owners, trainers, horse race organisers and others involved in the racing industry. The database contains information on (among other things) the pedigrees of about one million horses, and "prerace information" on races to be held in the United Kingdom. That information includes the name, place and date of the race concerned, the distance over which the race is to be run, the criteria for eligibility to enter the race, the date by which entries must be received, the entry fee payable and the amount of money the racecourse is to contribute to the prize money for the race.
- Three main functions are performed leading up to the issue of pre-race information:
  - Registration of information concerning owners, trainers, jockeys and horses and records of the performances of those horses in each race.
  - Decisions on weight adding and handicapping for the horses entered for the various races.
  - Compilation of the lists of horses running in the races. This activity is carried out via a call centre manned by about 30 operators. They record telephone calls entering horses in each race organised. The identity and status of the person entering the horse and whether the characteristics of the horse meet the criteria for entry to the race are then checked. Following those checks the entries are published provisionally. To take part in the race, the trainer must

confirm the horse's participation by telephone by declaring it the day before the race at the latest. The operators must then ascertain whether the horse can be authorised to run the race in the light of the number of declarations already recorded. A central computer then allocates a number to each horse and determines the stall from which it will start. The final list of runners is published the day before the race.

- The cost of running the BHB database is approximately £4 million per annum. The fees charged to third parties for the use of the information in the database cover about a quarter of that amount.
- The database is accessible on the website operated by the BHB. Some of its contents are also published each week in the BHB's official journal. The contents of the database, or of parts of it, are also made available to Racing Pages Ltd, which then forwards data to its various subscribers, including some bookmakers, in the form of a "Declarations Feed", the day before a race.
- Satellite Information Services Limited ("SIS") is authorised by Racing Pages to transmit data to its own subscribers in the form of a "raw data feed" ("RDF"). The RDF includes a large amount of information, in particular, the names of the horses running in the races, the names of the jockeys, the numbers and the weight for each horse. Through the newspapers and the Ceefax and Teletext services, the names of the runners in a particular race are made available to the public during the course of the afternoon before the race.
- William Hill, which is a subscriber to both the Declarations Feed and the RDF, provides offcourse bookmaking services in the United Kingdom to both U.K. and international customers. It launched an online betting service on two websites. Those interested can use these sites to find out what horses are running in which races at which racecourses and what odds are offered by William Hill. The information displayed on William Hill's websites is obtained, first, from newspapers published the day before the race and, second, from the RDF supplied by SIS on the morning of the race.
- The information displayed on William Hill's Internet sites represents a very small proportion of the total amount of data on the BHB database, given that it concerns only the following matters: the names of all the horses in the race, the date, time and/or name of the race and the name of the racecourse where the race will be held. Also according to the order for reference, the horse races and the lists of runners are not arranged on William Hill's websites in the same way as in the BHB database.

The BHB brought proceedings against William Hill in the High Court of Justice in England alleging infringement of the database right in the BHB database. They argued:

- that each day's use by William Hill of racing data taken from the newspapers or the RDF was an extraction or re-utilisation of a substantial part of the contents of the BHB database; and
- that even if the individual extracts made by William Hill are not substantial they should be prohibited because they were repeated and systematic extraction of insubstantial parts of the database that prejudiced their exploitation of the database.

Decision of the ECJ

The High Court referred a number of questions to the European Court of Justice, which took the following view of the case:

- Investment in the selection, for the purpose of organising horse racing, of the horses admitted to run in the race concerned relates to the *creation* of the data that makes up the lists for those races that appear in the BHB database. It does not amount to investment in *obtaining* the contents of the database (see comments on the football fixtures decision, above).
- The process of entering a horse on a list for a race required a number of prior checks as to the identity of the person making the entry, the characteristics of the horse and the classification of the horse, its owner and the jockey. However, such prior checks are made at the stage of *creating* the list for the race in question. They therefore also amount to investment in the *creation* of the content of the database and not in the *verification* of that content.
- It follows that the resources used to draw up a list of horses in a race and to carry out checks in that connection do not represent investment in the obtaining and verification of the contents of the database in which that list appears.
- In looking at an alleged act of extraction or re-utilisation of a protected database, it did not matter exactly what the purpose was of the extraction or re-utilisation, provided it caused significant detriment to the investment that had been made in the database. It was not relevant therefore, what use the person extracting or re-utilising the data put the data to, exactly. The fact that the data was not being used, for example, to create a competing database did not matter, provided there was still some significant detriment to the database owner's investment.

Extracting and re-utilisation must therefore, be treated as meaning any act of appropriating and making available to the public, without the consent of the maker of the database, the results of his investment, thus depriving him of revenue which should have enabled him to recoup the cost of the investment. Clearly, the terms are interpreted very widely.

- William Hill carried out acts of extraction and re-utilisation within the meaning of the directive. It extracted data from the database by transferring the data from one medium to another. It integrated the data into its own electronic system. It re-utilised the data by making the data available to the public on its own website in order to allow its clients to bet on horse races.
- However, that was not the end of the issue. The ECJ also said that the materials displayed on William Hill's websites, which were derived from the BHB database:
  - represented only a very small proportion of the whole of that database. It therefore appeared those materials did not constitute a substantial part (in terms of *quantity*) of the contents of that database; and

- concerned only the following aspects of the BHB database: the names of all the horses running in the race concerned, the date, the time and/or the name of the race and the name of the racecourse. In order to decide whether those materials represented a substantial part (in terms of *quality*) of the contents of the BHB database, it was important to consider whether the human, technical and financial efforts put in by the maker of the database in *obtaining*, *verifying* and *presenting* the data that was being extracted or re-utilised constituted a substantial investment. As already mentioned, the resources used for the *creation* of the materials concerned cannot be taken into account. The resources employed by BHB to establish, for the purposes of organising horse races, the date, the time, the place and/or name of the race, and the horses running in it, represent an investment in the *creation* of materials contained in the BHB database. As a result, because those were the only materials extracted and re-utilised by William Hill, that did not involve the extraction or re-utilisation of a substantial part (in terms of *quality*) of the BHB database.

Overall Result

The most important point to come out of these cases is that the investment put into creating material to be included in a database, does not count in deciding whether or not that database is protected by database right. All that matters is the investment (if any) in *obtaining* the content, *verifying* the content and, finally, *presenting* the content.

This may cause a significant problem for many people that exploit databases. In particular, it will cause a problem in relation to a database that might have quite sophisticated content but where obtaining, verifying and presenting the content involved very little work, over and above that required to create the database. The ECJ made a rather artificial distinction here, in that it said (in effect) that if obtaining the data, verifying it and presenting it all formed part of creating the data in the first place, then none of the investment in doing this would count in deciding whether or not database right would apply to the completed database.

With many databases, it is very difficult to separate out the "creation" of the content from the obtaining, verification and presentation of that content. If a single business sets out to create a database, unless it is obtaining the data to be included from somewhere else, the processes involved in creating, obtaining, checking and presenting the data will all be part of a single process/part of one organic process?. On the basis of the ECJ's reasoning, that will disqualify the database from protection under database right. According to the ECJ, in order for the database to be protected by database right, it will have to be possible to separate the process of creating the data in the first place from a subsequent process of obtaining, verifying or presenting the data and you will have to show that a separate, substantial investment went into the subsequent process as well as the first.

The horse racing case illustrates this quite starkly. The ECJ agreed that substantial effort had gone into (among other things) verifying the data relating to the horse races. However, the ECJ said that because this process of verification was part of the creation of the data in the first place, it did not count in deciding whether or not there had been any substantial investment in the database so as to qualify it for protection.

Thus if obtaining the content, arranging it in the right way, checking it and presenting it to the user do not require much work of themselves and are separate from creating the content in the first place, it will be arguable that the database is not the subject of database right.

On this basis, it is difficult to see what type of database *would* qualify for protection under database right. If the creation process of most databases (as noted above) is analysed, there is often a single process that involves creation of the data, its verification and presentation, and it may be difficult (if not impossible) to separate them out/make these appear distinct?. It is hard to see in what circumstances obtaining, verification and presentation of the data would be separate from the creation of the data for use in the database. In short, although it may be too early to tell and specific analysis of particular types of database may be required, the ECJ may have effectively neutered database right as an effective form of protection. In doing so, it may have removed the ability of a number of businesses to make a return on the investment they have put into creating a given database. This is underlined by the reports in the press about the extent to which the decision might affect the future of the BHB, if it is deprived of the income from exploiting the database of runners and riders.

If the selection or arrangement of the content in the database is not particularly original, then copyright will not protect the database either.

In that case, the only remaining line of protection is likely to be any intellectual property rights that subsist in the content itself. Sophisticated content (such as sound recordings, literary works and pictures) is likely to be protected by copyright in its own right. This may help the owner of the database to control use of the content of the database, provided that he owns the intellectual property rights in that content. However, this is not always the case. For example, someone may have assembled a database using data obtained from third parties (the intellectual property rights in which data are owned by third parties). If the person who creates the database has no rights in the content, then whether or not there is any independent copyright or database right in the database itself will be very important. Without it, the creator of the database may be unable to control the use of the database that, in turn, means that he may be unable to exploit the database to make money so as to repay the investment in creating it.

If the data itself is simple enough not to attract copyright protection in its own right, then this may introduce a further problem. A name and addresses is somewhat difficult to protect as a copyright work. Consequently, an alphabetical list of names and addresses may be difficult to protect at all *unless* sufficient investment had to be made in obtaining the relevant names and addresses in the first place to qualify the collection for protection by database right. Even then, if that investment can be regarded as part of the "creation" of the data, then database right protection may not apply either.

To cap this, the ECJ also established that extraction or re-utilisation of any part of the database in relation to which there had not been substantial investment so as to

qualify that part of the database for protection, could not be treated as extraction or re-utilisation of a substantial part of the database. The position may have been different if the data being used by William Hill constituted a large part (in terms of quantity) of the database when measured against the database as a whole, but that was not the case here as only a very small proportion of the data was being reused.

In effect, the ECJ also suggests that even if the database as a whole does attract protection, extraction of re-utilisation of any of the contents will only be prohibited if:

- it is of a substantial quantity of the data in the database (measured against the quantity of data in the database as a whole); or
- it is of particular data in relation to which the owner can show there has been substantial investment in the organisation, verification or presentation of the data concerned.

Otherwise, even if the data has some considerable commercial importance (as in this case), its extraction or re-utilisation will not be prevented.

Conclusion

This decision of the ECJ shifts the goalposts in relation to protection of databases. It restricts the extent to which database right can be claimed to protect databases and it may make a number of databases that are currently being commercially exploited somewhat more difficult to protect (and therefore to exploit).

It is difficult to generalise about the exact effect the decision will have, but what is clear is that anyone producing or exploiting a database will need to look carefully at the investment that went into creating it, in order to decide to what extent it is now protected by database right or copyright. The rather artificial distinction between "creation" of data for a database on the one hand, and "obtaining, verifying and presenting" the data on the other, may introduce a hurdle that the owners of at least some types of database may find difficult to clear/overcome?

