WORLD DATA PROTECTION REPORT

Volume 3, Issue 4 April 2003

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

BNA International Inc., London

INTERNATIONAL INFORMATION FOR INTERNATIONAL BUSINESS

World Data Protection Report

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

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

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, Heron House, 10 Dean Farrar Street, London SW1H 0DX; tel. (+44) (0)20 7559 4807; fax (+44) (0)20 7233 2313; 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: Heron House, 10 Dean Farrar Street London SW1H 0DX, England. Tel. (+44) (0)20-7559 4801; Fax (+44) (0)20-7222-5550; E-mail marketing@bnai.com. In the U.S. call toll-free on: 1-800-727-3116.

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

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

Welcome to the April issue of World Data Protection Report. This month we report on the new privacy rules introduced by the Italian Data Protection Authority to regulate the use of Multimedia Messaging Services ("MMS"). Alessandro del Ninno examines the new Guidance.

Our article from Singapore comes from Rizwi Wun, who looks at the impact of the recently established Consumer Credit Bureau on banking secrecy laws in Singapore.

We also include Part II of our article by Dr. Perri 6 on entitlement cards, which asks if the U.K government's proposals for cards comply with data protection principles. Dr. 6 is Director of the Policy Programme at the Institute for Applied Health and Social Policy at King's College, London. A leading expert in the field of privacy, he is also well known for his work on "joined up government", and the regulation of information technology.

Will Downing and Cara De La Mare provide a useful article for all U.K. employers providing e-mail and Internet access to their employees – implementing and maintaining an effective employment policy on use is essential. To read more, please turn to their article on page 21.

As many readers will know, the 25th International Conference of Data Protection and Privacy Commissioners is taking place in Sydney this year. Further details on the conference and how to register appear at the end of this issue.

As always, we trust that you will find this month's edition informative and valuable. I invite your comments, suggestions and contributions to nicholad@bna.com

Nichola J. Dawson

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

Dr Perri 6, Director, The Policy Programme, Institute for Applied Health and Social Policy, King's College, London; *Sally Annereau*, Taylor Wessing, London; *Malcom Crompton,* Australian Federal Privacy Commissioner; *William Downing* and *Cara De La Mare*, Trowers & Hamlins, London; *Christopher Kuner*, Hunton & Williams, Brussels; *Alessandro del Ninno*, Studio Legale Tonucci, Rome; *Massimo Riccio,* Baker & McKenzie, Rome; *Dr. Christine Riefa,* Faculty of Law, University of Hertfordshire; *Laurent Szuskin* and *Myria Saarinen,* Latham & Watkins, Paris; *Cristos Velasco,* Instituto Tecnologico Autonomo de Mexico; and *Rizwi Wun*, Khattar Wong & Partners, Singapore.

CONSUMER PROTECTION

News

ITALY

First Use of Consumer Protection Rules Against Financial Institution

As a first application of the rules adopted in July 2002, the Italian Data Protection Authority (IDPA) has enforced its rules concerning processing of consumers' data by databases of banks and financial institutions (aka. "risk centrals" recording, among others, data of consumers concerning late payments, delinquencies, outstanding debt, length of credit history and new applications for credit).

The enforcement followed a complaint filed with IDPA by a consumer who had been granted a loan by a consumer finance company. The consumer, after certain late payments and finally repaying the loan, had then requested – to no avail –that the consumer finance company delete the record (which continued to show him as a late payer) from its database. Upon request of clarification by the IDPA, the company had informed the IDPA that the consumer's record had been supplemented with the note "regular position", indicating that the consumer had made good his position on repayment of the loan.

However, the IDPA held that this was not sufficient: the rule being that the record of the interested consumer must be deleted one year after repayment. Keeping the record beyond such period of time is at odds with privacy rules.

For further information, see the IDPA Newsletter, March 3-9, 2003, which is available online (in Italian only) on the IDPA's website: *www.garanteprivacy.it*

By Massimo Riccio, Baker & McKenzie, Rome; e-mail: massimo.riccio@bakernet.com

LEGISLATION & GUIDANCE

Privacy Rules on the Use of MMS: Recent Guidelines Enacted by the Italian Data Protection Authority

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

The Italian Data Protection Authority (IDPA) has recently enacted an important set of rules aimed at protecting the privacy rights with regard to the personal use of Multimedia Messaging Services (hereinafter "MMS") by mobile phones.

The guidance, which was issued on March 14, 2003, comes in response to several notices and requests received by the IDPA in recent months to investigate how far these new technologies comply with the Italian Data Protection Law (Law No. 675/1996). The new mobile phones enable users to quickly collect and communicate images, sounds and short films to third parties, using General Packed Radio Service (GPRS) technologies and the Universal Mobile Telecommunication System (UMTS) network.

Anyone with a mobile phone capable of sending MMS can easily record and disseminate images and sounds collected in public or private places. This can be done without the consent or knowledge of the individuals in the surrounding area whose privacy could be breached.

In the recently published guidance, "MMS: the Rules for Personal Use"(hereinafter the "Rules"), the IDPA makes some preliminary considerations. It points out that even though the connection with a digital phone is more direct, the new services are no different from digital cameras connected to PCs that disseminate images to an undetermined number of addressees via the Internet.

The Rules differentiate between personal and non-personal uses of MMS. IDPA makes clear that the Rules are intended to deal with specific and illicit *individual* uses of MMS, as well as wider uses by other subjects, such as private detectives. More general and future problems, such as the use of MMS by fixed telephony, will be dealt with successively by the IDPA.

Use of MMS is "Processing" of Personal Data

The IDPA clearly states that the use of MMS can be regarded as the "processing" of personal data.

Images, sounds and short movies transmitted by MMS may contain personal information related to a data subject, identified or identifiable according to Article 1, paragraph 2, letter (c) of the Italian Privacy Law No. 675/1996, which provides that:

> "personal data shall mean any information relating to natural or legal persons, bodies or associations that are or can be identified, even indirectly, by reference to any other information including a personal identification number".

Images or sounds are therefore included in the definition of "personal data" set forth in the law, and their collection, storage, use and diffusion can be considered as the "processing" of personal data. In certain cases, this could also involve so-called "sensitive data", relating to the health or sexual life of a data subject (the IDPA points out the case, for example, of reproducing images of disabled persons).

The IDPA goes on to list the cases according to which the general discipline provided by the Italian Privacy Law No. 675/1996 shall, or shall not apply.

Circumstances in Which Law No. 675/1996 Shall Not Apply

Law No. 675/1996 shall not apply in all the cases where MMS do *not* include personal data, as specified above.

Further, if the use of MMS represents a processing of personal data carried out by natural persons for exclusively personal purposes (but provided that the data are not intended for systematic communication or dissemination), Law No. 675/1996 shall not apply. For example, the use of MMS shall not fall within the scope of Law No. 675/1996 if a picture is taken to be occasionally sent to friends or relatives: *i.e.*, if the person who creates the picture or short film by means of a digital phone is doing so purely for his or her own personal (non-commercial) interest and viewing of the image is strictly limited.

In cases where the images are collected – even for cultural or informative purposes – to be successively disseminated by the Internet or systematically communicated to third parties, Law No. 675/1996 shall apply.

There will be specific situations which fall somewhere between these two examples. Such cases will be hard to categorise and will need to be examined on a case-by-case basis. For example, an MMS could be sent by means of a unique and direct communication to third parties, but to a large number of addressees. In such cases, practical conditions could be matched so as an occasional sending of images is carried out with modalities which mean that the activity falls within the scope of Law No. 675/1996.

The new IDPA Rules do not exclude the application of other legal provisions. Individuals who use MMS for exclusively personal purposes must comply with the obligation to keep secure the information collected as per Article 3, paragraph 2, and Article 15 of Law No. 675/996, which introduces specific and compulsory obligations related to the adoption of minimum security measures in the processing of personal data. Further, individuals using MMS must also take into consideration the need to respect the fundamental rights of the data subjects, specifically their human dignity. In the case of breaches or damages caused to third parties by the use of MMS, the liable subject (*i.e.*, the author of the message) shall have to pay compensation, unless he or she is able to prove that they adopted all the precautionary measures available in order to avoid the damage.

Circumstances in Which Law No. 675/1996 Shall Apply

As mentioned above, Law No. 675/1996 shall apply when images, sounds and other personal data collected:

- are successively communicated, systematically, to one or more addressees other than the data subject; or
- are disseminated amongst undetermined subjects in any form whatsoever, including making the data available as searchable content on the Internet.

In the above specified cases, where the "exclusively personal purposes" cannot be recalled, Law No. 675/1996 shall consequently be wholly applicable, starting from the initial collection of personal information/images.

This means that the "data controller" (*i.e.*, "any natural or legal person, public administration, body, association or other agency that is competent to determine purposes and methods of the processing of personal data, as also related to security") responsible for the processing of any personal data contained in the MMS must first inform the data subjects in accordance with Article 10 (information provided when collecting the data) of Law 675/1996. Article 10 provides, *inter alia*, the following:

> The data subject as well as whoever is requested to provide personal data shall be preliminarily informed, either orally or in writing, as to:

- the purposes and modalities of the processing for which the data are intended;
- the obligatory or voluntary nature of providing the requested data;
- the consequences if he or she fails to reply;
- the subjects or the categories of subjects to whom the data can be communicated and the area within which the data may be disseminated;
- the rights as per Article 13.

The information mentioned above shall be provided to the data subject at the time of recording such data or, if their disclosure is envisaged, no later than the time at which the data are first disclosed.

Further, consent to the processing of their personal data by means of MMS shall have to be given by the data subject (consent may be given orally, but if "sensitive data" are processed, consent must be expressed in

writing), unless cases of derogation from the obligation to obtain previous consent are provided according to Law No. 675/1996.

The IDPA points out that the specific rules provided by the Italian Privacy Law with regard to the processing of personal data within the scope of the journalistic profession, or in the case of occasional publication of articles or essays, or in other cases of free expression of ideas and thoughts, shall in any case apply. For example, the specific set of rules provided for the journalistic profession (Article 25 L. 675/1996 and the Self-Regulation Code adopted by the related Association), shall also apply in the use of MMS, even if the IDPA recalls the important principles set forth in its Act of 1998, in which the Authority specified that – on the one hand – the processing of personal data within the scope of the journalistic profession is based on less strict limitations with regard to the protection of privacy, but – on the other hand – only if the requirement of the "essentiality of the information relating to facts of a public interest" is matched.

Use of MMS and Compliance with Other Obligations

Whoever uses MMS, independently of the application of Law No. 675/1996, must in any case comply with the other obligation set forth in different civil or criminal provisions with the aim of protecting third parties. Individuals must also comply with this obligation where MMS is used exclusively for personal purposes (as seen above, in this case Law No. 675/1996 shall not apply).

The collection, communication and eventual dissemination of images and sounds relating to subjects of interest must comply with Article 10 of the Italian Civil Code ("Abuse of third party's image"), which prohibits the unauthorised use of the third party's image and any use of the image, which might compromise the data subject's dignity and fundamental rights.

Further, the use of MMS must comply with the Italian provisions in the field of Intellectual Property and Copyright Regulations (see Article 96 of the Italian Copyright Law No. 633/1941) and successive modifications:

> "Subject to the provisions of the following Article, the portrait of a person may not be displayed, reproduced or commercially distributed without the consent of such person"; and
>
> Article 97:
>
> "The consent of the person portrayed shall not be necessary when the reproduction of the portrait is justified by his notoriety or his holding of public office, or by the needs of justice or the police, or for scientific, didactic, or cultural reasons, or when reproduction is associated with facts, events and ceremonies which are of public interest or have taken place in public. The portrait may not, however, be displayed or commercially distributed when its display or commercial distribution would prejudice the honour, reputation or dignity of the person portrayed".

Finally, the person using MMS shall have to take into consideration that such activities could imply the commission of certain crimes, such as:

- the illicit collection, disclosure or dissemination of images related to private life occurring in third parties' houses or in other places of private residence could be punished according to Article 615-bis of the Italian Criminal Code ("illicit interferences in private life");
- the crime of offence to a person's dignity, in the case of particular messages sent with the aim of offending the personal honour of the addressee (Article 594 of the Italian Criminal Code);
- the crime of obscene publications (Article 528 of the Italian Criminal Code); and
- crimes punishable by the Italian Law No. 269 of August 3, 1998, enacted to fight child pornography.

Any users of MMS will have to evaluate carefully all the circumstances and consequences as outlined above, in order to avoid acting illegally.

Final Suggestions

The IDPA points out three further aspects to complete the framework of guarantees:

- managers of certain places which are open to the public or subject to conditional access (*e.g.*, sport clubs, fitness centres, gyms, *etc.*) are required to prohibit or at least permit with due caution, the use of MMS in their facility. Members will be obliged to comply with the policy.
- a second aspect concerns the constitutional protection of the freedom and secrecy of telephonic communications, which implies the prohibition – even criminally sanctioned – for TLC service providers to retain MMS contents and/or, to access them by means of other persons in charge, except for the cases of particular services required by subscribers (based in any case on previous informative and due consent);
- the third and final point concerns the eventual temporary retention of MMS by TLC service providers, offering certain services for the sending and receiving of MMS. In particular, this applies to subscribers whose mobile phone devices are not technically capable of receiving MMS. In such cases, if MMS are made accessible to the subscriber/addressee via the Internet (through the provision of a personal pin code to the subscriber, by which he or she can access the stored MMS), the service provider is required to discontinue the storage of such data within a reasonable timeframe (usually considered to be once the addressee has accessed the data). The potential security risks raised by providing subscribers with their personal codes of access by the use of SMS will also need to be considered.

News

MEXICO

House of Representatives Plans Federal Privacy Legislation

The Commission of Trade and Industrial Promotion, part of the Mexican House of Representatives has recently organised a workshop to draft a bill on privacy. The content of the bill would cover the collection and processing of personal data of individuals and the regulation of transborder data flows, in both the online and offline environments.

The workshop has brought wide participation from different sectors, including IT and Telemarketing companies, Banking Institutions, Public Notaries, NGO's, Academic Institutions, Chambers and Associations. Representatives from government entities like the Banking Central Authority (Banco de México), Ministry of Economy (Secretaría de Economía), Federal Consumer Agency (ProFeCo), The National Institute on Information, Geography and Statistics (INEGI) and the Public Policy Development Office of the President's Office have also been involved.

The move comes following the introduction of two previous draft bills. The first bill was introduced before the House of Representatives on September 2001 by a representative from a left wing party (PRD). The second emerged from the Senate on April 2002. The two draft bills were then sent to the Commission of Trade for constitutional revision. It is important to point out that neither of these draft bills has been passed, mainly because they did not have the approval of the interested sectors of the Mexican society, which lead to the Commission of Trade organising a special workshop on these topics. The purpose of the workshop is not only to revise the two draft bills, but also to obtain feedback from the aforementioned sectors as to their views on the impact that the bills would have if approved, as well as their views on best practice for privacy regulation in general. In this way, the Commission of Trade aims to adopt a viable approach to regulating both the protection of individuals' personal data and transborder data flows that will be acceptable to all.

Considering there is only a short time available to the Commission of Trade in which to draft a comprehensive bill before the close of the current parliamentary session, it is highly unlikely that Mexico will have a privacy law in 2003. However, the Commission of Trade hopes to come up with a series of conclusions and agreed views with the participant sectors on the regulatory approach that can then be implemented after April 30, 2003 (the day on which the LVIII Legislature will end).

It is important to at least secure a draft bill so that the new Legislature coming in on October 2003 can re-visit the findings of the workshop and propose a solid piece of legislation to the Senate.

The preliminary draft bills and the presentations of this workshop are available in Spanish on the Commission of Trade's website at: *http://200.15.46.216/comcome/doctos/datos.asp*

By Cristos Velasco, Instituto Tecnologico Autonomo de Mexico (ITAM); e-mail: cristosuofa@yahoo.com

Banking Secrecy in Singapore: the Impact of the Consumer Credit Bureau

By Rizwi Wun, a Senior Associate of the IP & Tech Practice in Khattar Wong & Partners, Singapore. The author may be contacted by e-mail at: wunrizwi@khattarwong.com

Introduction

Credit Bureau (Singapore) Pte Ltd[1] ("the Bureau") was set up in Singapore in September 2002 in response to the long awaited need amongst banks in Singapore for a way to more easily assess the creditworthiness of their customers.

The Bureau has been helping financial institutions mitigate their credit risk through information pooling. It has enhanced the risk management policies of banks and financial institutions in Singapore who are members of the ABS ("Members"). Members will give selected credit information on their customers to the Bureau. The credit information is then collated into a credit report ("Credit Report") by the Bureau, and made available upon request to Members and other institutions approved by the Monetary Authority of Singapore ("MAS") for the limited purpose of assessing the credit worthiness of their customers. Such personal credit information is vital in order for Members to make timely decisions on whether to grant or sustain credit facilities.

Providing the Legal Framework: Amendments to Banking Secrecy Law

The Singapore Banking (Amendment) Act 2001 amended the existing Singapore Banking Act ("the Banking Act") and completely revamped the banking secrecy provisions in Singapore.

These amendments set out the legal framework for, amongst other things the disclosure of personal credit information by banks to a credit bureau and for disclosure by the credit bureau to others, and the terms of such disclosure, in the form of a legally recognised exception to general banking secrecy obligations.

The general basic rule of banking secrecy in Singapore is that

> "customer information shall not in any way be disclosed by a bank in Singapore or any of its officers to any other person except as expressly provided for in this Act".[2]

The Banking Act defines "customer information" as:

> "any information .... relating to an account of a customer of the bank, whether the account is in respect of the loan, investment or any other type of transaction" or "deposit information".

Deposit information is defined as:

> "any information relating to any deposit of a customer or, funds of a customer under management by the bank or any safe deposit maintained by, or any safe custody arrangements made by a customer".[3]

The significance of distinguishing the classes of customer information will be seen below.

A bank in Singapore may for specified purposes disclose customer information to specified persons or class of persons, provided such disclosure is in compliance with certain specified conditions as follows:[4]

- Disclosure that is only strictly necessary:
  - for the collation, synthesis or processing of customer information by the credit bureau for the purposes of the assessment of the creditworthiness of the customers of the bank; or
  - for the assessment of the creditworthiness of the customer of banks by another bank or merchant bank or a person as authorised by the MAS to receive the information, who are members of the credit bureau.
- Disclosure may only be made to:
  - a credit bureau of which the bank is a member; and
  - other members of the credit bureau who can be another bank or merchant bank or persons authorised by MAS to receive such information, where such other members receive such information from the credit bureau.
- No deposit information shall be disclosed;
- The disclosure by any credit bureau to other members of the credit bureau who can be another bank or merchant bank or persons authorised by MAS to receive such information, where that member receives such information from the credit bureau may be subject to conditions specified by MAS.

This means that:

- no information on the net worth of the customers can be disclosed by banks to the credit bureau, and
- the disclosing bank can only disclose to a credit bureau of which it is a member;
- anyone wishing to receive information can only do so for the limited purpose of assessing the creditworthiness of a bank's existing customer.

Under this new legal environment, the Bureau was approved by MAS as a credit bureau for the purposes of the Banking Act.

Privacy Concerns of the Public and the Safeguards Available

Banks have been amending the terms and conditions governing their customers' accounts to accommodate the new obligations in respect of the Bureau and have been giving notice of the same to their customers. This will provide a legal basis for the disclosure of such personal information to the Bureau.

Some members of the Singapore public have not been happy with the increased access to their credit history. Customers are concerned over the intrusion into their privacy, the lack of choice and consent over the secondary use of their personal information in the Credit Report, and the apparent lack of an effective procedure for redress. The other main cause for concern is the risk that the personal credit information available in the Credit Report may not be updated, resulting in an incorrect decision being made by the assessing party.

To this end, various safeguards have been put in place.

Criminal Penalties

Recipients of credit information are not allowed to make further disclosure of customer information unless authorised by the Sixth Schedule of the Banking Act or ordered by a court to do so.[5] A contravention of this restriction would result in the penalties set out below.

In addition the obligation on every officer or other person who receives customer information under Part II of the Sixth Schedule of the Banking Act continues even after the cessation or termination of his appointment, employment or other capacity in which he had received the customer information.[6] Potentially this means that the obligation stays with him for the rest of his life!

The Banking Act provides that any breach of the banking secrecy provisions is a criminal offence and subject to the following penalties:

- anyone in violation of the provisions will be liable to a fine of up to S$125,000 or a term of imprisonment of up to three years or both;[7]
- a bank, being a body corporate, will be liable to a fine of up to S$250,000,[8]
- any director, managing director or manager of a bank who fails to take reasonable steps to secure compliance with the provisions of the Banking Act will also be individually liable to a fine of up to S$50,000 or for a term of imprisonment of up to three years or both, unless he can show that he had reasonable grounds to believe that another person was charged with the duty of securing compliance with the requirements of the provisions infringed and that other person was competent and in a position to discharge that duty.[9]

To this end, the ABS assures that only relevant data would be given. The Credit Report will disclose basic personal information, payment trends and payment credit history and records obtained from public sources, but will not reflect the credit limit or periodic amounts paid. Neither will they disclose the net worth of customers.

Compliance with MAS Requirements

Only credit bureaus accredited and recognised by MAS will be allowed to receive and disclose customer information.

The MAS has given the assurance that individual privacy is paramount and data cannot be disclosed for purposes other than for which it was originally intended. High standards of confidentiality are expected of both the operators of the Bureau and of the Members.

The Singapore Parliament has stressed that the MAS will only accredit and recognise a credit bureau that can adequately address the financial privacy concerns and that can provide accurate Credit Reports. One such factor would be through compliance with a Code of Conduct. Should the credit bureau fail to maintain the high standards expected of it, MAS will not hesitate to revoke the recognition of that credit bureau.

Code of Conduct

The Bureau operates on a self-regulatory basis in strict adherence to a Code of Conduct.

This Code of Conduct[10] sets out in reasonably detailed terms, amongst other things, the following:

- Application of the code;
- Member's supply of received information to the Bureau;
- Bureau's obligations in respect of information;
- Member's obligations in respect of information obtained;
- Individual's access to own information;
- Investigation into disputed information;
- Rectification and updating of information by the Bureau; and
- Complaints as to breaches of the Code.

The significance of this Code is that it gives individuals whose customer information may be stored with the Bureau the right to access, conduct investigations as to any dispute, and even initiate a complaint against breaches of the Code. There is also in place provisions for a Compliance Committee to oversee the implementation of the Code by the Bureau.

The Future

Ultimately the justification of the Bureau stems from the confidence that the general public can draw, that customer information the Bureau receives and discloses is done in strict accordance with the law and the Code of Conduct.

The Bureau has only been in operation for about six months, and has seen an average of 20 requests per day for Credit Reports. At the moment, 10 banks with a local presence are members of the Bureau. While some customers have protested against the intrusion into their privacy, there have been no other problems so far.

The benefits and convenience of the service provided by the Bureau outweigh the concerns raised by the public over the lack of privacy in the dissemination of their personal credit information. Amid reports of local banks writing off S$124 million of bad debts in 2002 (a staggering increase of 56 percent over the previous year), the value of providing quick and accurate information for credit assessment, especially in the current economic downturn, cannot be underlined enough.

1 Credit Bureau (Singapore) Pte Ltd is currently the only consumer credit bureau in Singapore and is a joint venture between the Association of Banks in Singapore (ABS) and DBIC Holdings Pte Ltd. DBIC Holdings Pte Ltd is related to Dun & Bradstreet and was incorporated for the sole purpose of setting up the Consumer Credit Bureau with ABS.
2 Section 47(1) Banking Act.
3 Section 40A Banking Act.
4 Paragraph 7, Part II of the Sixth Schedule of the Banking Act.
5 Section 47(5) Banking Act.
6 Section 47(7)(b) