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 10 October 2004

## Articles



## Case Reports



## 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*

**Hong Kong** implemented its data protection legislation via the Personal Data (Privacy) Ordinance, which came into force in December 1996. Given that this was almost a decade ago, our article by Gabriela Kennedy and Katrina Partridge, reflecting on how Hong Kong's data protection regime has fared thus far is a timely one. The article focuses in particular on the evolving case law and guidance offered by the Privacy Commissioner. It also asks whether the Ordinance meets the demands of changing technologies.

As readers will know, we have followed the passage of France's new data protection legislation in *World Data Protection Report* and are pleased to include an article by Laurent Szuskin, Myria Saarinen and Jessica Magniez now that the new rules are in force (as of August 6, 2004). The new law modifies extensively, individual rights involved in the processing of personal data, and the obligations incumbent upon data controllers. It also strengthens the powers of the French Data Protection Authority.

The protection of one's identity, perhaps the "ultimate" personal data, is an important consideration in both personal and commercial transactions. Interestingly, a recent study by Michigan State University has shown that 70 percent of all identity-theft cases originate with information stolen in the workplace. Holly Towle provides us with a detailed article on Identity Theft in the United States on page 20.

Other commentaries in this issue come from Alexander del Ninno, who writes on Italy's new legislation on the processing of personal data and Christine Lyon, Laura Frederick and B. Scott Silverman of Morrison & Foerster report on the new privacy laws which have been enacted in California – a state which has once again pre-empted the introduction of federal regulations in this area.

Nichola J. Dawson

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

*Steve C. Bennett* and *Jonathan M. Redgrave,* Jones Day, New York and Washington, D.C.; *Ruth Hill Bro,* Baker & McKenzie, Chicago; *Rico Calleja,* Hammonds, London; *Margarida Couto* and *Cidália Neves,* Vieira de Almeida & Associados, Lisbon; *Tim Dixon,* Baker & McKenzie, Australia; *Laura Frederick, Christine E. Lyon* and *B. Scott Silverman,* Morrison & Foerster LLP; *Alejandra López Contreras,* Baker & McKenzie Abogados, Monterrey; *Gabriela Kennedy* and *Katrina Partridge,* Lovells, Hong Kong; *Alessandro del Ninno,* Studio Legale Tonucci, Rome; *Don McAleese,* Matheson Ormsby Prentice, Dublin; *Ilana Saltzman,* Baker & McKenzie, London; *Holly K Towle,* Preston Gates & Ellis LLP, Seattle; *Laurent Szuskin, Myria Saarinen* and *Jessica Magniez* and *Eric Andrews,* Latham & Watkins, Paris and Northern Virginia.

# Legislation & Guidance

## Hong Kong Data Protection Legislation: Attitudes and Law

*By Gabriela Kennedy and Katrina Partridge, Partner and Professional Support Lawyer, respectively, working in the Technology, Media and Telecoms group of Lovells in Hong Kong. The authors may be contacted at gabriela.kennedy@lovells.com or katrina.partridge@lovells.com.*

The Personal Data (Privacy) Ordinance (the "Ordinance") came into force in Hong Kong on December 20, 1996. Given the rapid approach of the "decade" marker it is perhaps timely to reflect on the way the data protection regime has fared in Hong Kong and analyse the case law that has evolved so far as well as the guidance offered by the Privacy Commissioner, and to ask whether the Ordinance meets the demands of changing technologies.

### Background

The Ordinance is based on the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1981), the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data issued by the Council of Europe (1981) and the European Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (1995), Directive 95/46/EC ("the European Directive").

One of the primary drivers behind the enactment of the Ordinance was the establishment of a data protection regime in Hong Kong that would ensure that data transferred to Hong Kong from Europe would receive adequate legal protection.

The Ordinance focuses primarily on information privacy (or the interest of the person in controlling the information held by others about him or her). Personal privacy *per se* is not covered by the Ordinance although recent Draft Guidelines issued under the Ordinance do touch on privacy issues such as freedom from surveillance and interception of one's communications.[1]

### Complaints under the Ordinance

One way of gauging whether a piece of legislation has been useful is to ascertain the general public's awareness of their rights, ease of access to complaint channels and rapid resolution of complaints.

Figures produced by the Office of the Privacy Commissioner ("the Privacy Commissioner") are telling. In 1996-7, the year prior to the Ordinance coming into effect, 2,423 enquiries and 52 complaints were received by the Commissioner. By 1997-8 this number increased to 13,551 enquiries and 253 complaints; 19,994 enquiries and 418 complaints in 1998-8; 15,557 enquiries and 568 complaints in 1999-2000; 21,174 enquiries and 789 complaints in 2000-1; 21,174 enquiries and 888 complaints in 2001-2; and 16,352 enquiries and 906 complaints in 2002-3.

Whilst some may argue that the increasing number of enquiries/complaints could be the result of widespread poor data management practices, others may perhaps (and fairly) surmise that increased public awareness may also be a direct cause of this increase.

It is interesting to compare the figures in Hong Kong with those in the United Kingdom. The United Kingdom Information Commissioner received 12,001 complaints in 2002-3 of which 91 complaints were brought to court.[2] What this comparison shows is not only that more complaints are brought in the United Kingdom (taking into account the lower population in Hong Kong) but also that there is more chance of a complaint being taken to court in the United Kingdom than in Hong Kong.

### To Whom Does the Ordinance Apply?

The Ordinance applies to data users, defined as persons who control the collection, holding, processing or use of personal data. Any business in Hong Kong is certain to be a data user since its employee records and customer records (where customers are individuals) consist of personal data which it controls. There are no registration requirements or notification requirements for data users in Hong Kong unlike in other jurisdictions (*e.g.*, the United Kingdom which has a registration requirement under the Data Protection Act 1998 ("the U.K. Act"). The Privacy Commissioner has the power to designate classes of data users to whom a notification requirement would apply. To date this power has not been exercised.

### What Does the Ordinance Require of Data Users?

#### Allow Access to Personal Data

The Ordinance requires a data user to provide a copy of personal data which it holds on an individual ("data subject") within 40 days of a data access request by the data subject and to correct such data within 40 days of a data correction request. Compliance with data access requests is subject to several exceptions and exemptions.

#### Limited use of Personal Data

The Ordinance specifically restricts the use of personal data for certain purposes, such as:

*Direct Marketing*

Where personal data are used for direct marketing purposes for the first time, the data user must inform the data subject that he has the right to require the data user to cease using such data for the purposes of direct marketing.

*Matching Procedures*

A matching procedure may not be carried out by a data user without the consent of each individual data subject or the Privacy Commissioner, or unless the procedure is otherwise authorised (*e.g.*, by a notice published by the Privacy Commissioner or by another Ordinance authorising a class of matching procedures).

A matching procedure is essentially the comparison by computer of personal data relating to ten or more individuals collected for certain purposes with personal data relating to the same individuals collected for different purposes in order to take adverse action against those individuals. For example, the comparison by computer of data provided to tax authorities with data provided to social security authorities in order to reduce social security payments would be a matching procedure if the data related to ten or more individuals.

*Transfer outside Hong Kong*

Although the relevant section of the Ordinance is not in force at the time of writing, when it comes into effect it will restrict the transfer of personal data to a place outside Hong Kong unless an exception applies. Exceptions to this rule include:

- where the relevant data subject has given consent to the transfer;
- where equivalent legislation is in force in the transferee jurisdiction; and
- where the data user takes precautions to ensure that the data will not be used in that jurisdiction in any manner which would contravene the Ordinance it if applied there. The Privacy Commissioner has published a form of agreement which can be adapted and entered into in order to ensure compliance with the latter exception.

### Compliance with the Data Protection Principles

The Ordinance is underpinned by six data protection principles ("DPPs"). Data users are required under the Ordinance to comply with the Data Protection Principles unless an exception applies. Breach of a DPP is not in itself an offence but a breach of a DPP may form the basis of a claim for damages and could give rise to a complaint to the Privacy Commissioner who may issue an enforcement notice (if the breach is sufficiently serious). In turn, the breach of an enforcement notice constitutes an offence. The six data protection principles are largely similar to the data protection principles in the Data Protection Act [U.K.] 1998.

## Data Protection Principles

A brief summary of the DPPs is offered below:

- DPP 1 relates to the purpose and manner of collection of personal data and requires that data should only be collected if they are necessary and not excessive for a lawful purpose directly related to an activity of the data user. Collection should take place by fair and lawful means. Where personal data are collected from the data subject he should be informed of: the purpose of collection; the classes of persons to whom they may be transferred; the right to, and practicalities of, access to the data; whether it is obligatory to supply the data and, if so, the consequences of not doing so.
- DPP 2 relates to the accuracy and duration of retention of Personal Data and imposes an obligation on data users to take all practicable steps to ensure that personal data are accurate and kept for no longer than necessary, having regard to the purpose for which they are to be used.
- DPP 3 relates to the use of Personal Data and requires that personal data should only be used for a purpose directly related to the purpose for which they were collected, unless the data subject expressly consents to another use.
- DPP 4 relates to security of Personal Data and requires data users to take all practicable steps to ensure that personal data are protected from unauthorised access, processing, erasure or other use.
- DPP5 relates to availability of information and requires data users to ensure that members of the public can ascertain its data protection policies, the kind of data which it holds and the purposes for which they are held.
- DPP6 relates to access to Personal Data and requires data users to allow access to their personal data as well as a right to data subjects to correct such data held about them.

## What is Personal Data?

The Ordinance applies only where personal data is collected and used by data subjects. "Personal data" is data relating to a living individual from which the identity of the individual can be ascertained and which is kept in a form which can be accessed or processed. Any investigation must therefore start with the question: "is the data which is the subject of the complaint 'personal data'?" If this question cannot be answered affirmatively then no obligations under the Ordinance arise.

The scope of "personal data" has been discussed in a Court of Appeal Case in Hong Kong in 2000 and in a ruling of the Privacy Commissioner in 2003.

The facts of *Eastweek Publishers Ltd & Another v. Privacy Commissioner for Personal Data* [2000] 2 HKLRD 83 make for interesting reading.

The complainant in the case had been photographed on a public street without her knowledge or consent by a photographer who worked for the variety magazine, *E*. The photograph formed part of an article that examined the fashion sense of Hong Kong women. The women who formed the focus of the article were all anonymous photographic subjects; their identity was not known at the time the article went to press. Unfortunately for the complainant, the article contained a series of unflattering photographs and critical comments about her fashion sense. She filed a complaint with the Privacy Commissioner for Personal Data under s.4 of the Ordinance which relates to the "fairness principle" of data collection under DPP 1(2)(b). The Commissioner found in the complainant's favour, *i.e.*, that there had been a breach of DPP1. Eastweek then applied for leave to seek judicial review of the matter. The application was dismissed at first instance. Eastweek appealed.

The Court of Appeal held that the essence of personal data collection was that the data user must be compiling personal information about an identified person or a person whom the

data user intended or sought to identify. The gathering of personal data about an anonymous subject does not constitute collection of personal data. The Court also held that the s.2 definition "representation of information …in any document" would cover a photograph. The fact that a photograph was capable of conveying the identity of its subject, did not make the act of taking the photograph an act of data collection if the photographer and his/her principals did not know and were not interested in ascertaining the identity of the subject.

The definition of "personal data" was also discussed in a ruling by the Privacy Commissioner (affirmed by an Administrative Appeals Board (AAB) decision) in 2003.[3] The complainant's case was that whenever he used his senior citizen concessionary pass through a railway ticket gate it activated a flashing light and a beeping sound thus alerting other passengers to the fact that he was over 65 years of age. The AAB noted that no identification was required of purchasers of the card and held that the signals only identified the type of card used and not the person using it. The Privacy Commissioner also held that the sound and light emitted were not in recorded form and therefore did not constitute "data", hence they did not constitute "personal data".[4]

The results of these Hong Kong cases are not particularly surprising.

Given that the Ordinance has taken inspiration from the European Directive and therefore has certain similarities with the U.K. Act, many in Hong Kong have followed with interest the discussion concerning the scope of "personal data" in the English Court of Appeal case of *Durant v. Financial Services Authority* [2003] EWCA Civ 1746.

The case arose in the context of a data access request. Data access requests may be used by data subjects as mere "fishing expeditions" when they are contemplating litigation or even after court proceedings are started, or after court proceedings are not successful (as was the case here).

In *Durant* the court adopted a narrow legislative interpretation of what amounts to personal data and held that personal data is information which strictly concerns that individual. A document which merely names the individual or discusses a transaction or issue in which the individual has been involved cannot constitute personal data.

The Court gave guidance on what is likely to be personal data. The emphasis is very much on identifying information which affects an individual's privacy (whether in his personal or family life, business or professional capacity).[5] First, the information needs to be biographical in a significant sense (*i.e.*, it should go beyond simply recording an individual's involvement in an event). Secondly, the information should have the individual as its focus (and not merely someone who is mentioned in passing).

If *Durant* is followed in Hong Kong the scope of the information which has to be provided in response to a subject access request could prove to be considerably narrower than in current market practice and may well reduce the use of the Ordinance as a "fishing expedition" in the context of litigation.

*Durant* makes it clear that data protection legislation is not to be used as a way of obtaining third party discovery with a view to litigation or for further investigation of a matter.

### Relevant Filing System and "Reasonably Retrievable"

In the *Durant* case, personal data in computerised form was given on request but data held on manual files was refused because the data did not constitute personal data as it was not considered to be held in a "relevant filing system". The court went on to explain when a manual file would be considered a "relevant filing system" but it is perhaps useful to note that in Hong Kong unlike in the United Kingdom, there is no distinction under the Ordinance between data held in automated systems and data held on manual files.

Under the Ordinance personal data has to be kept in a form which can be accessed and processed. What this means is that data should be "reasonably retrievable". At first glance, this could potentially provide someone who practices poor file management with the opportunity to claim that he falls outside the scope of the provision. It has been suggested by a number of commentators that in such a situation "reasonable" would be judged using an objective test which would not, therefore, entitle a data user to refuse data access just because he does not manage his files well.[6] The issue is yet to be tested in court.

## Cross-Border Transfers of Data

One of the most interesting questions for jurisdictions with data protection legislation in place concerns the cross-border transfer of data. The *raison d'étre* of the Ordinance appears to have been to enable the flow of data from Europe to Hong Kong, and re-assure Europe that data would be adequately protected whilst on Hong Kong shores. The re-assurance stopped here. It is interesting to note that the only provision under the Ordinance yet to come into force is section 33 which deals with the transfer of data from Hong Kong to other jurisdictions. The effect of this is that Hong Kong can now be perceived as a sieve through which European data can flow to countries where no data protection is in place, such as the mainland of China.

As the trend towards off-shore outsourcing continues, the issue of trans-border data flows will continue to receive increased attention at the international level.

The Privacy Commissioner stated in the past that one of the reasons why section 33 had not yet been brought into force was because the cross-border data flow provision would hamper trading between Hong Kong and its major business partners, China, Japan and the United States, which at the time did not have data protection legislation.

In May 2003, Japan passed a set of five bills (the Japanese Privacy Law) which concern the protection of personal data. The Japanese Privacy Law applies to the private sector.

Meanwhile, rumours have been circulating in China that the government is considering bringing in data protection legislation in the future.

Given developments in the region, it is possible that at last the Privacy Commissioner may be persuaded to bring section 33 of the Ordinance into force.

## Codes of Practice

The provisions of the Ordinance have been clarified in a number of Codes of Practice issued by the Privacy Commissioner. The Codes are not binding, yet failure to abide

by the provisions of a Code will weigh unfavourably against the data user concerned in any case brought before the Privacy Commissioner.

So far, the Privacy Commissioner has issued the following codes:

- Code of Practice on Identity Card Numbers and Other Personal identifiers ("the HKID Code");
- Code of Practice on Human Resource Management ("the HR Code");
- Code of Practice on Protection of Customer Information for Fixed and Mobile Service Operators ( jointly issued by the Consumer Council, ICAC, PCO and OFTA);
- The Code of Practice on Consumer Credit Data ("The Credit Code");
- the Guide to Personal Data Privacy and the Internet ("the Internet Guidelines").

### The HKID Code

The Code sets out permissible methods of collection of HKID card numbers to ensure the collection of the personal data is accurate and sets out guidelines for the storage and keeping of HKID card numbers.

### The HR Code

This Code provides practical guidance for those data users who handle personal data in the human resource function of an organisation or in specialist recruitment or redeployment positions, *i.e.*, people who deal with prospective, current and former employees. The Code provides guidance on the collection, holding, accuracy, use of and security of data subject access as well as corrections to personal data.

### Code of Practice on Protection of Customer Information for Fixed and Mobile Service Operators

This Code recognises that a large amount of personal data relating to individual customers is collected by mobile and fixed telecoms service operators. The Code outlines good practices to prevent unauthorized disclosure of data by staff and general guidance on standards and measures that operators should adopt to protect customer information.

### The Credit Code

On November 27, 1998 the Code of Practice on Consumer Credit Data (the "Credit Code") was introduced in order to provide practical guidance in the sharing and use of consumer credit data by credit providers through a credit reference agency. The Credit Code has had two amendments in 2002 and 2003 respectively and now includes rules on positive credit data sharing among credit providers.

### Internet Guidelines

Data users who carry on business via a website must heed the Internet Guidelines. The Internet Guidelines prohibit the use of web façades and require data users to have personal information collection statements posted on the website. The Internet Guidelines also address the use of click-trail information. The Office of the Privacy Commissioner has conducted spot checks of Hong Kong websites to ensure compliance with the Ordinance and the Internet Guidelines.

## Conclusion

The Ordinance has been in force for eight years and so far although the number of complaints brought before the Privacy Commissioner have been on the rise, only a handful of cases have been referred by him to the courts.[7] Many of the provisions of the Ordinance have yet to be interpreted by the courts.

A number of Codes of Practice and one guide have been issued by the Privacy Commissioner offering guidelines for the interpretation of provisions in the Ordinance. Of all these, the Code of Practice on Protection of Customer Information for Fixed and Mobile Service Operators and the Internet Guidelines address data protection in the context of particular technologies and means of communications. These however, remain guidelines.

By contrast, in Europe specific directives or regulations have been introduced to complement the E.U. Directive and to address the fact that data can nowadays be collected and processed with ease using a host of new technologies and means of communication. Such legislation include, the Telecommunications (Data Protection and Privacy) Regulations 1999 (as amended by the Telecommunications (Data Protection and Privacy) (Amendment) Regulations 2000), and the EU Directive 2002/58/EC on privacy and electronic communications.

In Hong Kong the provision on cross-border transfers of data is yet to be brought into force. It appears that Hong Kong may have some catching up to do.

1 Report on the Public Consultation in relation to the "Draft Code of Practice on Monitoring and Personal Data Privacy at Work" released on December 18, 2003 following a consultation paper issued nine months earlier. As a point of comparison see also the draft Workplace Surveillance Bill which has recently been released for public comment in NSW, Australia, by the New South Wales Attorney-General. The Draft Bill prohibits certain forms of covert surveillance unless such surveillance is conducted pursuant to a covert surveillance authority. Importantly for many employers, the Draft Bill introduces legislative restrictions on the ability for employers to monitor their employees' e-mail and internet use and restricts and regulates the blocking by employers of e-mails and Internet access of employees at work. In early October, California Governor Arnold Schwarzenegger vetoed a bill that would require employers to notify employees in writing if they planned to monitor workers' e-mail or other Internet use, stating that to allow the Bill would be to stifle business interests.

2 United Kingdom Information Commissioner, Annual Report, July 2004.

3 A ruling of the Privacy Commissioner affirmed by the Administrative Appeals Board. (6/01) PCO Annual Report 2000-1 at p.40.

4 See footnote 3.

5 There have been some recent concerns raised by the European Commission who have suggested that the United Kingdom's narrow interpretation of "personal data" may in fact not comply with the European Data Protection Directive. The Commission has indi-0cated that the Directive had a much broader intention.

6 Berthold, M The Annotated Ordinances of Hong Kong, Personal Data (Privacy) Ordinance, 1999 Butterworths, Asia

7 *Eastweek Publisher Ltd & Another v. Privacy Commissioner for Personal Data* [2000] 2 HKLRD 83 (Court of Appeal), *Jiang Enzhu and Lau Wai Hing* [2000] 1 HKLRD 121 (Court of First Instance), *Ng Shiu Hung v. Sai Kung District Officer* [2001] HKEC 473 (Court of First Instance) *Tsui Koon Wah v. Privacy Commissioner for Personal Data* [2004] 2 HKLRD 840 (Court of First Instance).

# United States: California Enacts Four New Privacy Laws

*By Laura Frederick, Christine E. Lyon and B. Scott Silverman, Morrison & Foerster LLP*

On September 28 and 29, 2004 Governor Arnold Schwarzenegger approved four laws further extending privacy protection in California. These laws address spyware, security obligations with respect to personal information, collection of medical information for direct marketing purposes, and protection of social security numbers.

## SB 1436: The Consumer Protection Against Computer Spyware Act

The Consumer Protection Against Computer Spyware Act ("CPACSA"), Senate Bill 1436, is the first regulation of spyware in California and one of the first such anti-spyware laws in the country. "Spyware" refers to computer programs that perform functions on a computer often without the owner's knowledge. Once introduced, spyware may disable or change security settings on the computer or monitor the user's keystrokes to obtain passwords, account numbers and many other types of information.

The CPACSA makes it illegal for anyone to install software on someone else's computer and wilfully or in a deliberately deceptive way to use it for wrongful purposes, including to modify settings, collect personal information or take control of the computer to send commercial e-mails or viruses. Critics of the law argue that it does not go far enough, as it requires wilful or intentionally deceptive actions to trigger any violations. Further, it does not prohibit spyware, but just requires notification to the consumer before spyware is installed. The CPACSA goes into effect on January 1, 2005.

Specifically, the CPACSA prohibits anyone other than an authorised user of a California resident's computer from causing computer software to be copied onto that computer and using the software in a way that is intentionally deceptive to:

- modify the homepage, search engine or bookmark settings;
- collect personally identifiable information, including through recording keystrokes and website visits;
- prevent unauthorised blocking of a consumer's reasonable efforts to block the installation or disable the software
- misrepresent that the software is uninstalled or disabled, when it is not; or
- remove, disable or render inoperative any security, anti-spyware or anti-virus software installed on the computer.[1]

The CPACSA also prohibits anyone other than an authorised user of a California resident's computer from wilfully causing computer software to be copied onto that computer and using that software to take control of the computer to:

- initiate commercial e-mail or computer viruses;
- damage another's computer;
- open advertisements that can't be closed without turning off the computer or turning off the Internet browser;
- modify the security settings for the purpose of stealing the information or causing damage to computers;
- prevent the user from blocking the installation of or disabling software.[2]

Additionally, the CPACSA prohibits anyone other than an authorised user from (1) inducing a consumer to install software on a computer by misrepresenting that the software is necessary for security or privacy reasons, or to open, view or play a particular content; or (2) deceptively copying or executing software on a computer to cause the consumer to use the software in a way that violates the CPACSA.[3] However, these sections of the CPACSA do not apply to telecommunication carriers, cable operators, providers of information services, hardware or software providers, or providers of computer services who monitor or interact with a subscriber's computer or Internet connection for purposes of security, diagnostics, technical support, repair, installation of authorised updates, authorised remote system management or detection of unauthorised use or fraudulent or illegal activities.[4]

## AB 1950: Security Requirements for Companies that Own or License Personal Information

Assembly Bill 1950 requires companies that own or license unencrypted personal information about California residents to "implement and maintain reasonable security procedures and practices" for that data.[5] The level of security required is not detailed, but rather must be "appropriate to the nature of the information to protect the personal information" from unauthorised access, destruction, use, modification or disclosure. "Personal information" includes an individual's name in combination with one or more of the following data elements, if either the name or data element is unencrypted or unredacted: Social Security number, driver's licence or California identification card number, account number in combination with any security code or password, and medical information. [6] This statute also takes effect on January 1, 2005.

In addition to maintaining adequate security procedures, companies subject to this law may only disclose such information to unaffiliated third parties who contractually agree to maintain reasonable security procedures.[7]

Businesses that comply with stricter privacy requirements imposed by other laws are deemed in compliance with this law.[8] These include health care providers covered by the Confidentiality of Medical Information Act, financial institutions subject to California Financial Information Privacy Act, entities covered by the medical privacy and security rules of Health Insurance Portability and Availability Act (HIPAA), entities subject to the confidentiality requirements of the Vehicle Code and any other business that is regulated by the state or federal government and subjected to greater protection of personal information that required under this law.

## SB 1633: Restrictions on Collection of Medical Information for Direct Marketing Purposes

Senate Bill 1633 prohibits businesses from making a direct request to an individual for medical information for direct marketing purposes without first clearly informing the individual that the business intends to use the information "to market or advertise products, good, or services", and obtaining the consent of the individual.[9] Oral disclosures and consents must be recorded and maintained for two years and written disclosures must include a written consent. The law does not apply to health care plans, insurance companies or agents, and certain telephone companies. SB 1633 takes effect on January 1, 2005.

## SB 1618: Restrictions on Displaying Social Security Numbers on Paychecks

Senate Bill 1618 amends the Labor Code to change requirements relating to information displayed on itemised wage statements. Existing law in California requires employers to display on each pay stub the name of the employee and social security number. The new law provides that, by January 1, 2008, employers shall display only the last four digits of an employee's social security number (or another employee identification number) on pay stubs or other checks, drafts or vouchers.[10]

1 California Business & Professions Code §22947.2.
2 Cal. Bus. & Prof. Code §22947.3.
3 Cal. Bus. & Prof. Code §22947.4.
4 Cal. Bus. & Prof. Code §22947.3(d), §22947.3(b).
5 California Civil Code §1798.81.5(b).
6 Cal. Civ. Code §1798.81.5(d)(1).
7 Cal. Civ. Code §1798.81.5(c).
8 Cal. Civ. Code §1798.81.5(b).
9 Cal. Civ. Code §1798.91.
10 Cal. Labor Code §226(a).

# United States: Proposed Amendments to the Federal Rules to Address E-Discovery Developments

*By Steve C. Bennett and Jonathan M. Redgrave, Partners with Jones Day in the New York and Washington, D.C. offices of the firm, respectively.*

Over the past several years, the Discovery Subcommittee of the Advisory Committee on Civil Rules of the U.S. Judicial Conference has been studying the impact of "electronic discovery" on litigation, as well as the adequacy of the current rules to handle disputes arising in the era of digital communications and documents. As a result of a number of conferences, the subcommittee recommended that the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States publish proposed rules for comments. The recommendation was adopted, and draft rules changes were published for public comment on August 9, 2004. The Report of the Civil Rules Advisory Committee (dated August 3, 2004) outlining the proposed rules and notes is available on the U.S. Courts website at *www.uscourts.gov/rules/comment2005/CVAug04.pdf*.

## Why Change the Rules?

The August 3, 2004 Memorandum from the Chair of the Advisory Committee on Civil Rules notes that the Committee spent five years examining whether the rules adequately accommodate discovery of information generated by, stored in, retrieved from, and exchanged through computers. Significantly, the memorandum noted that in the last few years,

> "electronic discovery has moved from an unusual activity encountered in large cases to a frequently-seen activity, used in an increasing proportion of the litigation filed in the federal courts".

The Committee identified several distinctive features of electronic documents that may warrant separate treatment in the rules:

- The exponentially greater volume that characterises electronic data that can make discovery more burdensome, costly, and time-consuming.
- Electronically stored information may exist in dynamic databases that do not correspond to hard-copy materials.
- Electronic information, unlike words on paper, is dynamic. The ordinary operation of computers – including the simple act of turning a computer on or off or accessing a particular file – can alter or destroy electronically stored information, and computer systems automatically discard or overwrite data as a part of their routine operation.
- Computers often automatically create information without the operator's direction or awareness, a feature with no direct counterpart in hard-copy materials.
- Electronically stored information may be "deleted" yet continue to exist, but in forms difficult to locate, retrieve, or search.
- Electronic data, unlike paper, may be incomprehensible when separated from the system that created it.

These differences can lead to increased costs and uncertainty as to how to treat electronic documents under the current rules and could result in inconsistent legal doctrine. In sum, the August 3 memorandum noted that "[i]f the rules do not change, they risk becoming increasingly removed from practice".

The Advisory Committee noted the increasing number of "local rules" (*i.e.*, rules in particular jurisdictions) addressing electronic discovery. Of course, as recognised by the Advisory Committee, local rules can be both a blessing and a burden – very beneficial for experiments to see how different standards

work in practice but formulating disparate practices between jurisdictions that, over time, may make a uniform national standard harder to implement.

## What are the Proposed Changes?

The Standing Committee on Rules of Procedure and Practice approved for publication proposed amendments to Civil Rules 16, 26, 33, 34, 37, and 45 dealing with the discovery of electronically stored information. There are seven distinct aspects to these proposed rule changes:

- "updating" the language in Rule 34 to reflect changes in technology that have made some of the language outdated;
- providing for explicit discussion of electronic discovery issues at the outset of litigation (Rules 16 and 26);
- creating a procedure whereby issues regarding the form of production are addressed early in the discovery process;
- providing a mechanism whereby interrogatory responses can refer to electronically stored information as well as business records (Rule 33);
- providing a general procedural mechanism whereby inadvertently produced privileged materials (including electronic data) are returned and establishing a process for any challenges to privilege claims;
- creating a two-tiered approach to electronic documents whereby discovery of documents or data that are not accessed in the ordinary course of business (or some other defined set of documents and data) are treated as subject to discovery only upon a showing of good cause; and
- establishing a "safe harbor" whereby the routine or automated deletion or destruction of certain data is not subject to sanction under Rule 37, provided certain conditions are met.

The first four propositions are not dramatic, nor are they expected to be particularly controversial. However, they are intended to be beneficial for the judiciary, bar, and parties by setting common expectations and understanding regarding the role of electronic discovery in civil litigation.

The fifth proposed modification – protecting privileges in the case of inadvertent productions – recognises that the sheer volume and the unique character of electronic information significantly increases the likelihood of inadvertent productions and sets forth a procedure that allows for the information to be quarantined or destroyed until a substantive decision regarding privilege, if necessary, can be made. This quarantine process does not address the impact on privileges in light of the Rules Enabling Act, which precludes use of the rules process to affect substantive laws governing privilege. Nonetheless, the proposal essentially codifies emerging best practices, which would benefit all parties.

The sixth proposed change is to Rule 26(b)(2) and builds on a two-tier structure of discovery scope suggested in Rule 26(b)(1), applying the structure to the burden of discovery of electronically stored information. In essence, a party must provide discovery of relevant reasonably accessible electronically stored information without a court order, but a party need not review or provide discovery of electronically stored information that it identifies as not reasonably accessible. If the requesting party moves for discovery of purportedly inaccessible information – the second tier – the responding party must show that the information sought is truly not reasonably accessible. The court would then balance the burden or expense of the proposed discovery against its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery, in resolving the issues as set forth in Rule 26(b)(2)(i), (ii), and (iii).

The seventh area is a proposed amendment to Rule 37 to provide a "safe harbor" to a party that fails to provide electronically stored information, under specified circumstances. In essence, the proposed amendment would protect a party from sanctions under the Civil Rules for failing to provide electronically stored information lost because of the routine operation of the party's computer system. The safe harbor would not apply if the party violated an order issued in the action requiring it to preserve electronically stored information, or if the party failed to take reasonable steps to preserve the information after it knew or should have known the information was discoverable in the action. As currently framed, the proposed amendment does not define the scope of a duty to preserve and does not address the loss of electronically stored information that may occur before an action is commenced.

The safe harbor is the most controversial and least settled proposal. Indeed, the Advisory Committee memorandum reflects the extensive debate on the issue and includes a reference to a possible alternative Rule 37(f) that frames an amendment in terms of intentional or reckless failure to preserve electronically stored information lost as a result of the ordinary operation of a party's computer system.

The Advisory Committee has invited comments on all aspects of the proposed amendments and has indicated certain areas in which comment will be particularly helpful, including:

- whether the proposed Rule 26(b)(2) and Note give sufficient guidance to litigants, lawyers, and judges on determining the proper limits of electronic discovery and on appropriate terms and conditions, including allocating the costs of such discovery.
- whether proposed Rule 37(f) and Note adequately and accurately describe the kind of automatic computer operations, such as recycling and overwriting, that should be covered by a "safe harbor".

There are also three public hearings scheduled to take testimony on the proposed amendments: January 12, 2005 in San Francisco; January 28, 2005 in Dallas; and February 11, 2005 in Washington, D.C.

Further information regarding the rules amendment process is available at *www.uscourts.gov/rules/submit.html*.

## Other E-Discovery Guidance

The case reporters across the country continue to reflect an increase in the number of cases where "e-discovery" issues have been addressed – either in terms of discovery or spoliation of evidence disputes. Unfortunately, but not unexpectedly, the myriad and disparate facts involved in these cases make it hard to discern patterns of guidance for parties

and litigants to follow. Fortunately, there have been some recent developments in 2004 that help to bridge the gap.

### August 2004 Amendments to ABA Civil Discovery Standards

At the August 2004 Annual Meeting of the American Bar Association, the Association considered and adopted recommended amendments to its Civil Discovery Standards addressing electronic discovery. The changes and summary documents explaining the modifications are published by the Litigation Section of the ABA at *www.abanet.org/litigation/documents/home.html*. The documents explain that while the 2004 amendments "are not intended to restate the law or replace existing court rules", they are designed to supplement existing rules and address practical aspects of electronic discovery not addressed by the rules.

### The Sedona Conference℠

The Sedona Conference℠ Working Group Addressing Electronic Document Retention and Production currently involves more than 120 participants, members, and observers who have contributed their talents and perspectives under the auspices of The Sedona Conference℠ to address leading-edge issues involving electronic document retention and production.

The Working Group's first publication, *The Sedona Principles for Document Production,* offers 14 principles and commentary to state a view of the law that should apply to the preservation and production of electronic documents in litigation. First published in Spring 2003, the document was revised and expanded in January 2004 to reflect new developments in the law. The document has been discussed at numerous legal seminars throughout the country and has been cited in articles and legal memoranda as well as in the recent decisions in *Zubulake v. UBS Warburg* ((S.D.N.Y.), see *World Data Protection Report*, May 2004).

In September 2004, the Working Group released its second major publication: The public comment draft of *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age*. This document addresses the complexities of managing information and records in the digital age, looking at the issues from the legal, records management, and information technology perspectives. The fifth of these proposed guidelines addresses the "legal hold" process for litigation. Comments are being taken until March 1, 2005, and a revised document will be published by Summer 2005. The document is a companion to *The Sedona Principles*.

The Working Group is looking at opportunities to address these same issues as they are impacted by a global economy. In Summer 2005, a Sedona Conference Working Group meeting will be convened in Cambridge, England to bring together lawyers, academics and corporate counsel from Europe and the United States to address these issues, and other similar meetings are planned for the future. One of the issues that will be addressed is the confluence of privacy concerns in Europe and the discovery contours in the United States.

### *Jones Day's E-Discovery Committee*

*In recent years, as businesses have increasingly come to rely on electronic documents (especially e-mail) to conduct their affairs, discovery of such e-documents has become an important issue in litigation. Indeed, several high-profile cases have shown that e-documents, and the e-discovery process, can have a significant impact on the course and outcome of litigation.*

*Jones Day lawyers have been dealing with e-discovery issues for years. Their experiences have established a valuable base on which to draw when e-discovery issues arise in – or in anticipation of – the next case. The firm formalised its commitment to this area by forming its E-Discovery Committee in 2000 to collect the experiences of lawyers throughout the firm and make the work product developed by those lawyers accessible.*

*Jones Day lawyers have been significantly involved in the discussion and debate regarding potential rules amendments in this area. Six members of the firm's E-Discovery Committee have been actively involved in The Sedona Conference℠ effort. Jonathan Redgrave (Washington) is the chair of the Working Group, Editor-in-Chief of The Sedona Principles, and also one of the Editors-in-Chief of The Sedona Guidelines. Other Jones Day lawyers participating in The Sedona Conference℠ Working Group include Sharon Alexander (Dallas), Steven Bennett (New York), Laura Ellsworth (Pittsburgh) (one of the Managing Editors for the 2004 Annotated Sedona Principles), Jeffrey Joyce (Dallas) (a contributing editor for the 2004 Annotated Sedona Principles), and Ted Hiser (Cleveland) (a Senior Editor for The Sedona Principles).*

*The views expressed in this article are solely those of the authors and do not reflect the view or position of the firm or any of its clients.*

# Case Report

## UNITED KINGDOM

### Text Message Marketing: Opportunity to Opt-Out

Another ruling from the ASA suggests that the Authority may not be on the same wavelength as the Information Commissioner when it comes to the application of rules based on the e-Privacy Directive (2002/58/EC). The ASA adjudication was given on July 28, 2004 in what is in danger of becoming a real problem area for direct marketers – mobile text messaging.

### The Adjudication: O2

The ruling related to a promotional text message sent to an O2 customer that stated "Get sport alerts & more. Text ACTIVE to 2020 2 set up, then go 2 Info services 2 subscribe 2 alerts. Terms@o2.co.uk. Each alert from 13p to receive". The customer complained that the text message did not

include an opportunity to opt-out of receiving further marketing text messages.

In their defence, O2 said that their current practice required customers to give explicit consent to receive electronic marketing communications when they took up a contract, and that the terms and conditions of the service told customers how to opt-out of receiving marketing text messages. O2 referred to the Information Commissioner's guidelines on the e-Privacy regulations, which state that electronic marketing communications can be sent provided that customers fully appreciated what they were consenting to when they opted-in to receive them. O2 argued that, as an existing customer, they already had the complainant's consent to send marketing in any form, including text messages. They argued that, because the complainant had given permission for them to send marketing communications, they did not need to provide an embedded opt-out or unsubscribe option in every text message.

The ASA rejected O2's explanation. It noted that the complainant's contract was signed in 1998, with BT Cellnet, and that consent to receive marketing communications had been given. However, the complainant would not have been able to opt-in to receive marketing text messages, because at that time there was no such thing. The Authority noted that the complainant had not opted-in to receive marketing by text message when she became a customer or subsequently when text message marketing became established. Whilst it acknowledged that O2 had obtained consent to send marketing communications, because they had not obtained explicit consent to send them by text message, the Authority concluded that the complainant should have been told she had the opportunity to opt-out in every text message.

### Comment

O2 can feel aggrieved by the ASA's decision, if not a little confused. The Committee of Advertising Practice Help Note on Mobile Marketing states that mobile marketers who have themselves obtained explicit consent from consumers need not tell them in every message that they can opt-out of or unsubscribe from having their data used for direct marketing purposes, as long as each message contains the identity of the marketer and a valid address (for example, a web address or text-back channel that allows consumers to send opt-out requests and access the full address).

It would appear, therefore, that the ASA felt that the complainant's consent to receive marketing communications given when she joined up with BT Cellnet was not explicit enough and O2 did not have the option of merely providing a text-back channel.

Unfortunately, the latest version of the Information Commissioner's guidance on the e-Privacy Regulations is not entirely consistent with the CAP guidance on text messaging. The Information Commissioner says that provided the recipient has "clearly consented" to the receipt of messages, each message will have to identify the sender and provide a valid suppression address. It is at least arguable that the Information Commissioner would accept that O2 had, in the circumstances, clear, as opposed to explicit, consent.

The two regulators also appear to have a different approach to the requirement that a valid address must be provided in each message. Originally, the Information Commissioner took the view that only a postal or e-mail address would be valid. However, he has taken on board the impracticalities of opting-out by formal letter and is now prepared to allow the use of short codes as a valid address provided the sender is clearly identified in the message, e.g. "PJLtd". If a short code is used as a valid address, the Information Commissioner suggests that the following format is used: "PJLtd2STOPMGSTXT'STOP'TO (then add 5 digit short code)". The ASA, on the other hand, whilst adopting similar wording for marketing text messages to existing customers where explicit consent has not been obtained, appears to be satisfied with a text-back channel where explicit consent has been given. No format as such is prescribed by the ASA beyond the inclusion of the identity of the text marketer.

Marketers would be wise not to try to play one regulator off against the other. Being seen to be doing the right thing, that is by providing an easy way to opt-out in all cases, appears to be the best option.

*By Rico Calleja, Commercial & IP Department, Hammonds, London.*

# News

## AUSTRALIA

### Review of the Privacy Act

Various provisions of the Australian Privacy Act 1998 ("the Act") regulate the handling of personal information by private sector organisations. The Australian Attorney General has requested that the Federal Privacy Commissioner review the operation of the private sector provisions of the Act, to consider their effectiveness in both protecting the privacy of consumers and facilitating the free flow of information required for businesses to operate efficiently.

The Attorney General has published terms of reference for the review, which will consider to what extent the private sector provisions of the Act have succeeded in:

- establishing a single comprehensive national scheme that regulates the collection, storage, use, correction, disclosure and transfer of personal information by private sector organisations; and
- achieving this in a way that (i) meets Australia's international obligations relating to privacy, (ii) recognises the interests of individuals in protecting their privacy and (iii) recognises important human rights and social interests that compete with privacy.

The Attorney General has asked the Commissioner to complete the review and deliver her report by March 31, 2005.

The Office of Federal Privacy Commissioner has recently been taken on by Karen Curtis, replacing the previous Commissioner, Malcolm Crompton. In comments made since taking office, Ms Curtis indicated that she may take a softer approach to enforcement than her predecessor, which has worried some privacy advocates, who want to see stricter enforcement of the Act.

*By Tim Dixon, a Partner with Baker & McKenzie, Australia; e-mail: Tim.Dixon@bakernet.com*

# IRELAND

## Data Protection Commissioner Issues Four New Guidance Notes

Following on from the publication by the Data Protection Commissioner of his Guidance Note of July 5, 2004 on the interpretation of what is deemed to constitute "personal data" and what is to be regarded as a "relevant filing system" under the Data Protection Acts 1988 and 2003, the Data Protection Commissioner has published four further Guidance Notes in September 2004.

These Guidance Notes which are available at *www.dataprivacy.ie/7.htm* cover the following topics:

- the contents and use of privacy statements on websites;
- monitoring of staff;
- data protection access requests for personnel records;
- getting organised for data protection.

*By Don McAleese, Partner and Head of Information Technology Law Group, Matheson Ormsby Prentice, Dublin.*

# JERSEY

## Draft Data Protection Law Approved

The draft Data Protection Law was approved by the States of Jersey on June 30, 2004. Once in force, the new Law will implement the European Directive on data protection which affects the free movement of information and freedom to trade as well as the freedom of individuals.

The new Law will repeal the existing Data Protection (Jersey) Law 1987 which has rapidly become outdated because of dramatic developments in information and communication technology in recent years. Drafting the Law has involved a long consultation process involving both the private and public sectors.

Finance and Economics Committee Vice President Senator Philip Ozouf said: "This is a very big and important piece of legislation. It has implications for all businesses and data users and it also provides important safeguards for the use of personal information, which has implications for everyone in the community".

Senator Ozouf went on: "By harmonising local law with European Law, we will enhance Jersey's reputation as a highly reputable and safe jurisdiction with which to do business and Island residents will enjoy important protection of their personal information. This is a very important step for the Island and it will help us to maintain our global reputation for sound ethical practice and solid reliability".

Jersey and the other Crown Dependencies have based their local legislation on the U.K. Data Protection Act 1998. Therefore, those individuals and organisations who deal with the other Islands or the United Kingdom will already be familiar with the Law's requirements.

The prime purpose of the new Data Protection Law is:

- to safeguard the rights of individuals with regard to their personal information which may be held, stored or processed about them;
- to establish legally enforceable criteria that must be met before any holding or processing of personal information can commence;
- to ensure that organisations and individuals holding or processing such information notify with the Data Protection Authority, declaring the purposes for which the information is being held or processed, to whom it will be disclosed and the security measures to be applied;
- to ensure that organisations and individuals hold and process personal information that is accurate, up-to-date and only used for the purposes that are described in their notification details to the Data Protection Authority;
- to establish a supervisory authority that can act with independence in exercising the statutory powers entrusted to them by Law.

Data Protection Registrar Emma Martins said: "The Data Protection office will work hard to prepare for the transition as well as support and assist those organisations that need to comply with the new Law. I hope that we will see the appointed day act before the end of the year".

# MEXICO

## A New Public Registry Will Allow Net Users to Opt-Out from Spam

A recent study published by the International Data Corporation ("IDC") on September 1, estimated that unsolicited e-mail messages or "spam" now accounts for 38 percent of the e-mail messages sent in the United States this year – an increase of two percent on 2003 figures.

The distribution of unsolicited e-mail messages, which are usually of a commercial nature and often fraudulent and offensive, are sent to thousands of net users every day. Spam wastes users' time, as well as the resources of the net, and not surprisingly many companies are implementing software to block it.

The U.S. Congress recently published the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003", or "CAN-SPAM Act", which regulates the reception of these types of messages and the liability of the sender. However, eight months after its implementation, the problem continues to grow.

Mexico is making its first attempts to regulate unsolicited information.

The use of databases, including personal information, is currently regulated in Mexico by article 109 of the Federal Copyright Law. Access to personal data about individuals which is contained in databases, as well as the publication, reproduction, disclosure, public communication, and transmission of such information, requires prior authorisation by the people in question.

From November 4, 2004, when recent amendments to the Federal Consumer Protection Law (or the "LFC", according to its Spanish initials) comes into effect, a public registry of

  WDPR ISSN 1473-3579

consumers ("PRC") will be created. Any interested party may ask to be included, so that his or her information cannot be used for marketing or advertising purposes.

For the purposes of the LFC, marketing or advertising purposes means the offering and promotion of goods, products, or services to consumers, and thus, it will be prohibited to send advertisements to consumers who expressly state they do not want to receive such advertisements or to those who are included in the PRC.

While it is true that the LFC refers to all kinds of information, it is not difficult to imagine the application of these provisions to unsolicited e-mail messages.

Consumers may file a form with the Federal Consumer Protection Agency ("FCPA"), either in writing or via e-mail, requesting registration in the PRC. They may also file a complaint for violations committed by providers or companies that use information pertaining to persons included in the PRC.

The FCPA will have the power to demand providers cease to provide any information or advertising which violates the provisions of the LFC and, as appropriate, the media disseminating it. The FCPA may also impose penalty fines ranging from $300.00 to $960,000.00 pesos, or in the case of repeated offences, impose fines of double this amount.

Advertising sent to consumers must indicate the name, address, telephone, or e-mail address of the provider or of the company that is sending the advertisements on behalf of the provider, as well as information on the FCPA.

In this way, consumers who do not wish to receive unwanted information have the right to register with the PRC. On the other hand, providers or companies should pay special attention to ensure that they comply with the provisions of the LFC.

*By Alejandra López Contreras, Baker & McKenzie Abogados, Monterrey; e-mail: alejandra.lopez-contreras@bakernet.com.*

# TAIWAN

## Government Proposes Tougher Data Protection Laws

According to a recent report in the *Taipei Times*, the Taiwanese Cabinet has approved a new draft law on data protection which is primarily aimed at entrusting local governments with the responsibility of implementing the data protection law. The need for this law has come about following recent scandals in which civil servants and employees of private companies were found to have illegally leaked personal information in return for bribes.

The newspaper reports that in May 2004, the Kaohsiung District Prosecutor's Office brought criminal charges against a number of civil servants and civilians, alleging that they had leaked large quantities of personal information (including home and mobile telephone numbers, car registrations and bank account details) to crime syndicates in return for bribes. The defendants included law enforcement officers, coast guard examiners, and employees of telecommunications companies.

In an effort to prevent a recurrence of this case, Premier Yu Shyi-kun ordered government agencies to take measures to toughen laws protecting personal information, which involved revisions to the Computer-Processed Personal Data Protection Law. Subsequently the measures that have been adopted in the draft law include extending the scope of the statute to personal data held manually, as the statute currently only applies to data held electronically (*i.e.*, on computers).

The penalties for unlawfully releasing personal information for commercial gain have been increased, longer jail terms have been created and greater fines for infringers.

*By Tim Dixon, a Partner with Baker & McKenzie, Australia; e-mail: Tim.Dixon@bakernet.com*

# UNITED KINGDOM

## Code of Practice Introduced for the Use of Passive Location Services

An industry working group, comprising mobile network operators and location service providers (LSPs), developed principles of good practice for the provision of passive location services. These principles were introduced on September 24, 2004 in the form of a Code of Practice.

### Background

Passive location services are defined as "those services where a mobile phone user, once s/he has enabled the service, consents to be located by another, when that other person initiates a location request (either from another mobile phone or from a PC)".

The Code is not a substitute for the law, but aims to provide a more detailed framework within the law, setting out principles and procedures that should be followed by all LSPs. Applicable legislation in this area is the Data Protection Act 1998 as well as the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426). The Regulations (which came into force on December 11, 2003) require that the locatee (the person being located in a passive location service) must have given his or her prior consent to the operation of the service, and must be able to withdraw that consent at any time.

### Code of Practice

The Code covers four types of passive location services:

- child location services;
- friend location services;
- mobile games supported by location services;
- corporate location services.

The following general principles are introduced and apply to any type of passive location service:

- Location services must be consent-based and simple for consumers to understand and use with confidence.
- Where practical, in the interests of simplicity, recommended industry standard text should be used for obtaining consents, sending alerts and stopping or suspending services.

- Location services should not be used to undermine customer privacy and, in particular, should not be used for any form of unauthorised surveillance.
- Alert messages should be sent at random to guard against consumers being located without their knowledge.
- Location services should be easy to stop or suspend.
- Advice on how to use location services and key safety messages should be readily at hand.

The core consideration underpinning the Code is the need to strike a balance between privacy and safety. Thus the requirement for the consent of the locatee is central, and the Code provides details as to how this consent should be obtained so as to ensure its authenticity. This is coupled with additional guarantees in the form of random alerts to the locatee's mobile phone with a reminder that the location of the phone can be identified (while the service is switched on). In addition the Code introduces safeguards in relation to the valid identification of the locator, and the confirmation of the relationship between the locator and the locatee. Some of the services are made available only to users of a minimum age (typically 18). The consent of children below the age of 16 should be provided by the parent/guardian as well as by the child. The service should not be until the LSP has received the authenticated consent of the locatee.

In the context of child location service, the Code introduces marketing rules, requiring that such services should not be marketed in a way which exploits parents' concern or fear that their child may become a victim of crime, taking account of the fact that knowing the location of the phone does not necessarily confirm the location of the child, or whether the child is safe. A standard statement to this effect, agreed by industry, should be included in all marketing communications by LSPs.

*By Ilana Saltzman, a Partner with Baker & McKenzie, London; e-mail: Ilana.Saltzman@bakernet.com*

# UNITED STATES

## Actions for Violation of U.S. National Do Not Call Registry

The U.S. National Do Not Call Registry ("Registry"), which came into effect in October 2003, was created by amending the Telemarketing Sales Rule ("TSR"). The Registry enables consumers to opt-out of receiving unsolicited marketing telephone calls by registering their telephone numbers with the Registry. Both the Federal Trade Commission ("FTC") and the Federal Communications Commission ("FCC") have been active in enforcing the new rules, as evidenced by two recent cases.

## FTC Takes Action against Braglia Marketing Group

On August 30, 2004, the Department of Justice, at the request of the FTC, filed a complaint in the U.S. District Court for the District of Nevada against Braglia Marketing Group, LLC ("Braglia") claiming violation of the Registry requirements in the TSR. The FTC is seeking monetary civil penalties, a permanent injunction, and other equitable relief in relation to the alleged violation. This is the first time that the FTC has sought civil damages in connection with the Registry. A violation of the TSR constitutes an "unfair or deceptive act or practice in or affecting commerce" in contravention of section 5 of the FTC Act.

The FTC alleges that Braglia made more than 300,000 marketing calls to consumers whose phone numbers were on the Registry, thus violating the TSR. In addition, the FTC claims that Braglia made over 10,000 calls to phone numbers without paying the annual access fees applicable to those numbers. Finally, the FTC has charged Braglia with abandoning calls to consumers by failing to connect the individuals to a representative within the prescribed 2-second limit of the call being answered.

## FCC Settles with Primus Telecommunications

On September 7, 2004, the FCC released a consent decree with Primus Telecommunications, Inc. ("Primus") in relation to the FCC's investigation into the company's potential non-compliance with the Registry requirements. The investigation, which was launched in December 2003, concerned Primus' solicitation of customers in relation to its international long-distance services. Primus had hired Spanco Telesystems & Solutions Ltd, an entity based in India, to conduct the telemarketing on its behalf.

Under the terms of the consent decree, which terminates the FCC's investigation, Primus has agreed to adopt a comprehensive telemarketing compliance program, including:

- adopting written policies and procedures in a telemarketing compliance manual;
- providing its telemarketing compliance manual to employees and telemarketing companies;
- training employees involved in telemarketing campaign management;
- including appropriate provisions in contracts with telemarketing companies; and
- implementing procedures to audit compliance with the do-not-call rules.

In addition, Primus has agreed to make a voluntary U.S$400,000 contribution to the Treasury as part of the settlement.

*By Ruth Hill Bro, a Partner with Baker & McKenzie, Chicago; e-mail: Ruth.Hill.Bro@bakernet.com*

# Personal Data

## France: The Protection of Individuals with Regard to the Processing of Personal Data

*By Laurent Szuskin, Myria Saarinen and Jessica Magniez, Latham & Watkins, Paris, with the assistance of Eric Andrews, Latham & Watkins, Northern Virginia, for review of the English translation.*

The new law 2004-182 of August 6, 2004[1] has come into force. It modifies the law of 1978 on computerised data, files and civil liberties by, among other things, enhancing the protections for individuals with regard to the processing of their personal data. It implements, almost six years late, the "personal data" Directive 95/46/EC of October 24, 1995 (the "Directive"). On July 29, 2004, the Constitutional Council to which this text was referred, rendered a decision that invalidated only one of the five provisions that had been referred to it.[2] The original 1978 law was retained for symbolic reasons; however, the structure and terminology of that law were updated to make it consistent with the Directive and France's rapidly changing information society. We will endeavour here to present some of the main provisions of the new law.[3]

### Material and Geographical Scope of Application

This law applies to the automated processing of personal data – as these terms are defined by the law – as well as non-automated processing of data which form part of a filing system or are intended to form part of a filing system, with the exception of processing in the course of a purely personal activity. It applies to processing for which the data controller is established on French territory, and to processing for which the data controller, without being established on French territory or on the territory of another Member State of the EC uses processing means located in French territory. Nevertheless, excluded from this perimeter are processing used only in transit through French territory or through that of another Member State.

### The CNIL: Changed Procedures and Reinforced Powers

#### Notifications, Authorisations or Exemption from Prior Formalities

The new law abandons the distinction between public and private processing and requires data controllers to provide prior notification of the processing to the CNIL. This notification must include a commitment that the processing will be conducted in accordance with the law's requirements. With respect to certain common types of processing that are not likely to adversely affect private life or civil liberties (as determined by the CNIL), the data controller is entitled to register a "simplified" notification with the CNIL. Some categories of processing are exempted from any prior formality, even though they may, in certain cases, involve sensitive data. The maximum penalties for failure to comply with prior formalities, provided for in Article 226-16 of the Criminal Code, has been increased from three years' imprisonment and a fine of €45,000, to five years' imprisonment and a fine of €300,000.

Nevertheless, the law provides for several limited categories of processing which, since they are likely to involve specific risks with regard to rights and liberties, require prior authorisation from the CNIL. Amongst them are automated processing which create an interconnection between files which have different purposes.

#### Exemption from the Requirement of Prior Formalities

*Appointment of a "Personal Data Protection Official"*

The new law allows data controllers to appoint "a personal data protection official". This position, provided for in the Directive and already in existence in several European countries, is a major innovation in France.

It means that a data collector may be exempted from certain notification formalities by appointing an official who has certain requisite qualifications and who is authorised to act independently to ensure compliance with law. Under this system, data controllers can avoid the CNIL notification requirements by appointing an official with the qualifications and authority described above. It is important to note that the designation of a data protection official only excuses data controllers from notification requirements and this excuse does not extend to any other legal obligations required for the processing. For example, the appointment of a data protection official will not excuse a data controller if prior *authorisation* from the CNIL is required. It should also be noted that this streamlining of procedure does not apply if transfer of data to a state that is not a member of the EC is envisaged.

#### New Investigative and Penalty Powers

The new law extends and reinforces the CNIL's investigative powers allowing CNIL members to make on-site visits and conduct investigations. They may require the production of any useful information and documents, obtain copies thereof, access computer programs and data, and obtain a transcription as necessary.

Henceforth the CNIL has administrative sanction powers, ranging from formal notice being served to the data controllers requiring an immediate halt to any illegal conduct, to an injunction to halt processing. In addition, the CNIL may impose monetary sanctions. These sanctions are to be levied in proportion to the seriousness of the offence, and range up to €150,000, or even €300,000 in case of a repeated offence (in case of a corporate data controller, five percent of pre-tax turnover for the last completed financial year, up to a limit of

€300,000). In urgent cases, where the use of data processing or the use of the processed data leads to a violation of rights and liberties, the CNIL may go as far as stopping the processing in question or blocking certain data, in each case for a maximum period of three months. Decisions pronouncing a sanction may appealed to the State Council.

The new law also creates an offence of hindering the action of the CNIL, punishable by one year's imprisonment and a fine of €15,000.

## Basic Rules: New Obligations, Rights and Exceptions

The new law substantially modifies basic rules affecting the conditions of lawful processing, the obligations upon the data controller, the rights of the data subject and the exceptions to these rules. In order to keep this text sufficiently brief, exceptions to some principles are detailed in the appendix.

Data processing and particularly data collection must be carried out in a fair and lawful manner. Any collection of data must be made for predetermined, explicit and legitimate purposes. Personal data thus collected must be adequate, relevant and not excessive in view of the purposes for which it is being collected.

### Obligations Incumbent upon Data Controllers

Obtaining the Data Subject's Consent

The new law is innovative in that it sets forth, as a condition of lawful processing, that the processing must receive the consent of the data subject, *or* that meet,

"one of the following conditions:

- compliance with a legal obligation incumbent upon the data controller;
- safeguard of the life of the data subject;
- performance of a mission of public service to be carried out by the data controller or the person for whom the data processing is intended;
- performance either of a contract to which the data subject is a party or pre-contractual measures taken at the request of the latter;
- performance of the legitimate interests of the data controller or the person for whom the data processing is intended, subject to not violating the interests or rights and fundamental liberties of the data subject".

While the final exception is potentially very broad, its meaning is not well defined and data controllers should be careful about placing too much reliance on it.

*Obligation of Informing the Data Subject*

This requirement existed already under the previous drafting of the law, and it is retained and extended in the new law. The person from whom personal data is collected must now be informed by the data controller. This notification must include:

- the identity of the data controller;
- the identity of its representative, where applicable;
- the intended purpose of the processing;
- the obligatory or optional nature of replies;
- the possible consequences, with regard to the data subject, of any failure to reply;
- the addressees or categories of addressees of the data;
- the person's rights to oppose, access and rectify data, by virtue of law; and finally
- where applicable, the intended transfer of data to a country that is not a member of the EC.

Moreover, anyone using electronic communications networks must be informed clearly and fully by the data controller, or its representative, of:

- the reason behind any action to access, by means of electronic transmission, information stored in the data subject's connection terminal equipment or any action to enter, by the same means, information into his/her connection terminal equipment; and
- the means the data subject has available to make opposition to such action.

### Data Subjects' Rights

*The Right to Object*

The principle remains that all private individuals have the right to object, if they can justify legitimate grounds, to the processing of personal data concerning them. The law now provides for an exception to the requirement for legitimate grounds. Any private individual may now object, *at no cost and without having to justify any legitimate grounds*, to the use of data concerning them for the purposes of *prospecting, specifically of a commercial nature,* by the data controller or any further data controller.

### The Right of Control over Processed Personal Data

*Access, Communication and Rectification*

Under the law, the right to access data is maintained and explained more fully. The law provides that any private individual may ask the data controller to confirm whether the personal data concerning him or her is or is not to be processed. In addition, the data subject has a right to receive a copy of his or her data. The individual may also obtain information as to:

- the end-purposes of such processing;
- the categories of data processed;
- the addressees or categories of addressees of the parties to whom the data will be communicated; and
- information relating to any intended transfer of data to a country that is not a member of the EC.

The right to rectification allows any private individual who can prove his identity, to have his or her data rectified, completed, updated, erased and now, as provided for in the Directive, blocked whenever those data are inexact, incomplete, equivocal, out of date, or where the collection, usage, communication or conservation of those data is forbidden.

### Management of Data Transfers to Third Countries

Taking account of the need for guarantees as to the security of cross-border flows, the legislator has introduced provisions for the management of data transfers to countries that do not belong to the EC.

Such transfer is not possible unless the country to which the transfer is planned ensures an adequate level of protection of the private life, civil liberties and fundamental rights of individuals, in terms of the processing to be carried out, or which may be carried out, of the data. It is for the European Commission to define, using a range of indices, whether the level of protection offered by the country is adequate. In making this determination, the European Commission will consider measures in force in the said country, security measures used there, specific characteristics of the processing in question, such as its purpose and duration, the type, origin or destination of the data being processed.

Transfer to a country that does not meet these requirements may nevertheless be made possible if the person concerned has consented to the said transfer, or if the transfer is,

"necessary for one of the following reasons:

- safeguarding of the life of the data subject;
- safeguarding of the public interest;
- compliance with obligation for the establishment;
- exercise or defence of legal claims;
- consultation, under normal conditions, of a public register which, by virtue of legislative or statutory provisions is intended to inform the public and is open for consultation by the public or by any person who can demonstrate a legitimate interest;
- the performance of a contract between data controller and the data subject, or of pre-contractual measures taken at the request of the latter; or
- the conclusion or performance of a contract signed or to be signed in the interest of data subject, between the data controller and a third party".

Moreover, an exception may be made to the ban on transferring data to the country in question if the CNIL decides that the data collector can guarantee an adequate level of protection of the private life, civil liberties and fundamental rights of individuals, particularly due to contractual clauses or internal rules to which it is subject.

## Transitional Provisions

The law is effective immediately. Nevertheless, data controllers, whose processing predated the enactment of the law and complied with the then applicable legal provisions, have a period of three years, counting from the date of this publication, within which to ensure that their processing complies with the provisions of the new law. If compliance does not result in any changes in terms of the previous situation, then the said processing is deemed to have met the requirements of prior formalities. Previous provisions remain applicable until processing is made compliant and, at the latest, until expiry of the three-year time limit.

Notwithstanding the above, some provisions are to be immediately applicable to processing:

- the provisions regarding the right to object;
- the rules relating to the powers of the CNIL to check on implementation of processing and, finally;
- the provisions governing the transfer of data to non-member countries of the EC.

Data controllers of non-automated processing of data have a time limit (until October 24, 2007) within which to comply with the provisions of the new law that concern them.

## Conclusion

The new law profoundly changes the rights of the data subject and the obligations incumbent upon data controllers. It also considerably reinforces the powers of the CNIL. All data controllers are therefore recommended to comply immediately with the new provisions – to this end, it would probably be useful to contact the CNIL in order to obtain its interpretation of some of the provisions that appear vague or too general. It is also recommended that companies evaluate their data practices (especially as they relate to data transfers) and consider incorporating policies and procedures governing the transfer of data files between companies in the same group and/or intended for non-member countries of the EC by means, for example, of contractual provisions or charters to this effect. It should also be noted that, where processed personal data relates to the employees of a company, some specific and additional provisions contained in labour law are applicable, involving, specifically, the consultation of staff representatives.

See "Appendix 1: Prior Formalities" and "Appendix 2: Main Obligations Incumbent upon Data Controllers and Rights of Data Subjects" on page 18.

1 Published in the French *Official Journal* of August 7, 2004, p. 14063.

2 Decision 2004-499 DC

3 This article is not exhaustive and some essential provisions in the law have not been specifically developed or studied here, such as: the conditions for lawful processing; rules on the processing of personal data for journalistic purposes and literary and artistic expression; rules relating to sensitive data or to data used for sub-contracting purposes.

4 The "Article 29" Group, instituted by Directive 95/46, adopted on May 30, 2002, a working document on "the international application of law in the E.U. in terms of data protection and the processing of personal data on the Internet by websites established outside the E.U." (document 5035/01/FR/Final WP 56, available on http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2002/wpdocs02_fr.htm). This document specifies the notion of establishment: it implies the actual exercise of an activity in a set place of establishment for an open-ended period of time. With regard to the specific case of a company supplying services through an Internet site, the place of establishment is not the one where the technology supporting its website is located, nor the place of access to the website, but the place where the company carries out its business. The notion of "using processing resources" located on the territory has, for its part, been interpreted as meaning that the use of cookies or Java applets placed on the hard disk of a computer located on French territory is considered to be the use of processing resources located on French territory.

5 Processing subject to authorisation due to a ministerial order made after motivated opinion from the CNIL, processing subject to authorisation by decree made at the Council of State after opinion from the CNIL, and processing subject to authorisation by order or, in case of processing performed on behalf of a public establishment or a corporate entity incorporated under private law and running a public service, on decision by the decision-making body with responsibility for their organisation, taken after published opinion from the CNIL, is not mentioned in this appendix due to its specific nature.

6 Provisions on so-called "sensitive" data are not dealt with here due to their specific nature.

## Appendix 1: Prior Formalities

| Formality required[5] | Types of processing |
|---|---|
| Prior notification | In principle for all automated processing of personal data. |
| No formality | 1. Processing whose sole object is the keeping of a register which, by virtue of legislative or regulatory provisions, is intended exclusively for public information and is open for consultation by the latter or by any person able to justify a legitimate interest.<br>2. Processing of "sensitive" data performed by a non-profit-making association/body of a religious, philosophical, political or trade-union nature (i) only for data corresponding to the aim of the association/body (ii) provided that the processing relates only to the members of the said association/body and, where applicable, people maintaining regular contact with the latter within the context of its activity (iii) subject to the processing involving only data not communicated to third parties, except where specific consent has been obtained from data subject.<br>3. Processing for which an "official" has been designated (except if processing is subject to authorisation, and except if transfer is envisaged to a non-member country of the EC). |
| Simplified declaration | The most commonly used categories of processing, the use of which is not likely to effect adversely private life or civil liberties and for which the CNIL has published a simplified standard. |
| Prior authorisation | 1. Processing of sensitive data (i) performed by INSEE or by a ministerial statistics department after advice from the National Council for Statistical Information or (ii) intended to be the object, within a short period of time, of an "anonymity process" recognised as compliant with the law by the CNIL, or (iii) justified by the public interest.<br>2. Automated processing involving genetic data (except processing used by doctors or biologists and necessary for the purposes of preventive medicine, medical diagnosis or the administration of care or treatment).<br>3. Processing involving data relating to offences, sentences or safety measures (except if used by legal auxiliaries for the requirements of their tasks in the defence of the people concerned).<br>4. Automated processing liable, because of its nature, scope or end-purpose, to exclude people from benefiting from a right, service or contract in the absence of any legislative or regulatory provision.<br>5. Automated processing with the aim of (i) the inter-connection of files managed by one or several corporate entities running a public service and whose end-purposes are different public interests (ii) the inter-connection of files managed by other entities and whose main end-purposes are different.<br>6. Processing involving data that includes people's registration numbers on the national register of identity of private individuals and processing that requires consultation of this register without including the registration number of people on this register.<br>7. Automated processing of data including assessments of individuals' social difficulties.<br>8. Automated processing including the biometrical data required for identity checks on people.<br>9. Processing whose end-purpose is limited to ensuring the long-term conservation of archive documents. |

## Appendix 2: Main Obligations Incumbent upon Data Controllers and Rights of Data Subjects

| Provisions applicable | Principle | Exceptions |
|---|---|---|
| Consent | Processing must have received consent from the person concerned | If the processing meets one of the following conditions:<br>i) compliance with a legal obligation incumbent upon the data controller, ii) safeguard of the life of the data subject, iii) performance of a mission of public service to be carried out by the data controller or the person for whom the data processing is intended, iv) performance either of a contract to which the person concerned is a party or pre-contractual measures taken at the request of the latter, v) performance of the legitimate interests of the data controller or the person for whom the data processing is intended, subject to not violating the interests or rights and fundamental freedoms of the data subject. |
| Data relating to offences, sentences, safety | Processing of such data cannot, in principle, be performed | If processing is performed by:<br>(i) The courts, public authorities and corporate entities running a public service, acting within the context of their legal competence, (ii) legal auxiliaries, for the strict requirements of the tasks entrusted to them by law, (iii) management societies dealing with the protection of copyright and rights of performers, producers of phonograms and videograms, acting for the rights managed by them or on behalf of victims of copyright violation as provided for in books I, II and III of the Intellectual Property Code, for the purposes of defending these rights. |
| Obligation of information | The person from whom this data is collected must be informed, except if he or she has been informed previously by the data controller/his representative (obligation limited if the data collected is due to be made anonymous within a very short period of time and when the data is collected by questionnaire). | If the data has been initially collected for another reason, the obligation of information does not apply to processing required for the conservation of this data for historical, statistical or scientific reasons or to the re-use of this data for statistical purposes.<br>If the data subject has already been informed or when it proves impossible to inform him or her or would require disproportionate efforts in terms of the purpose of the process.<br>If the data has not been collected from the data subject and is used during a process performed on behalf of the state and involving state security or public safety and defence or with the aim of executing criminal sentences or security measures, insofar as such limitation is required for compliance with the ends sought by the processing.<br>If data processing has the aim of prevention, research, establishment of or proceedings against criminal offences. |

## Appendix 2: Main Obligations Incumbent upon Data Controllers and Rights of Data Subjects (continued)

| Provisions applicable | Principle | Exceptions |
|---|---|---|
| Obligation to inform people using electronic communications networks | Clear, full disclosure by the data controller or his representative | If access to the information stored in the user's terminal equipment or input of information into the user's terminal equipment – in either case, if the exclusive aim is to permit or facilitate electronic communication, or is strictly necessary for the supply of an online communication service at the specific request of the user. |
| Right to object | All private individuals have this right, if they can provide legitimate reasons. | If the processing meets a legal obligation. If application of these provisions has been dismissed by a specific provision in the act authorising the processing. |
| Right to object to the use of data for commercial prospecting reasons | All private individuals have this right, which costs nothing, and does not require any legitimate grounds. | |
| Right to access and communication | All private individuals who can prove their identity have this right. | If the data is kept in a form that clearly excludes any risk of impact on the private lives of the people concerned and for a period that does not exceed that required for the sole purposes of the establishment of statistics or for scientific or historical research purposes. If requests are clearly unfair particularly with regard to their number, or the fact that they are made repeatedly or systematically. |
| Right to rectification | All private individuals who can prove their identity have this right. | |
| Transfer of data to a non-member country of the EC | Possible if the state to which data is transferred ensures an adequate level of protection of the private lives, and fundamental liberties and rights of people in terms of the processing which is performed, or may be performed, of the data. | Transfer to another country not meeting the conditions laid down is nevertheless possible:<br>If the person to whom the data refers has specifically agreed to its transfer or if the transfer is necessary for one of the following reasons: i) safeguarding of the life of this person, ii) safeguarding of the public interest, iii) compliance with obligations for the establishment, exercise or defence of legal claims, iv) consultation, under normal conditions, of a public register which, by virtue of legislative or statutory provisions is intended to inform the public and is open for consultation by the public or by any person who can show a legitimate interest, v) the performance of a contract between the data controller and the data subject, or of pre-contractual measures taken at the request of the latter, vi) the conclusion or performance of a contract signed or to be signed in the interest of the data subject, between the data controller and a third party.<br>If the CNIL decides that the data collector can guarantee an adequate level of protection, particularly due to the contractual clauses or internal rules to which it is subject. |

# A New Regulation on the Processing of Personal Data in Portugal

*By Margarida Couto and Cidália Neves, Vieira de Almeida & Associados, Lisbon. The authors may be contacted on tel. +351 311 34 87, or by e-mail: mc@vieiradealmeida.pt or csn@vieiradealmeida.pt*

Following a nine month delay and infringement procedures by the European Community, the law transposing the European Directive 2002/58/CE of July 12, 2002 on the treatment of personal data and protection of privacy in the electronic communications sector ("the Privacy Directive") finally entered into Portuguese law with its publication in the Official Journal on August 18, 2004.

Law no. 41/2004, which revokes the existing national law concerning this matter (Law no. 69/98 of October 28, 1998, now outdated as a consequence of technological developments in the industry), applies to the treatment of personal data in the context of (fixed and mobile) telephone and Internet services.

The Portuguese transposition scheme however, contains a peculiar detail regarding the safeguards against unsolicited communications for direct marketing purposes ("spam"). In fact, the Portuguese Government chose to make a partial and previous implementation of the Privacy Directive (article 13) by regulating this matter together with Decree-Law 7/2004, of January 7, 2004 which implemented Directive 2000/31/EC governing certain aspects of the information society services (electronic commerce in particular).

The main goal of Law no. 41/2004 is to create mechanisms to protect the privacy of citizens in light of the technological progress in electronic communications services.

With a view to ensuring an ever greater degree of privacy, the treatment of traffic data (such as data concerning the number called, the start and end time and duration or volume of data relating to a certain communication) is permitted in a very restricted way and, save where the purpose of such data treatment is to invoice for the service, it can only be done by the companies which provide the services in question, subject to the prior consent of the subscriber or user (and, even in this case, solely for the purposes of supplying added value services or providing electronic communication services).

One of the novelties of the law concerns the treatment of location data – data which indicate the geographic position of the terminal

equipment – which is allowed in the context of the provision of value added services, but only if subscribers or users are previously informed of the data treatment in question and give their prior consent. This matter is of particular significance and may become controversial in respect of its application to certain cases, such as the location of employees or leased vehicles.

Another important matter that has now been regulated concerns the use of so-called "cookies", "spyware" and other similar devices, which are able to enter the users' terminal equipment without their knowledge in order to obtain access to data, store hidden data or make it possible to trace the user's activities and which, to this extent, may constitute a severe intrusion into the users' privacy.

Another relevant aspect of the new law is the substantial increase of the penalties for non-compliance with some of these provisions, which have risen from a minimum of approximately €45,000 to a maximum of €5,000,000.

Extraordinarily, the new law came into force exactly one day after its publication in the *Official Gazette*, which is unusual considering the complexity and novelty of the new regime it enforces.

# Identity Theft in the United States

*By Holly K Towle, a Partner in the Seattle office of Preston Gates & Ellis LLP and chair of the firm's E-Commercial Law practice group.. The author may be contacted at hollyt@prestongates.com*

For centuries, philosophers have considered the concept of human identity, a notion that refers to an individual's sense of "self" and distinguishes one individual from another. In modern society, not only does one's identity – and the ability to prove it – serve to distinguish one person from another, but it also plays an obvious role in many of today's commercial and personal transactions.

In one sense there is nothing new here given that determining with whom one is really dealing has always been important.[1] However, making that determination becomes more complex when e-commerce is involved because there is no face-to-face interaction and a driver's licence picture or handwritten signature cannot be easily examined (even assuming they are valid). Data can be collected that tends to identify a person, but laws may restrict that collection and some identifiers may be public information or discoverable with an ease that may make the information of questionable use. This situation provides opportunity for illegal activity which can be exacerbated in electronic settings.

But the reality is that this opportunity has always existed and that "offline" methods for illegal activities cannot be ignored. For example, a 2003 survey by the United States Federal Trade Commission (FTC) indicated that *a lost or stolen wallet or pocket book, or theft of the victim's postal mail (including lost or stolen credit cards, checkbooks, and social security cards),* was the most commonly mentioned way that an identity thief obtained information.[1] A study by Michigan State University study to be published later this year, echoes or expands this by apparently finding that as many as 70 percent of all identity-theft cases originate with information stolen in a workplace, rather than through hacker intrusions, home robberies or mail fraud.[2] Identity thieves also include persons who give the name of another person in order to delay or avoid being charged with a crime, and there is nothing more "face-to-face" or "non-electronic" than an arrest.

The likely difference between now and yesterday is not a difference between online and offline activities, but changes in technology generally which allow thieves to do more, online or offline:

> At one time, not that many years ago, a breeder document, such as a driver's license, meant something; it could be used to establish a person's identity with little or no question. Now, technology has enabled criminals to produce fraudulent documents, which can be used to procure additional fraudulent documents. Counterfeit documents, such as credit cards, used to be easily detectable; now it is relatively easy to produce a counterfeit hologram that usually passes for the real thing. . . . Technology and the ability of the criminal element to adapt and defeat existing identification methodologies, predicated on breeder documents that are susceptible to counterfeiting, have made it necessary to develop different, more advanced identity authentication systems.[3]

Whether real or hyperbole, identity theft is being tied to the information age and has been described as "the crime of the new millennium".[5] While certainly this potential exists, the FTC's 2003 study actually indicates that all forms of identity theft have impacted only 4.6 percent of the U.S. population.[6] While no one would want to be in any group of identity theft victims, the point is that media coverage tends to leave the impression that this is an urgent, major crime for a hugely significant portion of the American public, and legislators are scrambling to get on the bandwagon with ever increasing amounts of legislation. Hence the need to look at this topic in more detail, including from a legal perspective.

## What is Identity Theft?

"Identity theft" is a term referring to a variety of crimes, all of which involve "stealing" someone's personal identifying information. The identity thief may use a variety of methods to obtain this information, ranging from "basic street theft" to "sophisticated, organized crime schemes involving the use of computerised databases or the bribing of employees with access to personal information on customer or personnel records".[7] Once the thief obtains the necessary information, he can transact business posing as his victim. In a recent Internet twist, two identity thieves opened accounts to sell goods on an Internet auction site – but there were no goods and they had opened their accounts under the names of their victims. When buyers at the auction did not receive their goods, they thought the victims, not the thieves, were the sellers who had defrauded them.[8]

What does identity theft typically involve? As explained by one group:

> The term, "identity theft," is itself complicated because it is used to refer to several different types of crimes in which personal or financial data is compromised. However, as the

  WDPR ISSN 1473-3579

number of cases have increased, patterns have emerged, making it possible to classify identity theft into the following categories:

- Fraudulent Authentication/One-Time Identity Theft
- Financial Institution Fraud
- Credit Card Fraud
- Fraudulent Loans
- Communications and Utilities Fraud
- Other.[9]

An identity thief's fraudulent activities generally take one (or both) of two basic forms: so-called "criminal identity theft" (providing a victim's personal identifying information to law enforcement upon arrest) or financial fraud, further distinguished as "true name fraud" (using a victim's identifying information to open new accounts in the victim's name) and "account takeover" (gaining access to a victim's existing accounts and making fraudulent charges). Although criminal identity theft does take place, traditionally the vast majority of identity thefts in the United States have been financially related[10] and are usually a component of one or more other white-collar or financial crimes. However, there is also "identity fraud," which encompasses identity theft but also includes creating or using a *fictitious* identity, as opposed to stealing and using a real one.[11] In modern society, it may be that we will actually see as much or more of that kind of criminal activity than the type to which regulators tend to be responding most:

> The use of a false identity created from fraudulent documents or a stolen identity (identity theft) in the commission of a crime has long been used by criminals and criminal organizations to facilitate criminal activities and avoid detection. As is evident from the previous section, quantifying the impact of identity fraud is difficult, but as the statistics in the next sections report, terrorism, money laundering and financial crimes, drug trafficking, alien smuggling, and weapons smuggling are growing concerns for the public and private sectors. Laws and regulations that have been instituted since 1998 are another indicator of the dramatic increase in the widespread use of these methods by criminals and terrorists.[12]

## How Does Identity Theft Happen?

An endless list of scams provides an opportunity for identity theft. Many of them are listed at a site maintained by the Identity Theft Resource Centre.[13] But even ordinary activities provide opportunity for identity theft: lost or stolen items such as postal mail, wallets, purses, checkbooks, and cards (social security or credit cards) are common causes. A catalogue of additional methods can be found in a paper prepared by the National Automated Clearing House Association.[14]

## Who is an Identity Thief?

According to the FTC's 2003 Report, if the victim knows the thief then the crime is usually more serious – 26 percent of all victims knew the thief's identity,[14] which tended to be as follows:

- In 35 percent of the cases where the victims know (nine percent of all victims), the thief is a *family member or relative*.[16]
- In 23 percent of the cases (six percent of all victims), the thief was someone who worked at a *company or financial institution* that had access to a victim's personal information.[17]
- In 18 percent of the cases (five percent of all victims) the thief was a *friend, neighbor, or in-home employee.*[18]
- In 16 percent of the cases (four percent of all victims), the thief was a *stranger* but the victim later became aware of the identity.

The above statistics are interesting because some media coverage leaves one with the impression that identity theft is committed by faceless strangers. To the contrary, that is the lowest category of known thieves. Of course, the above accounts for only nine percent of all victims so, obviously, most victims do not know who the thief was and, thus, a range of additional possibilities exists. It may be that in this large group lies the stranger-thiefs of the policy debate.

## Responses to Identity Theft

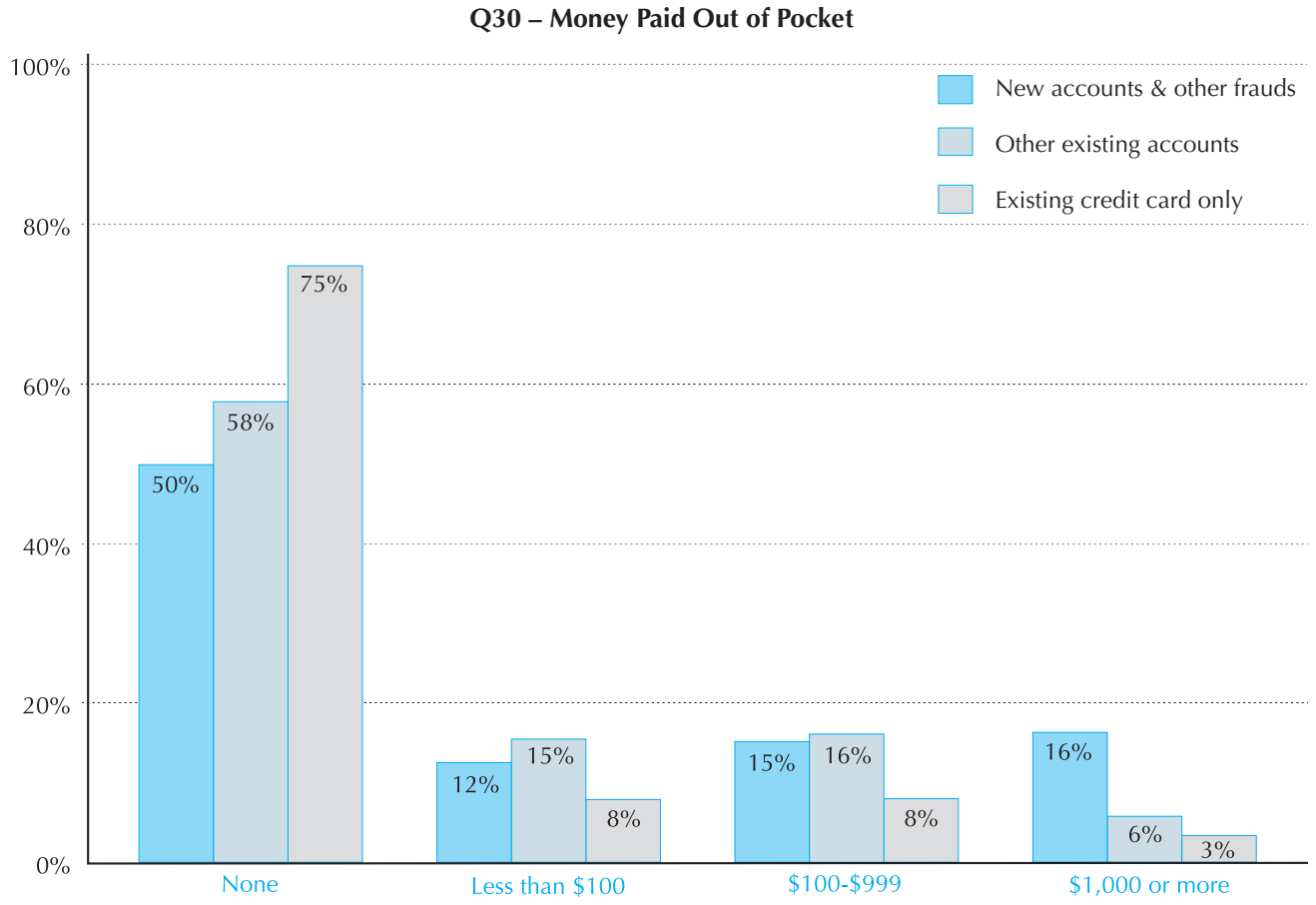
Interestingly, the FTC 2003 Report indicates that for most victims of identity theft (63 percent), there is no loss of money out-of-pocket';[19] 35 percent of all victims were able to resolve all problems in one hour or less;[20] and regardless of the misuse the victim encountered, over half of those surveyed said they were "not very" or "not at all" concerned that it might happen to them again.[21] This may result from the fact that the most common instances of theft pertain to existing credit card accounts, and victims were "overwhelmingly" satisfied with the credit card issuer's response to the victim's report of misuse.[22] Satisfaction also existed, however, with respect to new credit card accounts.[23] Both of these outcomes are logical, given that consumers generally are not liable for unauthorised uses of their credit card.[24]

A very different story is reported in the media and even by state regulators. For example, a California regulator describes the same 2003 FTC Report this way: "The costs of the crime are alarming. Recent studies estimate the average victim's out-of-pocket expenses at $500 to $740, and the time spent clearing up the situation at from 30 to several hundred hours".[25] While that is true, it is out of context and quite misleading. As noted, the FTC report says that for 63 percent of victims, that is, a sizable majority, there was no loss of money at all, and that is shown on the following copy of the report's graphic (shown overleaf). In the graphic, the first group of vertical bars is where the 63 percent average comes from, that is, a majority of victims suffered no loss. Thus, the median of all victims have zero loss; the mean would be higher. The California regulator obtained its $500 number by focusing solely on the third group of vertical bars in the chart, but did not put that group into context.

In any event, statistics are just that and no one would want to fall within them even if they are not as alarming as portrayed by regulators with an agenda. Also, the fact that the "victim" suffered little or no financial loss does not mean that a loss did not occur for someone. Retailers, card companies and others may have suffered some loss even though the "victim" that is the focus of these statistics did not.

The problem caused by exaggeration, however, is the response it creates – that is, overreactive legislation that is passed in haste or based on false assumptions. This is particularly troublesome with identity theft because there are two victims, not just one. The victim treated by most legislation is the one whose identity is stolen; but the second victim is the business victim who is duped: each deserves consideration and exaggeration tends to preclude that.

## Money Paid Out of Pocket by Identity Theft Victims




- For most victims of Identity Theft (63%), there was no loss of money out-of-pocket.
- Almost three-quarters of victims who only suffered the misuse of existing credit card accounts had no out-of-pocket losses. However, even for victims of the more serious kinds of ID Theft — "New Accounts & Other Frauds" — about half of victims reported incurring no out-of-pocket expenses.
- The average amount of out-of-pocket expenses incurred by victims of ID Theft was $500. For those who suffered from "New Accounts & Other Frauds" ID Theft, the average out-of pocket expense was $1,200.
- Victims who quickly discovered that their information was being misused were less likely to incur out-of-pocket expenses. No out-of-pocket expenses were incurred by 67% of those who discovered the misuse less than 6 months after the misuse began. Only 40% of victims who took 6 months or longer to discover the misuse were able to avoid incurring some such expenses.

N.B. This graphic is reproduced from the FTC Identity Theft Survey Report (at p.43), as prepared by Synovate (September 2003). A copy of the report is available at *www.ftc.gov/os/2003/09/synovatereport.pdf*. Please see the FTC Report in full for a complete picture.

While reasonable minds may differ regarding the actual facts about identity theft. Laws are increasing at a rapid rate. In the United States, a massive new law has been adopted, the Fair and Accurate Credit Transactions Act of 2003[26] ("FACT"). It focuses on consumer reporting agencies (aka credit reporting agencies) and use of credit reports and credit scores. However, it also contemplates a much broader application that will affect essentially every entity engaging in U.S. commerce for consideration – each such business must establish procedures to respond to consumer claims of identity theft. It also affects other issues such as the ability to sell or transfer debt involving identity theft; what may be printed on a receipt for a credit or debit card; how change-of-address requests for credit or debit cards may be processed; sharing of consumer information among affiliates; and limitations on the use of medical information and so on.[27] FACT imposes or increases procedural and substantive requirements on disclosure and use of credit reports and credit scores and on businesses that deal with identity thieves. In addition to being a complex statute in itself, FACT contemplates the issuance of extensive regulations by the FTC or other regulators supporting its provisions.

## What Other U.S. Laws Address Identity Theft?

In addition to FACT, a wide range of federal and state laws relate to identity theft. Some specifically address identity theft as a crime and some can be used to charge identity thieves with other related crimes. There are also "privacy or data collection" laws that can help prevent identity theft by regulating how personal information can be collected and when it can be disclosed, or

help identity theft victims restore their credit ratings and limit their liability for unauthorised debts. Identity theft is also one of the suspected criminal violations that require a U.S. financial institution to file a "suspicious activity report".

## Policy Issues

Two general points should be made laws before turning to laws specifically related to identity theft. First, at times the risk of identity theft will have to give way to other public policies. Second, laws regarding privacy and identity theft are pushing in opposite directions and will, inevitably, clash. This may be true in other countries as well, but it particularly true in the United States because of the heavy policy emphasis, both constitutionally and by culture, on the free flow of information.

### *Identity Theft vis a vis Other Public Policies*

*In re Crawford*[28] is illustrative of the point that the risk of identity theft may have to give way to other U.S. public policies. In this Ninth Circuit case, the court examined the disclosure, as opposed to the collection, of social security numbers. It started with the premise that a constitutional "zone of privacy" has been firmly established by the U.S. Supreme Court although the boundaries of that zone are not clear:

> We have observed that the relevant Supreme Court precedents delineate at least two distinct kinds of constitutionally-protected privacy interests: "One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions".[29]

The court noted that not all circuits agree and that some have "disavowed the notion of *informational*[30] privacy as a constitutionally protected interest." The court characterised that as the minority view and inconsistent with the law of the Ninth Circuit.[31] It then turned to the question at hand, which was whether a federal bankruptcy statute was unconstitutional because it required non-attorney preparers of bankruptcy petitions to list their social security number. A preparer alleged that this was unconstitutional because the petition became a public record, and such a forced disclosure of his SSN exposed him to crimes such as identity theft. The court agreed that the "indiscriminate public disclosure of SSNs, especially when accompanied by names and addresses, may implicate the constitutional right to informational privacy".[32] However, that right must be weighed against the governmental interests underlying the statute, and the court concluded that those outweighed the preparer's interests.[33] The "speculative possibility of identity theft is not enough to trump the importance of the governmental interests behind" the federal statute and the court could not say that Congress transgressed the bounds of the Constitution in enacting the statute.[34]

Public policies come in various shapes and sizes. An obvious one is the policy of preventing identity theft itself or other crimes or terrorism. As laws are enacted to address one aspect of a particular policy, that very law may exacerbate problems under other aspects of the same or a different policy. For example, the federal Fair and Accurate Credit Transactions Act of 2003 (FACT), in an effort to assist victims of identity theft, imposes significant obligations to adopt procedures to avoid errors and resolve disputes on various persons, including those furnishing information to a consumer reporting agency and persons using consumer reports from those agencies. A logical response for a business subject to those obligations and regulations would be to cease using or providing shared information. But the effect of that will, in fact, clash with the public policy of preventing identity theft and other crimes.

To illustrate, assume an identity thief opens five new accounts in a single week, having stolen the identity of John Doe. Three of the accounts are opened at a telephone company, a department store, and a car rental agency, each of which has determined not to obtain credit reports from consumer reporting agencies and not to provide information to them, all in order to avoid the procedural and other obligations imposed by, and legal compliance costs of, FACT. Each has weighed the costs of compliance against the likelihood of dealing with an imposter and has determined simply to avoid sharing information. Thus, the information about John Doe from those three companies will not enter the reporting system and will not be available to be noticed by either of the other two businesses that are obtaining consumer reports or reporting information and checking for indications of fraud (such as any unusual frequency of account openings or activity by John Doe). Information about John Doe will simply drop out of the reporting system and soon the thief will have an open field to commit even more identity thefts. Competing policies are at work and dealing with one may adversely impact the other.

### *Collision of Identity Theft and Privacy*

Laws regarding privacy and identity theft are pushing in opposite directions and will, inevitably, clash. We discuss below a California statute[35] allowing the imposition of a $30,000 penalty on a vendor who, as a victim itself of identity theft, continues to pursue its claim against the other victim (the person whose identity has been stolen) after the vendor has been presented with facts that later entitle the other victim to obtain a judgment eliminating the purported obligation. Similarly, FACT requires various levels of proof of identity in order to complete a transaction or provide certain information, including a "high degree of confidence" that one is dealing with the correct person.

These kinds of statutes send this message to vendors and service providers: "unless you find ways actually to prove with whom you are dealing, you will suffer not only the loss of an unauthorized transaction, but will also be heavily penalized." The obvious and legitimate response by vendors and service providers is to require significantly more identification before entering a transaction or a relationship. But when the vendor collects that additional information, it will run into claims that the collection violates the customer's privacy. This places the vendor in the classic position - living between a rock and a hard place.

How this will play out in the courts is not yet known. Two cases are illustrative. In *Messing v. Bank of America*,[36] a bank was sued by a payee of a check. The payee went to the drawee bank and sought its acceptance of the check and payment. That bank was part of a program intended to reduce check fraud and had a stated policy of requiring non-customers to provide a thumbprint on a device leaving no ink stains. The payee refused to provide the print, claiming that this would violate his right to privacy and that it was not the kind of identification contemplated by Uniform Commercial Code (UCC) Article 3, the law in each U.S. state regarding payments by check. The court had to decide whether the bank could be viewed as having "dishonored" the check by requiring the thumbprint: UCC Article 3-501(b)(2)(ii) allows a bank to request "reasonable identification" and if the request is reasonable, then there is no dishonour under UCC Article 3-501(b)(3)(ii). The payee argued it was not reasonable: He had already presented a credit card and driver's license which the bank had entered on the back of the check; also, even if he

supplied a thumbprint, that would not tell the bank who he was at the time of payment – it would only be useful later. The court disagreed, noting that other courts had determined that requiring a thumbprint was not an invasion of privacy in non-criminal contexts, and concluding that even if a thumbprint does not provide immediate identification, it does provide a powerful deterrent to those who might attempt to pass bad checks. It held that this reduction of risk promotes the expansion of commercial practices contemplated by the UCC and that the bank's requirement of a thumbprint by non-customers was reasonable.[37]

*Messing* illustrates that as adverse consequences are allocated to service providers, they will respond by requiring more identification and that at some point, customers will claim that the new requirements invade their privacy.

Ironically, that debate will be complicated by the fact that consumers will also claim that the service provider should have requested *more* information and is liable for not doing so. *Andrews v. TRW, Inc*.[38] is illustrative of consumer claims even though it was ultimately reversed. There, the victim of identity theft sued TRW, a credit reporting agency, for supplying credit reports to vendors who believed they were dealing with the victim but were actually dealing with the thief. Under the Fair Credit Reporting Act (FCRA), TRW could only furnish a credit report when it had "reason to believe" the report would be used in connection with a credit transaction involving the suwo data elements matching, given the universe of names and numbers, was very small.[39] The Ninth Circuit reversed and remanded, concluding that the issue was a question of fact and that a jury should decide "whether identity theft has been common enough for it to be reasonable for a credit reporting agency to disclose credit information merely because a last name matches a social security number on file."[40] The standards set in FCRA are statutory and higher than those that tend otherwise to be set in ordinary commerce, and the amendment of FCRA by FACT directly or indirectly mandates the collection by businesses of ever more identifying information. Thus, the dilemma remains: Customers will argue both for and against more privacy and this will create tension under identity theft statutes and procedures necessary to attribute acts to particular persons. Confusion is certain; answers are not.

### U.S. Federal Criminal Statutes

#### *The Identity Theft and Assumption Deterrence Act of 1998*

The federal Identity Theft and Assumption Deterrence Act of 1998[41] specifically labels identity theft as a crime. Prior to the act's passage, 18 USC 1028(a) criminalised the unauthorised use or transfer of identity documents such as a social security card, and 18 USC 1029 made illegal the unauthorised use of credit cards, ATM (automated teller machine) codes, and the like.[42] While those sections continue in force, the act added a new subsection, 18 USC 1028(a) (7), which applies when a person "knowingly transfers or uses, without lawful authority, a *means of identification* of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law. . . ." The act defines "means of identification" as:

> …any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any –
>
> (A) name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
>
> (B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
>
> (C) unique electronic identification number, address, or routing code; or
>
> (D) telecommunication identifying information or access device (as defined in section 1029(e)).[43]

This broadened the scope of 18 USC 1028(a) to include the misuse of information while retaining use or transfer of documents such as a social security card. Thus, the statute has recognised since 1998 that criminals do not need documents to assume an identity – "often they just need the information itself to facilitate these types of crimes."[44] The fact that this expansion was necessary is not surprising and, in fact, is symptomatic of the information age: Most U.S. laws, including commercial laws such as UCC 2 (sales of goods), were written with tangible objects in mind such as the social security card, as opposed to the information, and cannot be or should not be applied to information.[45]

#### *Other Laws*

The Identity Theft and Assumption Deterrence Act of 1998[46] can be applied to a wide range of offences that can be independently prosecuted under the act or other numerous statutes. For example, the unauthorised use of credit cards was already illegal under 18 USC 1029, but after 1998, it can be prosecuted under that section or under the act. "In total . . . the violation of some 180 federal criminal statutes can potentially fall within the ambit of 18 USC 1028(a)(7)."[47]

Most states have also enacted laws criminalising identity theft: about forty-four states have specific laws, and five others have laws covering activities "included within the definition of identity theft".[48] According to the FTC, identity theft crimes can be considered felony offences in forty-five of the forty-nine states that have relevant laws.[49] The previously noted federal Fair and Accurate Credit Transactions Act[50] will preempt some of the state laws in varying degrees. But FACT itself if a comprehensive new law regarding identity theft.

## How Can Potential Victims Decrease the Risk of Identity Theft?

The FTC 2003 Report indicates several things that potential victims of identity theft can do to forestall it. All harmful repercussions seem to be reduced by prompt discovery of misuse, such as exambject of the report. It argued it had fulfilled this obligation by supplying the report after receiving the name and social security number of the supposed customer. The lower court granted summary judgment, reasoning that the random chance of those tining monthly statements of accounts: 52 percent of all victims cited this as the way that they discovered they were victims of identity theft.[51] Other suggestions made by those surveyed for the report included:

> Many victims thought better awareness on their own part of how to prevent and respond to identity theft would have been most helpful. Specific areas where greater awareness was cited included taking greater security precautions in handling their personal information, such as destroying materials that contain personal information instead of simply putting them in the trash, not placing personal information on the Internet, and securing their personal information in their homes and at work. Maintaining greater vigilance, such

as monitoring their mail, billing cycles, and credit reports more carefully was also cited. Lastly, knowing who to contact, and notifying the affected companies and credit reporting agencies more quickly when they detected something wrong, was identified as an important factor in recovering from identity theft.[52]

1 For a discussion of the various methods established by U.S. law to "attribute" acts to a particular person, see Chapter 6 of Holly K. Towle and Raymond T. Nimmer, The Law of Electronic Commercial Transaction (A.S. Pratt & Sons, 2003).

2 FTC Identity Theft Survey Report at 9 and 30, prepared by Synovate (September, 2003) (copy available at *www.ftc.gov/os/2003/09/synovatereport.pdf*, visited 19/08/04) (hereafter, "FTC 2003 Report"). This was 25 percent of those who actually knew how their information was obtained. This group accounts for 51 percent of all victims (leaving almost half of victims not knowing how their information was obtained). Id. at 9 and 30.

3 See "Big Trust in Database Leads to Big ID Thefts," Mark Jewell, *The Seattle Times* at D2 (8/10/04).

4 Joint Project of the Economic Crime Institute of Utica College and LexisNexis, a Division of Reed Elsevier Inc., Identity Fraud: A Critical National and Global Threat at 4 (October 28. 2003) (copy available at *www.ecii.edu/identity_fraud.pdf*).

5 S.B. Hoar, "Identity Theft: The Crime of the New Millennium", 80 Or. L. Rev. 1423, 1423 (2001).

6 FTC 2003 Report at 7. The 4.6 percentage figure converts to 9.91 million people. California regulators view this number with much more alarm, using it as a basis for guidance issued in connection with a California statute requiring notice when there is a breach of security of certain computerised systems. "A national survey conducted by the Federal Trade Commission found that the number of victims in 2002 approached 10 million, and two other recent surveys estimated the number at seven million. That's nearly 10 times greater than the previously quoted estimate of less than a million a year. If the same rate is applied to California, then over a million Californians became victims of identity theft in the past year." See CA Office of Privacy Protection, Recommended Practices on Notification of Security Breach Involving Personal Information at 5, regarding CA Civil Code 1798.82. On the other hand, identity theft is the most complained about crime based on reports made to the FTC. See FTC National and State Trends in Fraud and Identity Theft (1/2004), copy available at *www.consumer.gov/sentinel/pubs/Top10Fraud2003.pdf*.

7 S. Rep. No. 05-274, at 7 (1998).

8 See settlement order in *FTC v. James D. Thompson and Susan B. Germek (ND of Illinois, Eastern Division*), Case No. 0C3 2541; FTC File No. 032 3096.

9 NACHA Internet Council, *Internet Payments Fraud: A Primer for Merchants and Financial Institutions* (Feb. 3, 2003) (copy available at *http://internetcouncil.nacha.org/docs/Fraud%20Paper%20Final%20%20Jan%20%2703.pdf*, visited 19/08/04).

10 *FTC v. James D. Thompson and Susan B. Germek* (ND of Illinois, Eastern DiSee Joint Project of the Economic Crime Institute of Utica College and LexisNexis, a Division of Reed Elsevier Inc., *Identity Fraud: A Critical National and Global Threat*, (October 28. 2003). Copy available at *www.ecii.edu/identity_fraud.pdf*. This white paper defines identity fraud as follows:

"vision), Case No. 0C3 2541; FTC File No. 032 3096 at 9.

11 Identity fraud, which encompasses identity theft, is the use of false identifiers, false or fraudulent documents, or a stolen identity in the commission of a crime. It often emanates from a breeder document created from fictitious or stolen identifiers. The breeder document, such as a driver's license or birth certificate, is used to spawn other documents, resulting in the creation of a credible identity which allows a criminal or terrorist access to credit cards, employment, bank accounts, secure facilities, computer systems, and the like."

12 Id. at 13.

13 See *www.idtheftcenter.org/alerts.shtml*.

14 NACHA Internet Council, Internet Payments Fraud: A Primer for Merchants and Financial Institutions (Feb. 3, 2003) (copy available at *http://internetcouncil.nacha.org/docs/Fraud%20Paper%20Final%20%20Jan%20%2703.pdf*, visited 19/08/04).

15 See CDT January, 2004 letter regarding: *2003 Reports of Internal Fraud and Physical Security Problems at State Motor Vehicle Offices* (organised by state), copy available at *www.cdt.org/privacy/20040200dmv.pdf* (as of 1/04), at 28.

16 Id.

17 Id. See, *e.g.*, *Andrews v. TRW Inc.*, 225 F3d 1063(9th Cir. 2000), rev'd, 534 U.S. 19 (2001) (involving identity theft by receptionist in doctor's office of information supplied by the patient to the doctor; reversed as barred by statute of limitations).

18 Id.

19 FTC 2003 Report at 43.

20 Id. at 45. Some 29 percent required two to nine hours; 30 percent required more than ten hours; and six percent spent over 240 hours. Id.

21 Id. at 15. Slightly less than half (44 percent) said they were "very" or "somewhat" concerned that they will be victimised.

22 Id. at 52. Misuse of existing credit cards accounted for 56 percent of all identity theft victims; of those, 73 percent were "very satisfied" with how the credit card company responded to the report of misuse. Id. Where more than one existing credit card was misused, or a new credit card was misused, satisfaction levels dropped to 53 percent. Id.

23 Id. at 52–53. Victims of new account experienced slightly lower levels of satisfaction but still, 78 percent were satisfied.

24 See Holly K. Towle and Raymond T. Nimmer, *The Law of Electronic Commercial Transaction* (A.S. Pratt & Sons, 2003) at ¶ 6.06.

25 See CA Office of Privacy Protection, Recommended Practices on Notification of Security Breach Involving Personal Information at 5, regarding CA Civil Code 1798.82.

26 Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159 (December 4, 2003), hereafter "FACT".

27 For a full discussion of FACT and these topics, see Holly K. Towle and Raymond T. Nimmer, *The Law of Electronic Commercial Transaction* (A.S. Pratt & Sons, 2003) at Chapter 15.06[3] and chapters cited therein.

28 In re Crawford, 194 F3d 954 (9th Cir. 1999), cert. denied sub nom *Ferm v. U.S.* Trustee, 528 US 1189 (2000).

29 Id. at 959.

30 The discussion here focuses only on "informational" privacy as opposed to more traditional forms of privacy. There is myriad U.S. law, federal and state, on traditional notions of privacy. See discussion in Chapter 6 of Holly K. Towle and Raymond T. Nimmer, *The Law of Electronic Commercial Transaction* (A.S. Pratt & Sons, 2003), Chapter 12.

31 194 F3d 954 at n. 4.

32 Id. at 959. The court discussed the harm that can flow from misuse of social security numbers and distinguished them from names and telephone numbers because the SSN serves as a unique identifier that cannot be changed and is not generally disclosed by individuals to the public. Id.

33 Id. at 961 (legislative purpose of protecting persons filing bankruptcy from unlicensed preparers and benefits of public access to bankruptcy records).

34 Id. at 961. The court did note in footnote 9 that the preparer had raised valid privacy concerns and encouraged Congress to consider enacting rules to limit the disclosure of preparer SSNs.

35 California Civil Code 1798.92 through 1798.97.

36 *Messing v. Bank of America*, NA.., 373 Md. 672, 821 A2d 22 (2003).

37 Id. at 40.

38 *Andrews v. TRW*, Inc. 225 F3d 1063 (9th Cir. 2000), rev'd, 534 U.S. 19 (2001).

39 Id. at 1067.

40 Id. at 1067. The court also said the jury should assess whether the question of reasonableness was affected by information possessed by TRW such as the misspelling of the supposed customer's first name and a mistake in the birth date. "A jury will have to say how reasonable a belief is that let a social security number rump all evidence of dissimilarity between the Plaintiff and the Imposter." Id.

41 18 USC 1028 (2003).

42 GAO, Identity Theft: Greater Awareness and Use of Existing Data Are Needed at 5 (June 2002).

43 Id.

44 S. Rep. No. 105-274, at 6 (1998).

45 This topic is the subject of debate in the U.S. as courts and legislatures struggle to draw appropriate dividing lines and free themselves of thinking that works for "goods" but not for "information." See, *e.g.*, *U.S. v. Stafford*, 136 F3d 1109, 1115-1116(7th Cir. 1998), *modified*, 136 F3d 1115 (7th Cir. 1998) and cert. denied, 525 U.S. 849 (1998), in which the court said:

The government concedes that the codes are not securities or money, but it says that they are goods, wares, or merchandise. They're not; they're information. No doubt Allison wrote them down rather than committing them to memory, but he was not charged with having transported pieces of paper containing codes across state lines and we need not decide whether such transportation would violate the statute. He was charged with transferring the codes themselves, which are simply sequences of digits. The sequences have no value in themselves; they are information the possession of which enables a person to cash a check.

See also *Specht v. Netscape Communications Corp*., 306 F3d 17, note 13 (2d Cir. 2002), stating, "Recognizing that 'a body of law based on images of the sale of manufactured goods ill fits licenses and other transactions in computer information', the National Conference of Commissioners on Uniform State Laws has promulgated the Uniform Computer Information Transactions Act (UCITA), a code resembling UCC Article 2 in many respects but drafted to reflect emergent practices in the sale and licensing of computer information".

46 18 USC 1028 (2003).

47 18 USC 1028 (2003).

48 GAO, *Identity Theft: Greater Awareness and Use of Existing Data Are Needed*, at 1, 6. Vermont was the only state that does not have a law that either specifically addresses identity theft or covers activities included within the definition of identity theft. See Chapter 15 of Holly K. Towle and Raymond T. Nimmer, *The Law of Electronic Commercial Transaction* (A.S. Pratt & Sons, 2003) (listing the states and the relevant state laws, as well as more federal statutes).

49 Id. at 6. Of those states that have not passed identity theft legislation, many are considering doing so. FTC, *ID Theft: When Bad Things Happen to Your Good Name* 1 (Sept. 2002), available at *www.ftc.gov/bcp/conline/pubs/credit/idtheft.pdf* at 25.

50 Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159 (December 4, 2003).

51 FTC 2003 Report at 39. Some 25 percent were notified by their account institution or other vendors who noticed suspicious account activity; eight percent discovered they were victims when they were turned down while attempting to obtain credit; and nine percent knew they had lost their information because they had lost a wallet or purse. Id. at 39 and 40.

52 FTC 2003 Report at 62. For a list of recommendations regarding avoidance of identity theft, see Holly K. Towle and Raymond T. Nimmer, *Law of Electronic Commercial Transactions*, Chapter 15.07 (A.S. Pratt & Sons 2003).

*Holly is the co-author of The Law of Electronic Commercial Transaction, (H. K. Towle and R. T. Nimmer), A.S. Pratt & Sons, 2003.*

# Security & Surveillance

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

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

Processing of personal data by means of video surveillance devices and systems is one of the major topics in the data protection sector, both at a European level and also in Italy. The E.U. Data Protection Working Party adopted an Opinion on the topic earlier this year ("Opinion 4/2004 on the processing of personal data by means of video surveillance", adopted on February 11, 2004 (*http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp89_en.pdf* )), and the E.U. Data Protection Directive 46/95/EC has already provided that the definition of "personal data" also include images or sounds capable of identifying individuals.

In Opinion 4/2004, the European Data Protection Authorities stated that over the past few years, public and private bodies have had increasing recourse to image acquisition systems. This circumstance has raised a lively debate both at Community level and in the individual Member States in order to identify pre-requisites and limitations applying to the installation of equipment giving rise to video surveillance, as well as the necessary safeguards for data subjects.

Evidence over the last few years, following transposition at national level of Directive 95/46/EC, has shown the huge proliferation of closed circuit systems, cameras and other more sophisticated tools that are used in the more diverse sectors.

Furthermore, the development of the available technology, digitalisation and miniaturisation considerably increase the opportunities provided by image and sound recording devices also in connection with their deployment on intranets and the Internet. In addition to the processing operations in the employment context, the growing proliferation of video surveillance techniques can be easily appreciated by all citizens. There is also a growing trend towards interconnection of video surveillance systems.

A non-exhaustive analysis of the main applications shows that video surveillance can serve quite different purposes. These can be grouped into a few main areas:

- protection of individuals;
- protection of property;
- public interest;

  WDPR ISSN 1473-3579

- detection, prevention and control of offences;
- making available of evidence; and
- other legitimate interests.

In light of the increasing recognition of just how widely such systems are used in everyday life, it is interesting to note the detailed list of cases mentioned by Opinion 4/2004 about the different places, events and purposes according to which video surveillance systems are installed:

- within and near public and/or publicly accessible buildings such as museums, places of worship or monuments in order to prevent offences and/or minor acts of vandalism;
- within stadiums and sports facilities, especially in connection with certain events;
- in the transport sector and in connection with road traffic with a view to monitoring traffic on highways and motorways, or else in order to detect speed limit offences and/or breaches of regulations by traffic in city centres, or to control underground premises giving access to subway lines, to monitor petrol stations and inside taxi cabs;
- in order to prevent and/or detect unlawful conduct in the surroundings of schools, also in connection with the soliciting of minors;
- within medical facilities during surgery and/or with a view to, for example, providing distance care to or monitoring patients in intensive care units and/or in areas where seriously ill and/or quarantined patients are hospitalised;
- in airports, onboard ships and near border areas in order to monitor smuggling, as well as to facilitate searching minors and other missing persons;
- by private detectives;
- within and near supermarkets and shops, especially when dealing with luxury goods, with a view to making evidence available, in case offences are committed, as well as for the purpose of marketing goods and/or profiling consumers;
- within and in areas adjacent to private condominiums both for security purposes and in order to make evidence available in case offences are committed;
- for journalistic and advertisement purposes that are pursued online by means of either web cams or cameras, for example, to promote tourism as relates to beach resorts and nightclubs where customers and visitors are filmed at regular intervals without warning.

In light of the above, the European Data Protection Authorities analyses in Opinion 4/2004. the current situation regarding the employment of video surveillance and addresses some recommendations to Member States relating to privacy protection.

## Italian Rules on Video Surveillance

At a legislative level, the Italian Code on Privacy (the legislative decree of June 30, 2003, no. 196) while confirming that the processing of images is a processing of "personal data" falling within the scope of the Code, also provides (under section 134) that the Italian Data Protection Authority (the "IDPA") shall adopt a code of conduct and professional practice, applicable to the processing of personal data that is performed by means of electronic image acquisition devices. This should be done by setting forth specific processing arrangements and simplified mechanisms to inform data subjects, in order to ensure lawfulness and fairness of the processing.

The drafting of this specific code of conduct and professional practice (based on the co-operation and confront between the interested categories and the IDPA) is actually under way, and is expected to enter into force within the first half of 2005.

Beyond the limited legislative rules, it must be pointed out that since 2000 the IDPA had enacted the so-called "Video Surveillance Decalogue" of November 29, 2000 which was an administrative act providing concrete rules for the lawful employment of video surveillance devices and systems compliant with the data protection legal framework.

The act has recently been updated and developed by the General Act on Video Surveillance of April 29, 2004, which provides a detailed set of practical rules to adhere to with 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.

The General Act on Video Surveillance is divided into three parts. In the first part, the IDPA recalls the general principles governing the installation of any kind of video surveillance device. In the second part, the act lists the obligatory fulfilments to be carried out by the processors/holders of video surveillance systems; and in the third part the specific rules governing the video surveillance in particular sectors are provided.

Please note that the following considerations are focused on the first part of the General Act on Video Surveillance: the analysis of the remaining two parts will follow in Part II of this article, to be published in the November issue of *World Data Protection Law Report*.

## The IDPA General Act on Video Surveillance

### Analysis of the Main Principles Governing the Lawful Use of Video Surveillance Devices and Systems

The installation of video surveillance devices and systems and the related processing of personal data must be compliant with the "principle of lawfulness", which for public entities means that such installation is licit if aimed at carrying out institutional tasks, while for private entities is licit when the installation is carried out in order to fulfil a legal obligation provided by the law or the data subject has given his free and previous consent to the processing of his image.

Further, the installation of video surveillance devices and systems must comply not only with the rules contained in the Code on privacy, but also with other applicable rules provided by different laws implied by the setting up and installation of audio-visual devices: the rules provided by the civil and criminal code about illicit interferences in private life and the prohibition of the interception of communications, protection of human dignity, protection of the domicile and other places (such as toilets, hotel rooms, locker rooms, *etc*). Further, the installation of video surveillance devices and systems must also comply with the rules related to the protection of employees which prohibit the employer from carrying out controls at a distance.

### Principle of Necessity

Considering that the installation of video surveillance devices and systems introduces a limitation for citizens in practice, the

so-called "principle of necessity", shall apply. This means that such installation cannot be superfluous or redundant and any kind of excess with regard to the core reasons for the installation must be avoided. As a consequence, each informative system and the related computer programs supervising the video surveillance must be set up from the outset in a way that personal data and images relating to identifiable subjects shall not be used when the purposes of the video surveillance can be matched by utilising only anonymous data: for example, setting video surveillance systems for urban traffic monitoring purposes and the related supervising computer programs in a way that the filming is general and the possibility to enlarge the images is excluded. Further, the software must be set up in a way that the data and images recorded are periodically and automatically deleted.

If in the installation of video surveillance devices and systems the "principle of necessity" is not complied with, the video surveillance itself shall be deemed as unlawful. The "principle of necessity" is generally provided by Article 3 of the Italian Code on Privacy:

> Article 3 (the Data Minimisation Principle). Information systems and software shall be configured by minimising the use of personal data and identification data, in such a way as to rule out their processing if the purposes sought in the individual cases can be achieved by using either anonymous data or suitable arrangements to allow identifying data subjects only in cases of necessity, respectively.

### Principle of Proportionality

When considering the necessity of installing video surveillance devices and systems in light of the concrete risks according to which the installation is carried out, the processing of data and the recording of images with regard to areas or activities which are not subject to current risks or dangers must be avoided. The installation of video surveillance devices and systems is unlawful when it is only deterrent or when such installation is based on mere prestige or for reasons of appearance. The installation of video surveillance devices and systems is licit only when other alternative measures have been previously evaluated and deemed insufficient or impracticable. If the installation of video surveillance devices and systems is aimed at protecting property or goods, even against acts of vandalism, such installation shall be deemed lawful only once other measures have been previously evaluated as an alternative (*i.e.*, alarms, protection of entrances, *etc.*). It is not permitted to install video surveillance devices and systems simply because this is the least expensive, most straightforward or rapid solution to use; citizens' rights must be taken into account and balanced against the reasons for choosing this method.

Further, installing video surveillance devices and systems is unlawful when the video surveillance activity is not aimed at controlling events or situations or places, but its purpose is only promotional, for tourism *etc.* (*i.e.*, web cams or online cameras which identify individuals for such purposes). Installation of video surveillance devices and systems for merely demonstrative purposes (*i.e.*, video cameras are installed but are not activated or working) is not lawful either, even if the processing of personal data is not implied: in any case, the presence of the related devices (even if they are not in operation) can be used to condition the behaviour of individuals in public or private places.

The installation of video surveillance devices and systems is lawful when the principle of proportionality is complied with, both in the choices of the kind of filming devices employed and in the various phases of the processing of images. The principle of proportionality allows the processor to freely carry out such evaluation, but it does not imply that choices are absolutely discretionary or unquestionable.

So far the processor must evaluate:

- if shooting images which do not make individuals identifiable (even by enlargement of the images) is sufficient in light of the security need;
- if gathering and processing images is really necessary and essential for the singular purposes followed by the processor;
- the placing, the visual angle, the use of automatic zooms, the kind – fixed or moveable – of the video surveillance devices employed;
- what type of data and image will be recorded, if the recording is necessary, if a related data-bank must be created or an electronic communication network must be utilised; if operational functions like stop-image must be applied, if other information must accompany the images, if the video surveillance system must be interconnected with other systems managed by the same processor or by third parties;
- the duration for which the images will be retained.

Following the proportionality principle, the following must be duly restricted:

- filming private places or entrances of buildings when the video surveillance devices are lawfully employed in public places;
- employing specific solutions (*i.e.*, connection to "centres" to which audio or visual alarm signals are sent);
- doubling the recorded images;
- setting up specific databanks when, according to the purposes pursued, it is sufficient to install a closed circuit camera, aimed at uniquely broadcasting images without recording (*i.e.*, for urban traffic monitoring purposes or for controlling the stream of users by a public office).

### Principle of Finality

Installing video surveillance devices and systems must be based on lawful, certain and express purposes. This means that the processor is allowed to pursue only purposes falling within his competence.

The IDPA has often verified that certain private and public subjects justify the installing of video surveillance systems by referring to public security and prevention from crimes purposes. It must be pointed out that when these purposes are pursued (by means of video surveillance systems) by individuals or entities different from the competent public bodies (police or judicial authorities), the installing of such systems must be deemed unlawful.

If, on the other hand, the video surveillance devices are employed in order to complement or strengthen the security within buildings, industries, commercial centres, *etc.*, the video surveillance shall be deemed lawful only if the public is properly informed, by means of notices specifying the related purposes in a clear and detailed way.