1 *Fixtures Marketing Ltd v. Oy Veikkaus AB*, Case C-46/02.
Fixtures Marketing Ltd v. Svenska Spel AB, Case C-338/02.
Fixtures Marketing Ltd v. OPAP, Case C-444/02.
British Horseracing Board v. William Hill Organisation Ltd, Case C-203/02.

2 Directive 96/9/EC.

Legislation & Guidance

European Union: Report on the Implementation of Safe Harbor

By Richard Cumbley, a Managing Associate with the ITC Group of Linklaters, London. The author may be contacted by e-mail at richard.cumbley@linklaters.com

The E.U. Commission has just published a "Staff Working Document"[1] assessing the functioning of the U.S. Safe Harbor scheme. The document, which follows a similar report two years ago, looks at two things: firstly, trends in the level of compliance of U.S. organisations with the Safe Harbor Principles and Frequently Asked Questions ("FAQs"); secondly, the extent to which the bodies responsible for enforcing the Principles and FAQs are carrying out their functions and how they could improve.

What is the Safe Harbor?

As most readers will be aware, the E.U. Data Protection Directive 95/46 prohibits the transfer of personal information outside of the EEA, unless it is being sent to a destination which provides an adequate level of protection to such information. The United States does not fulfil those criteria, so that transfers of personal information from the European Union to the United States can only take place if one of the exceptions provided for under the Directive can be established. These exceptions, such as the use of consent of the subject of the information or a standard form European Commission approved "model contract", are often considered cumbersome and unwieldy. On July 26, 2000, the E.U. Commission adopted a decision[2] recognising an alternative method of transferring personal data to the United States in a legitimate way. That method, known as the "Safe Harbor", requires recipients to agree to comply with a set of principles, and more detailed standards set out in the FAQs.[3] The scheme is voluntary, and enforced ultimately by the Federal Trade Commission ("FTC"), but breach of the principles and FAQs can carry significant administrative and civil sanctions.

Scale of the Safe Harbor Scheme

When the analysis for the Staff Working Document was carried out (in November 2003), the Safe Harbor had just over 400 members, which at the time of writing, had increased to 614 members. In the document, the Commission state that they are pleased the number of registrants is constantly increasing, but it would like to see the membership of the scheme increase further. Ironically, part of the rationale of publishing the staff working document is to increase the awareness of the Safe Harbor program and thereby encourage the take up of the scheme

by U.S. organisations. It will be interesting to see if the already increased rate of sign up improves further after the document's publication.

Commission Comments on Participants' Involvement in the Safe Harbor

The Staff Working Document outlines the concern of the Commission that many self-certified organisations have failed to adhere to the Safe Harbor Principles. For example, one such principle requires that Safe Harbor organisations publicly state what they do with personal information, by means of a privacy statement. Some organisations, apparently, have no privacy statement at all stating their compliance with the Safe Harbor Principles whilst others have privacy statements that are only partly compliant with them. Similarly, under the principle of choice, organisations must provide individuals with the possibility to opt out of disclosure of their personal data to third parties. However the Commission has noted some of the companies signed up to the Safe Harbor do not give individuals the choice at all, whilst others do so in an unclear manner.

The Commission is particularly concerned with such practices, not only because it is mandatory for scheme participants to adhere to the Principles, but also because the basis of the FTC's jurisdiction to enforce the Safe Harbor is using unfair and deceptive trade practice law in the United States. Fewer public statements about Safe Harbor compliance (by not publishing a privacy policy) make those claims harder to bring. As a result, the Commission recommends that the Department of Commerce ("DoC") (which handles the Safe Harbor applications process), endeavours to "ensure that organisations that self-certify to the [Safe Harbor Principles] have a privacy policy publicly available *before* putting these companies on the Safe Harbor list". This reflects a persistent criticism of the Safe Harbor scheme that self-certification with the DoC is an easy hurdle, taken lightly by many applicants to the scheme.

Commission Comments on U.S. Regulator's Involvement in the Safe Harbor

The Commission's comments on enforcement fall into three broad areas. Firstly, the Commission would like the FTC to be more pro-active in enforcing the Safe Harbor principles, inviting them to undertake "*sua sponte* investigations", in a way that they have not done to date.

Secondly, the Commission is concerned that the FTC may not have jurisdictional "competence to enforce the Safe Harbor principles regarding human resources data". HR data has been something of a running sore for the Safe Harbor; the FAQs require those bodies submitting HR data to the Safe Harbor to submit disputes to an ADR panel operated by the European data privacy regulators. The threat of what that panel might do, and who it might comprise, has been a major disincentive for many organisations signing up to the Safe Harbor scheme for HR data. Perhaps as a result, no disputes have yet been heard by that panel. The private sector is, as a result, locked into a rather unhealthy spiral: relatively few organisations put HR data into the Safe Harbor because of fear about the operation of the dispute resolution panel; no disputes are heard by that panel; nothing exists to dispel the fear; few organisations put HR data into the Safe Harbor. It will only be when a body of cases have been heard by that panel, and it becomes clear what approach it will take, that this spiral will be broken.

Thirdly, the Commission is critical of a number of the other ADR mechanisms individuals can use to enforce their rights under the Safe Harbor. A number of commercial organisations offer their services as ADR for complaints under the Safe Harbor – including TRUSTe and the American Arbitration Association. The Safe Harbor principles require these ADR mechanisms to fulfil a number of principles, and it appears that a number of schemes are not currently doing so. Most importantly, the Commission is critical of a lack of transparency, both in telling individuals how complaints can be made, and in publishing the decisions reached in complaints cases.

Conclusions

Whilst the Document is critical of the implementation of the Safe Harbor scheme in many respects, this is a much more positive report in tone and content than the previous review of the Safe Harbor conducted in 2002. Certainly there is no indication that the Safe Harbor decision will be revoked. That news is welcome, but the continued focus of the European Commission on HR data in particular, is unlikely to provide comfort to those organisations wrestling with the potential risks of placing HR data in the Safe Harbor.

1 *http://eusafeharborreport.notlong.com*

2 520/2000/EC.

3 The Safe Harbor principles and FAQs can be found at *www.export.gov/safeharbor*.

  WDPR ISSN 1473-3579

United Kingdom: A Summary of the ICO's Guidance on PEC in 2004

By David Clark, Bird & Bird, London. The author may be contacted at david.clark@twobirds.com

The Information Commissioner's Office ("ICO") updated its guidance on the U.K. implementation of the Electronic Communications Privacy Directive (the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PEC Regulations")) in May 2004.

The update was necessitated by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2004 ("Amendment Regulations"), which allow corporate subscribers to register with the Telephone Preference Service ("TPS") from June 25, 2004.

The update also clarifies and expands other sections of the Part 1 guidance (*Marketing by Electronic Means*).

Telephone Marketing

Under the PEC Regulations, which came into force on December 11, 2003, corporate subscribers have an enforceable right to opt-out of receiving marketing calls which they can exercise by asking the marketer to cease calling particular numbers. The Amendment Regulations confer on corporate subscribers the further right, which individual subscribers already have, of registering with the TPS. Corporate subscribers need to register in writing (to prevent bogus or unauthorised registration), and although registration is free it must be renewed annually. It is not sufficient to register the organisation as a whole, each direct dial number must be registered.

Marketers who:

- conduct B2B telesales to existing contacts to whom they have not made a sale need to screen their numbers against the TPS;
- have been asked to call (for example, with a quote) by a corporate employee who has registered his/her number with the TPS, may do so, as this is a *solicited* call – the TPS only prevents *unsolicited* calls.

Where an employee gives consent on behalf of their employer, marketers can take the employee's authority to do so on good faith unless they have reason to believe otherwise (though marketers should still take a note of the employee's name and the date the authorisation was given).

There is no exemption for not-for-profit organisations such as charities and political parties, who will also have to screen against the TPS.

Valid Addresses

The PEC Regulations require unsolicited e-mails to include a valid address. This requirement also applies to SMS messages. The ICO now accepts that short code numbers in a SMS text message are "valid addresses" as long as the recipient's use of them to instruct the marketer to cease marketing does not incur premium rate charges. Previously e-mail or postal suppression addresses were required in each SMS message. The ICO now suggests the following format can be used:

"PJLtd2STOPMSGTXT'STOP'TO (then add 5 digit short code)"

Mailing Lists

The ICO warns that the latitude it has shown in the use of electronic mailing lists compiled before December 11, 2003 is coming to an end.

Own Lists

From the first anniversary of the PEC Regulations coming into force (December 11, 2004) the ICO is likely to become stricter on an organisation's use of electronic mailing lists it compiled before December 11, 2003, *i.e.*, lists must have been compiled on a strict prior consent basis from that point or must satisfy all of the "soft opt-in" criteria. However, it seems that the ICO will still allow marketers to carry on using lists which do not meet these criteria if the lists were lawful before the PEC legislation if they are used regularly, updated and weeded appropriately, and always accompanied by opt-out reminders.

Third Party Lists

The use of third party electronic mailing lists bought or rented from a third party after December 11, 2003, will only be legitimate if they are compiled on an *express consent* basis i.e. where the third party has obtained express consent from individual subscribers to pass on their details to other organisations for marketing purposes. Unlike an organisation's own mailing lists, third party mailing lists compiled after December 11, 2003 are unlikely to satisfy the soft-opt in criteria.

Several sets of example wording have been added to the guidance.

The guidance also states that mailing lists of named individuals will continue to be caught by the DPA after *Durant*.

New Sections

The ICO have added some new sections to the guidance, including:

Viral Marketing

This is a process – often incentivised – where a marketer asks someone to pass on a marketing message to friends or to pass over their friends' contact details to marketers. The ICO disapproves and the guidance makes it clear that this will not get around the prior consent rule.

E-Mail Tracking

This involves marketers adding tracking devices to their marketing e-mails to help them work out how successful their marketing campaigns have been. The recipient must be told such devices are being used and how to turn them off.

See also, "United Kingdom: Scope of the Data Protection Directive is Narrowed", *WDPR* (January 2004); and "United Kingdom: Interpreting the Data Protection Directive 1998", *WDPR* (February 2004).

The U.K. FOIA Exemptions and the Public Interest Test: Moving from Need to Know to Right to Know

By Hazel Grant and Rachel Fetches, Bird & Bird

The remaining sections of the Freedom of Information Act 2000 (the "FOIA") come into force in January 2005 and individuals will have a general right of access to information (the right to know) held by public authorities. This right of access is actually two rights: first, the right to be informed by a public authority whether it holds information (the duty – on the authority – to confirm or deny), and second, the right to have that information communicated to the applicant. These rights are then subject to 25 exemptions, which are contained in Part 2 of the FOIA. Of those 25 exemptions, 17 are qualified by the requirement for the public authority to consider a "public interest test" (see table 1). One of the keys to the success of the FOIA will be the application by public authorities of this test.

Prejudice and the Public Interest Test

Most of the exemptions only apply to the extent to which some harm – or in the terminology of the FOIA "prejudice" – would result if the exemption were not available. Therefore, a public authority must not only decide which exemption is most relevant, but also go on to consider whether any harm or prejudice would result if the information were not protected. The most important ramification of this is that prejudice-based exemptions will not cover whole classes of information and it is likely that at least part of the information requested must be revealed (see table 1).

Public Interest Test

Exemptions in the FOIA are categorised as either "absolute" or "subject to the public interest test" (commonly called "qualified"). For qualified exemptions, the public interest test states that a public authority must consider whether the public interest in maintaining the exemption outweighs the public interest in disclosing the information. As this test applies to the majority of exemptions under the FOIA, public authorities will have to learn how to apply the test in practice.

The Public Interest

The FOIA does not define the public interest, preferring instead to allow for flexibility in the interpretation of what the public interest is, depending on changing times and circumstances. This is in line with freedom of information legislation in other countries such as Canada and Australia.

It should be noted that the test states that the public interest in not disclosing information must *outweigh* the public interest in disclosing the information (or that the public authority holds the information). Therefore, if in determining the balance the two interests are the equal, the information should be disclosed.

Table 1: Exemptions under Part 2 of the Freedom of Information Act 2000

Section	Title	Qualified or Absolute Exemption	Prejudicial exclusion of information
21	Information accessible by other means	A	No
22	Information intended for future publication	Q	No
23	Security matters	A	No
24	National security	Q	No
26	Defence	Q	Yes
27	International relations	Q	Yes
28	Relations within the U.K.	Q	Yes
29	The economy	Q	Yes
30	Investigations by public authorities	Q	No
31	Law enforcement	Q	Yes
32	Court records	A	No
33	Audit function	Q	Yes
34	Parliamentary privilege	A	No
35	Formulation of government policy	Q	No
36	Prejudice to effective conduct of public affairs	Q/A*	Yes
37	Communications with Her Majesty and honours	Q	No
38	Health and safety	Q	Yes***
39	Environmental	Q	No
40	Personal information	Q/A**	No
41	Information provided in confidence	A	No
42	Legal professional privilege	Q	No
43	Commercial interests	Q	Yes/No****
44	Prohibitions on disclosure	A	No

* This exemption is absolute insofar as it applies to information held by the House of Commons and the House of Lords.

** The absolute exemption applies to s. 40(1), and s. 40(2) insofar as it relates to cases where the first condition (set out in s. 40(3)(a)(i) or (b)) is satisfied.

*** The harm in s. 38(1) is endangerment.

**** This exemption is class-based insofar as the information constitutes a trade secret s. 43(1).

  WDPR ISSN 1473-3579

At this point it is also a matter of debate as to what counts as the public. Does this mean all of the public, a section of the public or an individual member of the public? In other jurisdictions, the term has been interpreted as having a geographic or numeric sense but it has also been considered to potentially apply to a single individual. Thus, it seems that "the public" may vary depending on the circumstances.

Information Commissioner's Guidance

To help public authorities in the application of the public interest test, the Information Commissioner (the "IC") has produced a series of awareness and guidance notes, which can be found on the IC's website (*www.informationcommissioner.gov.uk*). Guidance number 3[1] discusses the public interest test and gives some examples. The IC notes that it is difficult to give clear guidance on this test but does give some factors that public authorities should consider or ignore (see figure 1).

Figure 1: Weighing the Public Interest

Weighing the Public Interest

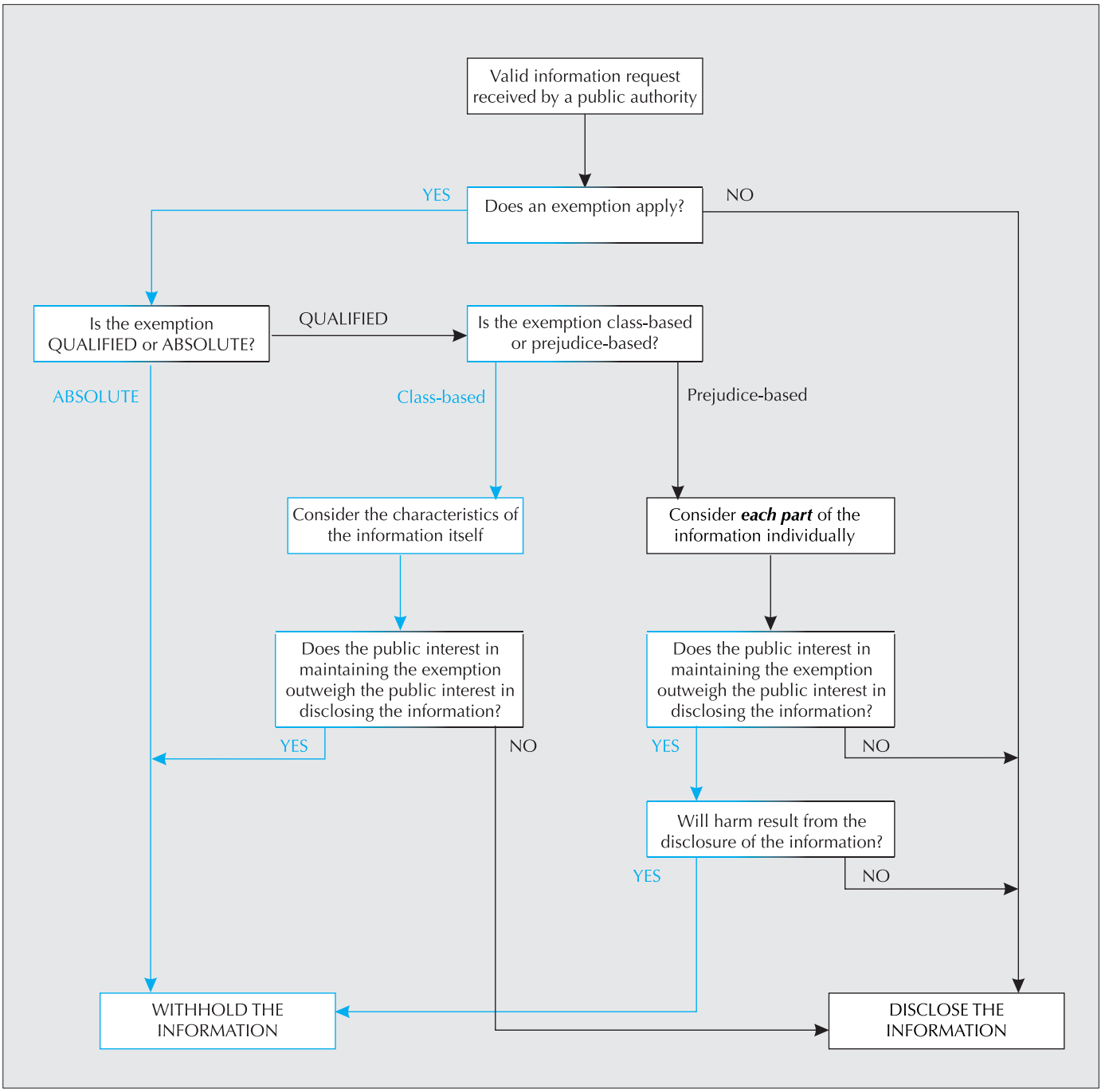
Factors to be considered:

- Assisting in public debate
- Ensuring accountability and openness in decisions
- Ensuring accountability and transparency in spending
- Allowing individuals and companies to understand and challenge decisions that affect them
- Ensuring prompt disclosure of public health and public safety information

Factors to be ignored

- Public curiosity
- Potential embarrassment of the government
- The complexity of the information

Flowchart: The Public Interest Test



These factors are mostly gleaned from research commissioned by the IC in August 2003 from UCL's Constitution Unit ("Balancing the Public Interest: Applying the Public Interest Test to Exemptions in the UK Freedom of Information Act 2000"[2]). The research looks at decisions of the U.K. Parliamentary Ombudsman under the "Open Government Code of Practice on Access to Government Information".[3] This non-statutory Code has been in operation since 1994 and includes its own public interest test. An analysis of the Parliamentary Ombudsman's decisions between 1994 and 2002 showed that the public interest was considered in 21 out of 106 decisions. In approximately 66 percent of those cases, the public interest did not outweigh the potential harm caused by disclosure and the information was withheld.

The research also looks at decisions under similar freedom of information legislation in Ireland, Canada, Australia and New Zealand. It is important to note that the public interest test in these jurisdictions is not exactly the same as the public interest test in England and Wales. Although there is a requirement to consider the public interest, the tests have different wordings and emphasis. In addition, as in England and Wales, the public interest test is very context specific and so where a topic is of great interest in one country, it may be of little or no relevance in another.

Conclusion

Despite the obvious importance of the public interest test to the application of the FOIA, it is difficult to provide general guidance on how to apply the test. The test is very context specific and whether information is disclosed or not will depend on the timing of the request and what is already in the public domain. What is clear is the determination to change the culture of Government from the need to know to the right to know. In shifting the balance in favour of greater openness, the public interest test will be an important factor. (See Flow Chart on the previous page.)

1 www.informationcommissioner.gov.uk/cms/DocumentUploads/AG%203%20-%20Pub%20Int%20reform.pdf

2 http://www.humanrightsinitiative.org/programs/ai/rti/international/laws_papers/uk/public_interest_MCook_Aug03.pdf

3 *http://www.dca.gov.uk/foi/ogcode981.htm*

See also "United Kingdom: The Freedom of Information Act 2000", *WDPR* (September 2004).

Case Report

EUROPEAN UNION

Privacy Laws Do Not Prevent Itemised Phone Bills

The European Court of Justice has confirmed the European Commission's view that E.U. data privacy rules do not prevent telephone operators from providing telephone bills that list individual calls.

The Revised Voice Telephony Directive[1] aims to ensure the availability throughout the European Union of good quality public telephone services. It defines a set of services to which all subscribers should have access and specifically provides that itemised billing should be available on request. Itemised bills must show a sufficient level of detail to allow verification and control of the charges incurred, and a basic level of itemised billing must be available at no extra charge to the subscriber.

The Austrian authorities transposed the requirements of the Revised Voice Telephony Directive into their national law, by providing that a "standard" bill would include, if requested by the subscriber, itemised details, but for bills showing a higher level of detail than a standard bill, a fee could be charged. The European Commission took the view that the information provided by Austrian telephone operators did not allow subscribers to carry out an effective verification and control of their telephone charges. In particular, a standard bill only allowed subscribers to deduce that they have made a certain number of calls costing a certain amount within the different tariff bands during the period covered by the bill. Standard billing does not enable verification of the date on which a call was made or the number called and therefore does not permit an effective verification of charges. In other words, verification of charges could only be performed upon payment of an extra charge.

The European Commission took its case to the European Court of Justice, which found that Austria had failed to provide detailed arguments supporting its assertion that more detailed bills would infringe European data protection legislation. It seems as if it was trying to argue that there was a potential conflict between European telephony and data protection legislation.

Data protection legislation protects the rights and the privacy of individuals by limiting the way that a business can use individuals' personal data. An itemised bill lists the telephone number of all those called by a subscriber, and these numbers could be seen as personal data of the subscriber in question. If telecommunication companies were required to list such personal data on a subscriber's itemised bill, it is likely that this would amount to a breach of an individual's rights under data protection legislation.

However, the Directive on Privacy and Electronic Communications[2] provides that subscribers "shall have the right to receive non-itemised bills", and it goes on to provide that national laws must reconcile the rights of subscribers receiving itemised bills with the right to privacy of calling users and called subscribers,

> "for example by ensuring that sufficient alternative privacy enhancing methods of communications or payments are available to such users and subscribers".

These provisions are reflected in The Privacy and Electronic Communications (EC Directive) Regulations 2003[3] which imposes a duty on OFCOM to have regard to the need to reconcile the rights of subscribers receiving itemised bills with the rights to privacy of calling users and called subscribers, including the need for sufficient alternative privacy-enhancing methods of communications or payments to be available to such users and subscribers. Examples of alternative privacy enhancing methods in the United Kingdom include pre-paid telephone cards and services.

1 Directive 98/10/EC of the European Parliament and of the Council on the application of open network provision to voice telephony and on universal service for telecommunications in a competitive environment.

2 Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

3 SI 2003/2426.

By Charlotte McConnell, Bristows, London.

  WDPR ISSN 1473-3579

News

CANADA

Guidelines on the Protection of Personal Information in the Private Sector

The Privacy Commissioner of Canada (the "Commissioner") has recently released the following five fact sheets, which clarify and interpret some of the key provisions of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 ("PIPEDA").

Determining the Appropriate Form of Consent under PIPEDA

Organisations subject to PIPEDA must generally obtain consent from individuals when collecting, using or disclosing personal information. This fact sheet reviews the common types of consent that may be obtained and provides guidance on when each type may be relied upon. "Express" or "opt-in" consent invites an individual to take action to give consent (*e.g.*, checking off an "I Consent" box), and is the recommended form of consent when an organisation is handling sensitive personal information. "Opt-out" consent assumes consent is given, requires an individual to take action to decline consent (*e.g.*, un-checking an "I Consent" box), and is not recommended for use when handling sensitive personal information. Whether an organisation obtains an opt-in or opt-out consent, it must clearly inform individuals of the purposes for which their personal information will be used. "Implied consent" may also be relied upon by an organisation in circumstances where an individual can reasonably anticipate the purposes for which his/her personal information will be used. Whenever sensitive personal information is involved, the threshold of reasonableness will generally be higher. Determining the appropriate form of consent to obtain is essential to an organisation's compliance with PIPEDA, and when approached strategically this decision can assist an organisation in minimising compliance challenges and costs (see *www.privcom.gc.ca/fs-fi/02_05_d_24_e.asp*).

Dealing with pre-PIPEDA Personal Information (Non-Grandfathering)

Unlike provincial private sector privacy legislation in British Columbia (*Personal Information Protection Act*, S.B.C. 2003, c. 63) and Alberta (*Personal Information Protection Act*, S.A. 2003, c. P-6.5), PIPEDA applies retroactively, covering personal information that was collected before PIPEDA came into force: January 1, 2001, for federally regulated business, and January 1, 2004, in provinces that had not at that time enacted "substantially similar" legislation. In this fact sheet, the Commissioner provides organisations with advice on how to comply with this "non-grandfathering" requirement under PIPEDA. In particular, an organisation should begin by reviewing the personal information in its custody and discarding data that is obsolete or unnecessary. An organisation should then confirm whether appropriate consent has been obtained in connection with the pre-PIPEDA personal information it elects to keep (*i.e.*, express/opt-in, opt-out, or implied). If consent has not been obtained, the organisation must obtain consent from the individuals concerned. Finally, an organisation must also ensure that it has clear policies in place to provide individuals with access to their personal information in its custody. While the challenges posed by the non-grandfathering provisions of PIPEDA are significant, the Commissioner's guidance is a useful starting point when working to comply (see *www.privcom.gc.ca/fs-fi/02_05_d_22_e.asp*).

Use of Social Insurance Numbers by the Private Sector

In a third fact sheet, the Commissioner affirms the well-established position that Social Insurance Numbers ("SINs") are a sensitive form of personal information that should only be collected and used for limited purposes, most of which relate to banking, employment and income tax reporting. For instance, it is generally reasonable for employers to collect SINs for income tax, Canada Pension Plan, and employment insurance purposes, and for financial institutions to collect SINs for interest-earning accounts or retirement savings plan contributions. In most other cases, however, the Commissioner recommends that organisations avoid collecting SINs. Further, where an organisation finds it is necessary to collect SINs, the organisation must generally obtain express consent, clearly identify the purposes for which the SINs are collected and used, inform individuals that providing their SINs for identification purposes is optional and not necessarily a condition to access the organization's basic services, and at all times adhere to best practices when complying with PIPEDA (see *www.privcom.gc.ca/fs-fi/02_05_d_21_e.asp*).

Protecting Personal Information Transferred Across Borders

A fourth fact sheet suggests how Canadians can prevent the transfer of their personal information to bodies in countries that do not yet provide the same level of protection for privacy and personal information as Canada. Individuals are advised to ask questions about organisations' personal information handling practices – and especially their outsourcing arrangements – to ensure that they fully comply with the organisation's obligations under PIPEDA. Individuals are advised to file complaints if they have concerns about an organisation's practices, and told that PIPEDA's whistleblower provisions can be used to protect their confidentiality when filing complaints. Organisations subject to PIPEDA that frequently transfer personal information internationally should be aware of the Commissioner's focus on international data transfer issues and be sure to structure their personal information handling practices accordingly (see *www.privcom.gc.ca/fs-fi/02_05_d_23_e.asp*).

Protecting Privacy on the Internet

Finally, the Commissioner has released a fact sheet that outlines several ways individuals can protect their privacy when using online services. When using the Internet, the Commissioner recommends that individuals review and possibly decline certain cookies, rely on secure encryption methods for financial transactions, use "disposable" e-mail addresses, and carefully review website privacy policies. Individuals are also encouraged to use pseudonyms and

disposable e-mail addresses in chat rooms or newsgroups. When sending e-mail, the Commissioner advises individuals to delete rather than respond to spam, avoid opening suspicious attachments, write messages with the realisation that they can be easily forwarded or intercepted, and watch for scams in which someone attempting to impersonate a legitimate business requests personal information ("phishing"). See *www.privcom.gc.ca/fs-fi/02_05_d_13_e.asp)*.

Although these fact sheets are not binding law, they provide useful insight concerning the Commissioner's approach to interpreting several central issues under PIPEDA. Organisations should carefully consider the guidance provided by the Commissioner in these and other fact sheets when formulating their compliance strategy and preparing policies and procedures, so as to minimise the risks and costs associated with non-compliance, privacy complaints and a possible investigation by the Commissioner's Office.

By William Karam (william.karam@bakernet.com), Arlan Gates (arlan.gates@bakernet.com) and Robin Rix (robin.s.rix @bakernet.com, Student-at-Law) of Baker & McKenzie LLP's International Commercial Group in Toronto; www.bakernet.com.

EUROPEAN UNION

Article 29 Working Party Sets out Strategy Plans

The Article 29 Data Protection Working Party, an independent advisory committee set up under the Data Protection Directive, published a strategy document setting out its priorities for the next few years.

In the document the working party emphasises the need for more uniform compliance with the Directive by governments across Europe and the need to improve enforcement mechanisms. The working party will also be working on Europe-wide data protection codes of conduct and promoting co-operation between the different European data protection authorities. Among the issues highlighted for consideration by the working party in the near future is the impact of new technologies including radio frequency identification, mobile and geo-localisation services and developments in e-government. Developments in nanotechnologies, genetics and biometrics will also be monitored for data protection issues. International transfers of personal data and particularly the use of binding corporate rules as a means for multinational companies to ensure sufficient protection for international transfers of personal data intra-group is also identified as an important area.

By Astrid Arnold, Lovells.

UNITED KINGDOM

Implementation of Data Protection Directive Gives Rise to Tensions with E.U.

In the aftermath of the *Durant v. FSA* case, the European Commission has commenced an investigation into the U.K. Government's compliance with the Data Protection Directive.

The Court of Appeal in Durant held that not all identifiable data, whether stored on computer or in a highly structured paper file, would necessarily be covered by the Data Protection Act 1998. There are comments in the case suggesting that only information affecting a person's privacy would be "personal data" for the purposes of the Act.

Earlier in 2004, and in response to the judgment, the Information Commissioner issued guidance which sought to expand upon the Court of Appeal's comments. The E.U. Commission has since issued a formal letter to the U.K. Government asking for a response to queries about the United Kingdom's implementation of the Data Protection Directive, including the impact of the Durant ruling and the Commissioner's guidance.

The Commission's letter will not be made public. However it is understood from Government sources that the Commission is concerned about the Information Commissioner's guidance as to when identifiable information will be considered to "relate to" and hence be "personal data". In particular, the Commissioner is believed to have highlighted inconsistencies between the broader interpretation of 'personal data' in the Directive and the Information Commissioner's guidance.

We understand that the Government Department handling the E.U. investigation considers that *Durant* is consistent with the Directive. The Department advises that,

> "the Court of Appeal judgment does *not* significantly restrict the definition of "personal data", which continues to have a broad meaning… In addition, the direct effect of the Directive would mean that any court considering similar issues would be bound to conclude that a narrow definition was not permissible and could not lawfully be applied".

Amongst the other issues it is understood that the Commission has raised are:

- the United Kingdom's laissez-faire approach to transfers of personal data outside the EEA;
- the lack of a statutory definition of "consent";
- whether powers available to the Information Commissioner are sufficient – in particular, whether the Commissioner should have powers to award compensation and/or impose actual penalties.

The Government is believed to have issued a response to the Commission's letter in early November, the details of which are yet to be made public.

By Victoria Sedgwick and Ruth Boardman, Bird & Bird, London.

See also, "United Kingdom: Scope of the Data Protection Directive is Narrowed", *WDPR* (January 2004); and "United Kingdom: Interpreting the Data Protection Directive 1998", *WDPR* (February 2004).

UNITED STATES

FCC Extends Stay of Key Provisions of Unsolicited Fax Rules

On October 1, 2004 the Federal Communications Commission released an Order, extending until June 30, 2005, its stay of important provisions of its July 3, 2003 Rule concerning unsolicited faxes. In particular, this Order stayed until June 30, 2005:

   ISSN 1473-3579

- the provision of its July 3, 2003 Rule which had determined that an "established business relationship" (such as an association membership) would no longer be sufficient to show that an individual or business had given express permission to receive unsolicited fax advertisements; and;
- the provision of its July 3, 2003 Rule which had required the sender of a fax advertisement to first obtain the recipient's express permission *in writing*.

Absent this extension, commencing January 1, 2005, associations would have had to obtain written consent from their own members and other existing customers in order to fax material to them advertising the commercial availability or quality of any property, goods or services, including, for example, association conferences and publications for which a fee is charged. The recent FCC Order is good news for associations, who may now continue until at least June 30, 2005 to fax unsolicited advertisements to their members and other existing customers without obtaining their express written consent to receive such faxes. Of course, associations must still check to make sure that no applicable state law would prohibit such an unsolicited fax advertisement.

The FCC issued this stay order in large part because the U.S. House of Representatives had passed a bill which would reinstate the established business relationship rule for faxes under certain circumstances under certain limits, and because the U.S. Senate is considering similar legislation. It is most possible that such legislation will not make it through this Congress. The stay through June 30, 2005 will give the next Congress time to consider and adopt legislation which would allow some form of fax advertisements to be sent to association members and others with whom an established business relationship exists, without prior written consent.

By Robert H. Jackson, Reed Smith, Washington D.C.

Personal Data

Privacy of Foreign Nationals under U.S. Law

By John W. Kropf

Trend: U.S. Government Access to Personal Data on Foreign Visitors

Since September 11, 2001, the United States has worked with foreign partners to improve U.S. access to information on international travelers. Examples include the Secretary of State's authorisation by the USA PATRIOT Act of 2001 to make agreements with foreign governments to share information from the visa lookout database for the purpose of fighting terrorism;[1] Homeland Security Presidential Directive 6 (HSPD-6) that tasked the Secretary of State to seek ways to access terrorist biographic screening information from foreign partners;[2] and a Department of State program to share lost and stolen passport data with foreign governments.[3]

Another example is the exchange of airline passenger information – known as Passenger Name Record (PNR) data – an agreement that the Department of Homeland Security (DHS) has entered into with the European Commission (EC) to enable the transfer of this information.[4]

The 9/11 Commission recognised the critical role information sharing plays in the fight against terrorism when it recommended that:

> The U.S. government cannot meet its own obligations to the American people to prevent the entry of terrorists without a major effort to collaborate with other governments. We should do more to exchange terrorist information with trusted allies, and raise U.S. and global border security standards for travel and border crossing over the medium and long term through extensive international cooperation.[5]

The Commission singled out exchanging lost and stolen passport information as having immediate security benefits that are particularly important so long as it is consistent with privacy requirements.[6]

Issue: Perceived Lack of Privacy Protection

After a year of negotiations, the EC agreed in May 2004 on a legal arrangement with DHS to provide PNR data relating to flights between the U.S. and E.U. Member States.[7] The European Parliament, disturbed over what it views as an attack on personal privacy, filed suit against the European Commission for entering into the agreement with DHS.[8] In fact, there seems to be a perception in the European Union, and possibly by other foreign partners, that the United States provides little or no privacy protection for foreign citizen data held by the U.S. Government.

In part, that concern centres on the perceived data access rights of outside entities, including corporations, the media, non-government organisations, foreign governments, and private individuals. Such perceptions impede the U.S. Government's attempts to enter into future agreements to exchange information.

Part of this negative perception may come from the limited protection of the Privacy Act of 1974.[9] The Act covers the privacy of U.S. citizens and lawful permanent residents (LPRs) but does not otherwise extend to foreign nationals. Some misperceptions may also be based on the differences between the U.S. common law legal system and the civil law systems that operate in most of the European countries and elsewhere.

Existing Authority to Protect Privacy of Foreign Nationals

Although foreign nationals who are not LPRs are not protected by the Privacy Act, they still can have their personal information protected under international information sharing agreements and U.S. laws like the Freedom of Information Act (FOIA).[11]

Typically, a request to publicly disclose information held by a federal agency must be filed under the FOIA.[12] If an agency receives a request from a member of the public for personal information on a foreign national obtained pursuant to an international agreement, the agency can deny the information on a number of grounds recognised under FOIA.[13] As a fundamental matter, the basic purpose of the FOIA is to shed light on the operations of the federal government[14] and this purpose is almost never served by disclosing personal information regardless of whether the individual is a U.S. citizen or not.

FOIA Exemptions

Exemptions 6 and 7(C): Personal Privacy

The strongest FOIA protections for personal privacy interests are Exemptions 6 (personal privacy) and 7(C) (personal privacy in law enforcement records).[15] Even where there is no agreement in place or where the non-disclosure provisions are inadequate, the privacy exemptions may be relied upon by an agency to protect information on foreign nationals.

Under Exemptions 6 and 7(C), courts regularly uphold the non-disclosure of information concerning marital status, legitimacy of children, welfare payments, family fights and reputation, medical condition, date of birth, religious affiliation, citizenship data, genealogical history, social security numbers, criminal history records, incarceration of United States citizens in foreign prisons, sexual inclinations or associations, and financial status.[16] In these cases, the courts have applied the traditional privacy analysis that information all individuals receives under FOIA – regardless of whether the person is a U.S. citizen or non-U.S. citizen – and have determined that disclosure of such information would shed little or no light on the Government's operations.[17]

The privacy interests of foreign nationals were recognised by the U.S. Supreme Court when it upheld the State Department's denial of a request from The Washington Post for documents indicating whether certain Iranian nationals held U.S. passports.[18] The Court said that citizenship data satisfied the "similar files" requirement of FOIA exemption for personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of privacy. Not only did the Court protect the information on privacy grounds but it also found significant the potential harm that could result to the individual if such information were disclosed. In offering assurances to foreign partners, it is worth noting that an individual's citizenship – seemingly the most basic, benign information – was protected the highest court in the land.[19] In addition to citizenship information, courts have also upheld protections of information concerning identities of asylum applicants and related data.[20] Thus, based on the view of Supreme Court and lower courts, an agency should be able to exempt personal information concerning passport information or PNR data on the basis of privacy.

Exemption 3

International Agreements: Treaties Subject to Advice and Consent of the Senate

Exemption 3 of the FOIA, which incorporates the various non-disclosure provisions that are contained in other federal statutes, may also provide a basis for non-disclosure.[21] This would depend upon whether the information sharing agreement contains a nondisclosure provision.[22] The standard Limitations on Use provision generally found in treaties on Mutual Legal Assistance in Criminal Matters (MLAT) is one example. Article 7 of the U.S. Government's MLAT with Australia states that:

> 1. If the Central Authority of the Requested State so requests, the Requested State shall not use any information or evidence obtained under this Treaty in any investigation, prosecution, or proceeding other than that described in the request without the prior consent of the Requested State.
>
> 2. The Central Authority of the Requested State may request that the information or evidence furnished under this Treaty be kept confidential or be used only subject to the terms and conditions it may specify. In such cases, the Requesting State shall use its best efforts to comply.[23]

In fact, provision two was added to address the concern of the Australians that information provided might be disclosed pursuant to a FOIA request.[24]

While the issue of whether a treaty such as an MLAT – which is subject to advice and consent of the Senate – can qualify as an Exemption 3 statute has not been tested in the courts, the Department of Justice is of the opinion that "there is a sound policy basis for concluding that a treaty can so qualify".[25] Therefore, if the personal information the agency receives is pursuant to a treaty that includes a relevant non-disclosure provision, the agency could cite to that treaty provision as providing a reason for non-disclosure pursuant to Exemption 3 and could defend denial on this basis in courts. It is reasonable to believe that such a defense could be successful.

Executive Agreements

In the case of an international agreement that does not require the advice and consent of the Senate, however, the courts have not definitively addressed the question of whether such agreements qualify as an Exemption 3 statute.[26] An agency should therefore be cautious about relying solely on a nondisclosure provision as an independent basis under Exemption 3 for withholding information that would otherwise be disclosable under the FOIA. Even though governments may declare themselves to be legally bound by their terms, part of the uncertainty is that such agreements are not "treaties" as the U.S. defines them domestically.- Despite this uncertainty, an Executive Agreement can still require the Parties use "best efforts" to protect against disclosure.[27] This could include the opportunity for the Department of State, or even the foreign government itself, to present its views through a written statement to a court, on why such information should not be disclosed.

In a case where the instrument in question is not legally binding and constitutes only a political commitment[28] – it is even more uncertain whether a court would find that such an agreement qualifies as a FOIA Exemption 3 statute.

Independent Statutory Authority

Regardless of the existence of an agreement, an agency may have independent statutory authority to exempt the information concerning foreign nationals from disclosure. For instance, information obtained from a foreign government that is used by the Department of State for the issuance or denial of a visa will be exempt under the section 222(f) of Immigration and Nationality Act INA 222(f).[29] This confidentiality statute has been held to qualify as an Exemption 3 statute.[30]

Exemption 1: National Security Information

While it is unlikely that personal information alone would be classified as national security information, the possibility should be considered. Under Executive Order 12958, as amended by E.O. 13292, the unauthorised disclosure of foreign government information is presumed to cause damage to the national security.[31] "Foreign government information" includes,

> "information provided to the United States Government by a foreign government or governments ... with the expectation that the information, the source of the information, or both, are to be held in confidence," and "information produced by the United States Government pursuant to or as a result of a joint arrangement with a foreign government ... requiring that the information, the arrangement, or both are to be held in confidence".[32]

In the case of an international information sharing agreement, the terms of the agreement that address the status of the information would evidence the Parties' expectation with respect to confidentiality and would control the status of the information. If the agreement provides that the personal information exchanged will be kept confidential, the information may be classified under section 1.4 of E.O. 12958, and withheld from disclosure in response to a FOIA request pursuant to Exemption 1.[33] If the U.S. intends to exchange information it deems classified, it will expressly negotiate such an agreement and the parties will mark all such information accordingly.[34] In the absence of an express classification provision, it is unlikely that the governments intended the personal information to be protected in this manner.

Procedural: Information Not Under Agency Control

The question of agency control should not be overlooked. The requested record must meet the two-part test for determining what constitutes an agency record under FOIA: agency records must be (1) either created or obtained by an agency, and (2) under agency control at the time of the FOIA request.[35] Assuming there is an international agreement in force, and depending on its provisions, the agency could argue that the information is not under the control of the agency and therefore not a record for purposes of FOIA.[36] For example, in response to a FOIA request, a court found that a Canadian Safety Board aircraft accident investigation report of an air crash, although possessed by the National Transportation Safety Board (NTSB), was not under agency "control" because of the nondisclosure restrictions imposed by the Convention on International Civil Aviation.[37] Likewise, if a similar non-disclosure provision were included in an agreement for sharing personal information on foreign nationals, the agency that possesses the information may be able to make a similar argument. In short, that the material is not "FOIA-able" as a threshold matter.

Waiver

A requester may argue that by sharing personal or biographic information with the U.S. Government, the foreign government waives whatever protections the foreign government applied to its information. Government-to-government sharing of information under controlled or confidential circumstances should not constitute a waiver, however. Such protection has been found where the U.S. Government has shared protected information with foreign governments in bilateral and multilateral contexts including a closed session of the UN Security Council and a diplomatic negotiation.[18] Similarly, receiving personal information from a foreign government authority under controlled or confidential conditions, such as those established by an international agreement, should demonstrate the same level of control. Even where there is no agreement and the sharing does not involve disclosure to the public, the information should still be protected. This protection also extends to an agency's sharing foreign government information among other federal agencies.[39] Thus, an agency should be able to make a successful defence against a waiver argument.

Conclusion

As the U.S. Government seeks to enter into more international agreements involving the exchange of personal data, it can offer foreign partners concrete assurances that it can protect their personal information. The Government can do this two ways: first, by drafting robust non-disclosure provisions in its agreements and second, by explaining the existing protections under the FOIA. The two work in tandem to provide a strong framework for protection. Even without the protection of an agreement, U.S. law still recognises privacy interests of non-U.S. citizens. In the course of any discussion on information exchange, U.S. negotiators should work to articulate these protections to foreign partners. By communicating the various options for protecting the data of foreign partners, the U.S. Government can help diminish the barriers to information sharing as it fights the war against terror.

1 Section 222(f) Immigration and Nationality Act (8 U.S.C. s. 1202(f)) as amended by s. 413 of the USA PATRIOT Act of 2001, Act of October 26, 2001, Pub. L. No. 107-56, 115 Stat. 272.

2 Section 5, HSPD-6, September 16, 2003. The Directive's implementing MOU stipulates that the Parties will make accessible appropriate information to foreign governments cooperating with the United States in the war on terrorists of global reach.

3 Frank E. Moss, Deputy Assistant Secretary for Passport Services Bureau of Consular Affairs, Address to the International Relations Committee, U.S. House of Representatives (June 23, 2004).

4 U.S. law requires airlines operating flights to and from the United States to provide DHS, Customs and Border Protection, with certain passenger information. 49 U.S.C. 44909(c)(3) and its implementing (interim) regulations, 19 CFR 122.49(b).

5 The 9/11 Commission Report (New York: W.W. Norton & Company), 390.

6 The 9/11 Commission Report (New York: W.W. Norton & Company), 389. The Commission did not specify if this meant the privacy of U.S. and non-U.S. Citizens or the privacy of U.S. citizens only.

7 Sara Kehaulani Goo, "EU Agrees to Give U.S. Airline Passenger Data", *The Washington Post*, May 15, 2004.

8 *EU Business*, "US, EU Confident Passenger Data Deal will Survive Legal Challenge," September 18, 2004, available at *www.eubusiness.com*.

9 5 U.S.C. 552a.

10 The Privacy Act applies to "a citizen of the United States or an alien lawfully admitted for permanent residence". 552a(a)(2).

11 5 U.S.C. 552.

12 The scope of this paper is limited to cases involving public disclosure and does not necessarily address the question of sharing among the agencies within the Executive Branch of the U.S. Government or with Congress.

13 For DHS's discussion of how the FOIA might apply to PNR data see Undertakings of DHS Bureau of Customs and Border Protection paragraphs 24-27, available at *www.dhs.gov/interweb/assetlibrary/CBP-DHS_PNRUndertakings5-25-04.pdf.*

14 *U.S. Dep't of Justice v. Reporter's Comm. For Freedom of the Press*, 489 U.S. 749, 773 (1989).

15 5 U.S.C. 552(b)(6), "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy; 5 U.S.C. 552(b)(7), "records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information...(C) could reasonably be expected to constitute an unwarranted invasion of personal privacy".

16 DOJ FOIA Guide May 2004, at 475–76, footnotes and case citations omitted.

17 Reporters Comm., 489 U.S. at 773.

18 *United States Dep't of State v. Wash. Post Co*., 456 U.S. 595, 602 (1982) cf. *Judicial Watch, Inc. v. Reno*, No. 00-0723, 2001 WL 1902811, at *8 (D.D.C. Mar. 30, 2001) (asylum application); *Judicial Watch, Inc. v. U.S. Dep't of Commerce*, 83 F. Supp. 2d 105, 112 (visa and passport data).

19 The Court cited an affidavit from a Department official stating that, "it is the position of the Department of State that any statement at this time by the United States Government which could be construed or misconstrued to indicate that any Iranian public official is currently a United States citizen is likely to cause a real threat of physical harm to that person." *United States Dep't of State v. Wash. Post Co*., 456 U.S. at 598; see also *Hemenway v. Hughes*, 601 F. Supp. 1002, 1006 (D.D.C. 1985) ("Nationals from some countries face persistent discrimination ... [and] are potential targets for terrorist attacks."); cf. Judicial Watch, 83 F. Supp. 2d at 112 (visa and passport data).

20 See *Shaw v. United States Dep't of State*, 559 F. Supp. 1053, 1067 (D.D.C. 1983); see also *United States Dep't of State v. Ray*, 502 U.S. 164 (1991) (applying traditional analysis of privacy interests under FOIA to Haitian nationals); *Ctr. for Nat'l Sec. Studies v. United States Dep't of Justice*, 215 F. Supp. 2d 94, 105-06 (D.D.C. 2002) (recognising, without discussion, the privacy rights of post-9/11 detainees who were unlawfully in the United States) (Exemption 7(C)), *aff'd on other grounds*, 331 F.3d 918 (D.C. Cir. 2003), cert. denied, 124 S. Ct. 1041 (2004); *Schiller v. INS*, 205 F. Supp. 2d 648, 662 (W.D. Tex. 2002) (finding that "[a]liens [and] their families ... have a strong privacy interest in nondisclosure of their names, addresses, and other information which could lead to revelation of their identities") (Exemption 7(C)); *Judicial Watch, Inc. v. Reno*, No. 00-0723, 2001 WL 1902811, at *8 (D.D.C. Mar. 30, 2001) (protecting asylum application filed on behalf of Cuban emigré Elian Gonzalez).

21 5 U.S.C. 552(b)(3). "specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld".

22 The Exemption 3 argument is very similar to the agency control argument discussed below but may be needed where the control argument fails and the court has gone on to consider FOIA exemptions.

23 Treaty on Mutual Assistance in Criminal Matters, Apr. 20, 1997, U.S.-Austl., 2117 UNTS 157.

24 S. Rep. No 105-22, p. 40 (1998).

25 *DOJ Freedom of Information Act Guide and Privacy Act Overview*, May 2004 ed., pp. 234, citing *Whitney v. Robertson*, 124 U.S. 190, 194 (1887) ("By the Constitution a treaty is placed on the same footing, and made of like obligation, with an act of legislation.").

26 *Pub. Citizen v. Office of the United States Trade Representative*, 804 F. Supp. 385, 388 (D.D.C. 1992) (stating that trade agreement not ratified by Senate does not have status of "statutory law" and thus does not qualify under Exemption 3), *appeal dismissed per stipulation*, No. 93-5008 (D.C. Cir. Jan. 26, 1993).

27 An international agreement done without advice and consent of the Senate is an "international agreement other than a treaty" for purposes of U.S. domestic law; this category of international agreement includes "executive agreements," which are done pursuant to the President's constitutional authorities. This category of international agreements also includes agreements done pursuant to U.S. authorising legislation. For international law purposes, both categories are considered to be "treaties", including as defined by the Vienna Convention on the Law of Treaties (VCLT), insofar as they are international agreements between two or more states or international organisations and are intended to be legally binding and governed by international law. While the United States is not a party to the VCLT, it accepts the VCLT's definition of a treaty as consistent with customary international law.

28 For example, a legally binding instrument contains terms such as "shall" or "will" as compared to a political document which contains terms such as "intends to" or "understands".

29 8 U.S.C. s. 1202(f).

30 *Medina-Hincapie v. Dep't of State*, 700 F.2d 737, 741-42 (D.C. Cir. 1983).

31 E.O. 12958, as amended, sections. 1.1(c) and 1.4(b). See also, 1.6(e) on foreign government classification markings.

32 E.O. 12958, as amended, 6.1(r).

33 5 U.S.C. 552(b)(1).

34 See *e.g.*, Agreement Concerning Security Measures for the Protection of Classified Information, June 25, 2002, US-Australia.

35 *United States Dep't of Justice v. Tax Analysts*, 492 U.S. 136, 144-145 (1989).

36 See, *e.g.*, *KDKA v. Thornburgh*, No. 90-1536, 1992 U.S. Dist. LEXIS 22438, at * * 16-17 (D.D.C. September 30, 1992).

37 *Thornburgh, Id*. Section 6.2 of Annex 13 to the Convention (Aircraft Accident and Incident Investigation) states that: "States shall not circulate, publish or give access to a draft report or any part thereof, or any documents obtained during an investigation of an accident or incident, without the express consent of the State which conducted the investigation, unless such reports or documents have already been published or released by that latter State".

38 See, *e.g.*, *Students Against Genocide v. Dep't of State*, 257 F.3d 828, 836 (D.C. Cir. 2001) (holding that government did not waive its right to invoke ... FOIA exemptions by displaying the withheld photographs to the delegates of ... foreign governments ... [because they] were not released to the general public); *Van Atta v.* DIA, No. 87-1508, 1988 WL 73856, at **2-3 (D.D.C. July 6, 1988) (holding that disclosure of information to foreign government during diplomatic negotiations was not "public disclosure").

39 See, *e.g.*, *Chilivis v. SEC*, 673 F.2d 1205, 1211-12 (11th Cir. 1982) (agency does not automatically waive exemption by releasing documents to other agencies); *Silber v. United States Dep't of Justice*, No. 91-876, transcript at 10-18 (D.D.C. Aug. 13, 1992) (bench order) (distribution of manual to other agencies does not constitute waiver). But cf. *Lacefield v. United States*, No. 92-N-1680, 1993 WL 268392, at *6 (D. Colo. Mar. 10, 1993) (attorney-client privilege waived with respect to letter from City of Denver attorney to Colorado Department of Safety because letter was circulated to IRS).

The author is an Attorney-Adviser in the U.S. Department of State's Office of the Legal Adviser. The views expressed here are his and not those of the Department of State of the U.S. Government.

  WDPR ISSN 1473-3579

News

CANADA

British Columbia IC Publishes Report on U.S. Patriot Act

On October 29, 2004 the Office of the Information and Privacy Commissioner for British Columbia (Canada) issued its report on the extraterritorial nature of the U.S. Patriot Act. This report is based on the results of a broad public consultation launched in May 2004 and concerns the possible implications of the Patriot Act for the outsourcing of public services by public bodies in British Columbia to service providers located in the United States.

The report broadly concludes that the outsourcing of public services to service providers in the United States is not per se illegal, but that certain protections (including amendments to Canadian privacy law) must be taken to preserve the confidentiality of personal information processed in the United States under such arrangements. Both the full report and a summary can be consulted at: *www.oipcbc.org/sector_public/usa_patriot_act/patriot_act.htm*.

By Christopher Kuner, Hunton & Williams LLP, Brussels

EUROPEAN UNION

Article 29 Working Party Holds Hearing on Binding Corporate Rules

On November 24, the Article 29 Working Party held a hearing in The Hague on binding corporate rules (BCRs) as a legal basis for data processing and transfer, hosted and organised by the Dutch Data Protection Authority. The hearing was part of the Working Party's consultation on BCRs that was launched in November 2003.[1] Attendance was by invitation only, and was limited to those organisations that had sent contributions to the Working Party's consultation.[2] There were approximately 30 representatives of business and the press in attendance, together with data protection officials and commissioners from the European Commission, Austria, the Czech Republic, Germany, Ireland, Latvia, Luxembourg, Malta, The Netherlands, Poland, Spain, Sweden, and the United Kingdom.

The morning session was devoted to presentations by the three companies that have submitted their BCRs to the Working Party for approval (namely DaimlerChrysler, GE, and Philips), and was closed to the other business representatives. The afternoon included presentations by various data protection commissioners and business representatives (including the author, who presented a new report on BCRs by the International Chamber of Commerce).[3] Particular attention was devoted to two documents that the Working Party was to consider for approval at its meeting in Brussels on November 25–26, namely:

- a proposed procedure for coordinating approval of BCRs among different data protection authorities (DPAs); and
- a checklist of points that companies should take into account when submitting BCRs for approval.

The event was significant as the first time the Working Party has ever held a hearing with participation from business representatives. From the discussions, most DPAs in attendance seemed to view BCRs positively as a way for companies to implement meaningful data protection measures throughout their organisations, but a few had concerns about ensuring that BCRs are made legally binding. Business representatives emphasised the need for "one stop shopping" for approval of BCRs to avoid the need to negotiate them with multiple DPAs, and the importance of avoiding unnecessary and overly-burdensome requirements on BCRs that go beyond what is required for other data transfer mechanisms.

By the end, there was a consensus that the hearing had produced an interesting and productive discussion that helped both DPAs and business representatives better understand each other's concerns. The hearing will hopefully mark the beginning of a more open dialogue between the Working Party and the business community on other issues as well.

1 See *www.europa.eu.int/comm/internal_market/privacy/workingroup/consultations/consultation_en.htm*.

2 See *www.europa.eu.int/comm/internal_market/privacy/workingroup/consultations/binding-rules_en.htm*.

3 See the ICC Report on Binding Corporate Rules for the International Transfer of Personal Data, *www.iccwbo.org/home/news_archives/2004/data_transfer.asp*.

By Christopher Kuner, Hunton & Williams LLP, Brussels

EUROPEAN UNION

Data Protection Supervisor Challenges PNR Deal

European Data Protection Supervisor Peter Hustinx is reported to have issued a request to the European Court of Justice, asking the Court to support the legal challenge by the European Parliament of the agreement between the European Community and the United States on the processing and transfer of PNR data by air carriers to the U.S. authorities. The EDPS office has insisted that this deal is a breach of citizens' privacy. In October 2004, the ECJ refused to treat the case (Case C-317/04) under the Court's expedited procedure. As a result, proceedings are expected to last several years.

By Christopher Kuner, Hunton & Williams LLP, Brussels

Security & Surveillance

Italy: The Processing of Personal Data by Means of Video Surveillance Devices (Part II)

By Avv. Alessandro del Ninno, Information & Communication Technology Department, Studio Legale Tonucci, Rome. The author may be contacted by e-mail at adelninno@tonucci.it

Part I of this article, concerning the General Act on Video Surveillance , as enacted by the Italian Data Protection Authority ("IDPA"), was published in the October issue of *World Data Protection Report*. This Act provides a detailed set of practical rules to adhere to when installing video surveillance devices and systems, in order to achieve full compliance with the privacy protection principles related to the processing of personal data and images set forth in the Italian Code on privacy.

Part I recalled the IDPA's general principles governing the installation of any kind of video surveillance device. In Part II, the obligatory and practical fulfilments to be carried out by the processors/holders of video surveillance systems will be analysed.

Practical General Fulfilments

The data subjects must be properly informed about the fact that they are in a place (or entering a place) subject to video surveillance monitoring (including the eventual recording of images): this obligation must also be complied with in the case of public events or shows (*i.e.*, concerts, sport events, *etc.*), or in cases of promotional and advertising activities (*i.e.*, web cams).

The information to be provided must contain all the elements set forth in Article 13 of the Italian Code on Privacy, even if by means of brief (but clear) statements (for such cases, the Italian Data Protection Authority – or "Garante" – has drafted an example of a brief information model to be provided to data subjects, and to be placed in external areas subject to video surveillance). In places other than external areas, the information model must be more detailed and shall include the main elements as per Article 13 of the Code on Privacy.

The sign containing the information:

- must be placed in the areas subject to video surveillance monitoring or close by, even if it is not necessarily placed in direct contact with the video cameras themselves;
- must have dimensions and placement so as to be clearly visible;
- can include an explicit and instantly recognisable symbol, clearly indicating that images are being captured or recorded.

Practical Specific Fulfilments

Prior Checking

- video surveillance systems gathering images to be successively compared and crossed with other particular data (*i.e.*, biometric data), or with electronic cards or with devices of voice recognition;
- video surveillance systems allowing the digital recording of images or automatic advanced research options identifying the single image;
- video surveillance systems not simply recording a place, but routes or facial characteristics or sudden events or behaviours which may not have been previously classified.

Data Processors

The Data Controller must appoint by means of a written act, all the individuals in charge of the processing and authorised to use the video surveillance devices, including the access to recorded images when necessary. The appointment must regard a limited number of individuals, especially when such persons are external collaborators (*i.e.*, private security guards).

The ordinary rules on the eventual appointment of a "Data Processor", contained in Article 29 of the Italian Code on privacy, must be complied with, in particular when the Data Controller use external subjects (*i.e.*, technical maintainers of the video surveillance devices).

When the images taken by the camera are also recorded and kept (for a limited period of time, according to the principle of proportionality), an internal policy regarding different access levels to the images must be set up. In particular, an integral access to the images can be allowed only in case of necessity (*i.e.*, maintenance of the video surveillance devices, request of the judicial or police authorities, *etc.*).

Finally, proper training initiatives for the persons in charge of the processing must be organised – both at the first setting up of the video surveillance system and successively, if technical modifications of the system are introduced – by the Data Controller with the aim of explaining tasks, responsibilities and guarantees.

With regard to the compulsory adoption, by the Data Controller, of the minimum security measures in the processing of personal data (and images), the general rules of the Code on Privacy shall apply also to the processing of images by means of video surveillance devices:

- personal data undergoing processing shall be kept and controlled, also in consideration of technological innovations, of their nature and the specific features of

the processing, in such a way as to minimise, by means of suitable preventative security measures, the risk of their destruction or loss, whether by accident or not, of unauthorised access to the data or of processing operations that are either unlawful or inconsistent with the purposes for which the data have been collected (Article 31 of the Italian Code on Privacy);

- where a data controller adopts minimum security measures by committing the relevant tasks to external entities, prior to implementing such measures he or she shall require the installing technician(s) to supply a written description of the activities performed, by which it is certified that they are compliant with the provisions set out in these technical specifications (see point n. 25 of Technical Annex B to the Code on privacy, regarding the Minimum Security Measures);
- whoever fails to adopt the minimum measures in breach of the relevant obligations shall be punished by detention for up to two years or else by a fine of between €10,000 and €50,000.

Duration of Retention Period for Recorded Images

According to the principle of proportionality, even the temporary retention of recorded images must be proportionate to the degree of necessity and only for the necessary and pre-determined period of time, in light of the purposes to be reached.

Keeping recorded images must be limited to few hours or, as a maximum, to the 24 hours following the recording, unless special needs for an extended period of retainment are stated (for example, in relation to the closure of offices) or the Data Controller must comply with a specific request of the police or judicial authority.

Only in specific cases, according to particular technical needs (*i.e.*, transportation) or according to the particular risks implied by the activity carried out by the Data Controller (*i.e.*, banks) a longer period for the retention of the images is allowed: but in any case such period cannot be in excess of one week, starting from the date of the recording.

A more permanent or extended period of retention must be evaluated as exceptional and in any case must be related to a need deriving from an event which has already happened or from a concrete and incumbent risk, or from the need to retain and deliver the images to the police or judicial authority (but not in general: only if an inquiry is already under way).

The video surveillance system must be programmed in a way that – where possible form a technical point of view – at a certain moment, an automatic cancellation of the recorded images is carried out in order to make the cancelled images no longer re-usable.

Written Documentation of Choices Regarding Video Surveillance Systems Employed

The Data Controller must draft and retain a written (internal) document justifying the licit choices on which the installation of video surveillance systems is based. This document can also be presented in the occasion of eventual inspections or can be placed at the disposal of the data subjects exercising their rights.

Data Subjects' Rights

The general rules provided by Article 7 of the Italian Code on Privacy (Right to Access Personal Data and Other Rights) shall apply to data subjects exercising their rights with regard to the processing of personal data and images by means of video surveillance systems.

Consent and the "Principle of Balancing Interests"

Private Data Controllers can process personal data (and images) only if an express consent has been given by the data subject or if one of the hypothesis set forth in Article 24 of the Italian Code on Privacy (Cases in Which No Consent Is Required for Processing Data) shall apply.

The employment of video surveillance systems often makes it difficult in practice, to acquire the data subject's consent (both for the high number of personal images recorded and because it is almost impossible to contact the data subjects before the processing of the images). Therefore, if a video surveillance systems is employed for security reasons, it will be contradictory to request a specific consent from a subject entering certain places.

Further, the consent (beyond previous information) is valid only if express: an implied or unspoken consent, presumed for example, by the fact that the data subject has entered the place where video surveillance systems are installed and working, is illicit.

To resolve the problem, the Italian Data Protection Authority has deemed as a valid alternative to the express consent, the so-called "principle of balancing interests". Thus, the General Act on Video surveillance provides that the processing of images can in certain cases, also be carried out without the need for the data subjects' previous consent if such processing is in compliance with rules of the Act and it is necessary to pursue a legitimate interest of the Data Controller or of a third party (*i.e.*, to provide proof) or to protect individuals or goods with respect to possible thefts, robberies, acts of aggression, damages, acts of vandalism, or for the purposes of preventing fires or for employee and employer security.

Conclusion

In conclusion, the following points can be made. First, the Italian Data Protection Authority recalls the set of sanctions (administrative and criminal) already provided in general by the Italian Code on Privacy for the breach of the related rules: such sanctions shall also apply to the processing of images by means of video surveillance devices.

Secondly, the General Act on Video Surveillance of April 29, 2004 provides specific rules with regard to the employment of such systems in particular sectors:

- in the employment sector, providing specific guarantees for employees;
- in the health sector (video surveillance in hospitals);
- in schools, churches or cemeteries;
- in the Public sector (video surveillance to record the carrying out of institutional tasks); and

- in the urban sector (video surveillance systems monitoring the access of vehicles in historical centres of cities or for urban transportation security needs).

Finally, the Italian Data Protection Authority also recalls the specific, future adoption of the conduct and professional practice on Video surveillance, rules for which are now in draft. Article 12 of the Italian Code on Privacy already provides that the Italian Data Protection Authority shall:

- encourage, within the framework of the categories concerned and in conformity with the principle of representation, the drawing up of codes of conduct and professional practice for specific sectors;
- verify the compliance of such codes with laws and regulations, by also taking account of the considerations made by the entities concerned; and
- contribute to the adoption of, and compliance with such codes.

This should be done with regard to the guidelines set out in Council of Europe recommendations on the processing of personal data Compliance with the provisions included in the codes referred to above shall be a prerequisite for the processing of personal data by public and private entities in order to be lawful.

News

EUROPEAN UNION

Commission Moves Towards Mandatory Retention of Traffic Data

Traffic data is back on the European agenda and will be "one to watch" in the coming months. The European Commission is currently in the throes of an open public consultation (initially indicated by the Commission in its Communication of June 16, 2004, following calls from several Member States for legislation to increase communications data retention requirements. The ever-increasing use of electronic communications networks generates significant amounts of traffic data, which provides information and details relating to e-mail, SMS, faxes, telephony and other uses of the Internet. The United Kingdom, France, Ireland and Sweden submitted a draft Council Framework Decision in April 2004, calling for the implementation of measures designed to make retention of traffic data compulsory for a period of 12 to 36 months for the purposes of prevention, investigation and detection of crime and criminal offences including terrorism.

In the United Kingdom, ISPs and other electronic network providers can optionally retain communications, service and subscriber data for prescribed periods of up to a year under the industry-wide voluntary Code of Practice. This Code of Practice came into force on December 5, 2003 under the Anti-Terrorism, Crime and Security Act 2001. It was suggested that the voluntary Code would become compulsory after an initial two-year trial period. Additionally, the European Directive on Privacy and Electronic Communications (2002/58/EC) restricts retention by Member States of data for billing and payment purposes only (but under strict conditions), and provides a derogation which allows for the introduction of legislative measures for data retention for the purposes of counteracting criminal activity. The draft Council Framework Decision aims to expand the scope of this derogation to make traffic data retention compulsory and harmonise industry practice across Member States. The proposals have been given further impetus and urgency as a result of the recent terrorist activity in the European Union, such as the Madrid train bombings.

The possibility of mandatory retention of communications data, however, has sparked controversy with respect to citizens' fundamental rights and freedoms although the Commission recognises a need to achieve an appropriate and proportionate balance within a democratic society. Consequently, the Commission (on the initiative of Directorates-General for the Information Society and for Justice and Home Affairs) has recently issued a public consultation document which aims to gather opinions from relevant sectors and stakeholders. Calling for dialogue and an open and transparent debate, the document is complemented by a public workshop, which was held on September 21, 2004.

The target date for adoption of a measure is June 2005 with implementation at national level by mid-2007.

By Marie-Claire McCartney, a solicitor in the IT/IP and Communications Group of Hammonds, London; e-mail: marie-claire.mccartney@hammonds.com

UNITED STATES

FBI Acts Unconstitutionally in Obtaining Customer Data from ISPs

A New York court has held that the FBI's use of "National Security Letters" – a type of administrative sub-poena – to obtain information from Internet service providers (ISPs) about their customers is unconstitutional. The court described the procedure used by the FBI as "a unique form of administrative sub-poena cloaked in secrecy". Under the procedure – restrictions on which were relaxed by the controversial Patriot Act after September 11, 2001, – the FBI may compel communications companies such as ISPs or telephone companies, to produce customer records provided that the records are "relevant to an authorised investigation to protect against international terrorism or clandestine intelligence activities". The individual receiving the sub-poena is prohibited from ever disclosing that the FBI has issued it; it is unclear whether they are even allowed to obtain legal advice. The court ordered the U.S. Government not to issue such sub-poenas in the future and not to enforce the non-disclosure provisions. In view of the seriousness of the court's decision, the judgment was, however, stayed pending appeal.

The Decision was handed down on September 28, 2004 by U.S. District Judge Victor Marrero.

By Astrid Arnold, Lovells

  WDPR ISSN 1473-3579

UNITED STATES

Employee Use of Personal E-Accounts and Wireless Communications

Informal e-mail chatter over employees' own personal accounts that are accessed during the workday through company computers has the potential to be even more problematic than personal messages sent over corporate e-mail accounts, according to employment law experts interviewed by BNA.

Almost eight in 10 employers now have policies addressing employee e-mail, according to a survey released earlier this year by the American Management Association and the ePolicy Institute.

However, many have not spelled out that personal e-mail accessed on a work computer is retrievable, can be monitored, and if offensive, can be evidence in complaints and lawsuits, according to employment attorney Janice P. Brown of Brown Law Group in San Diego.

E-mail and instant messaging (IM) create enormous temptations for employees to say things they never would say to another person out loud, and that temptation is even higher when an employee is using his own personal account, Brown said.

Personal e-mail and IM accounts, along with text messaging over cell phones and PDAs (personal digital assistants), are the latest electronic communications techniques that can cause a host of workplace problems, from company exposure to computer viruses and worms to sexual harassment lawsuits. Often they are being brought into the workplace and used by employees without the employer's knowledge.

Jeffrey Plotkin, an attorney with Eiseman Levine Lehrhaupt & Kakoyiannis in New York City, told BNA that employers should make clear to employees that "there is no such thing as personal e-mail at work".

Personal Transactions Not Private

Nancy Flynn, executive director of the ePolicy Institute, agreed that employers need to address the issue of personal e-mail accounts. "You can't rely on your employees to behave in a 100 percent responsible and compliant way 100 percent of the time."

Flynn also cited results from the survey showing that 20 percent of employers had e-mail subpoenaed, up from only nine percent in 2001. "E-mail is the electronic equivalent of DNA evidence", she said.

Not only is the exposure there for the employer, but employees are also at risk from accessing personal accounts at work. If they pay a bill online or buy a share of IBM, that transaction is not private, said Michael R. Overly, partner in the e-business and information technology practice of the Los Angeles office of Foley & Lardner. Each page view, including passwords, is logged on the employer's system and can be retrieved, unprotected by the encryption required by providers like AOL or Yahoo.

Liability Depends on Awareness

Monitoring software can allow employers to keep tabs on employee use of personal e-mail accounts on company computers. However, employers may be better off not knowing what is being written in these personal messages.

Employers' liability for the activity of employees over private e-mail accounts on company computers may be limited if the company can prove it was unaware of the content. If, for example, an employee is circulating racist diatribes or sending and receiving pornography on his or her personal account, Overly said, "if [the employer] is unaware, the exposure is minimal".

"If alerted, they have to be concerned", he said. One indication of pornographic activity is the presence of large attachments on employee e-mails, he said, which monitoring software can easily detect.

If such activity is noticed and reported, the employer should act promptly, and tell the employee the activity has to stop, Overly advised. If child pornography is involved, the employer has a legal obligation to report it to law enforcement and should consult counsel immediately, he said.

Despite all the risk, attorneys contacted by BNA agreed that employers should not try to ban all personal use of company computers.

Flynn said that while employers may want to ban the use of personal e-mail accounts in the workplace, they should allow some personal use of corporate e-mail.

"American workers today put in more on-the-job hours than at any time in history", Flynn said. "For employees who leave the house before dawn and don't return until well past dark, e-mail may be the most efficient and effective way to stay in touch with family members. For the sake of employee morale and retention, … employers generally are willing to accommodate their employees' need to check in electronically with children and spouses."

Offsite Activity

Along with employee use of personal e-mail accounts in the workplace, another murky issue for employers is the question of how much liability an employer bears for employees' electronic communications that take place outside of work hours. For example, what if an employee e-mails a co-worker from home and makes sexist or racist comments about a third employee?

"It's a very thorny question", Plotkin said. "It's a conduct issue where what happens offsite has reverberations in the workplace".

The message to employees wanting to maintain the sanctity of their own computers, laptops, cell phones or PDAs should be not to use personal devices for business at all, according to Plotkin. To do so risks having personal electronic devices searched during litigation, he said.

The problem is that the line between work and off-work is dissolving, as employees shift effortlessly between personal and company business and from personal to corporate electronic devices, Overly said. "People are working longer hours, and they are working with their offices with them", he said, referring to employees who work outside their offices using a laptop, cell phone, or BlackBerry.

Instant Messaging, Wireless Technology

Most employers have not yet addressed new technology such as instant messaging, text messaging, or picture phones, according to the ePolicy Institute/AMA survey.

Overly said these areas are ripe to produce significant litigation in the next few years. He recommended making written policy generic enough to cover rapidly changing technology, by making it an "electronic communications" policy rather than an e-mail policy.

Wireless devices such as PDAs, cell phones, pagers, and wireless laptops are proliferating rapidly, he said. Employees can easily lose these devices, exposing the employer to loss of proprietary or customer information.

Employees also frequently "upgrade" their company laptops with wireless cards without telling the employer, which creates puts the company's security at risk.

Most Employers Do Not Monitor IM

The survey also reveals that IM is becoming a major workplace tool, whether employers like it or not. Still, 64 percent of companies do not monitor IM, the survey found.

Brown said she once retrieved one of her own employee's IM traffic and proved that the employee was spending about half her time chatting with friends. Brown pointed out that many younger employees have grown up in an IM-enabled era and have trouble seeing it as something that should be curtailed in the workplace.

Instant messaging is easier to monitor and control than wireless communications because it is cached in the same way as personal e-mails and remains on a computer for at least a month, Overly said.

Retrieving and monitoring wireless text messages is much more problematic, Overly said, since it is cached for only a very brief time on the device. Most often it comes to light in complaints when someone keeps or records it, he said.

Picture phones pose an even greater threat to employers, Overly said. Many employers have banned picture phones from the workplace because of fears of intellectual property theft, but that fear is overblown, Overly said. The picture quality is too poor for corporate espionage, he said.

One way to monitor this kind of abuse, as well as pornography activity, is to set up a system to track e-mails that have ".jpg" attachments, a flag for photographic material. "It's easy to install, and the potential harm it can prevent is substantial", he said.

For employees, Brown said: "The bottom line is, don't ever include any information or discussion in electronic communications that could eventually come back to haunt you. And any message has the potential to do that under the right circumstances".

She advises employers to develop, implement, and enforce a written, company-wide e-mail and Internet-use policy. Also, Brown said, employers need to spell out in the company policy their right to monitor employees' messages, including those sent from personal e-mail accounts on workplace computers.

Advantages and Disadvantages of Employee Monitoring

However, an employee rights advocate commented that monitoring often is unnecessary.

"To say that all monitoring is evil is a little too simplistic, but it ought to be done in a limited way to minimize the invasions of privacy", said Lewis Maltby, president of the National Workrights Institute in Princeton, N.J. "I can hardly think of a legitimate reason to read an employee's e-mail", he said, unless a co-worker has filed a complaint.

He added that some companies rely on a culture of trust rather than monitoring employees' e-mail to achieve their goals. "Some might say that all this electronic monitoring is just a crutch for poor management."

Overly said that if employees are aware that messages can be monitored, they are less likely to do anything to put the company at risk. "The object is not to catch someone doing something," Overly said. "It's to tell them what you're doing so it won't happen."

  WDPR ISSN 1473-3579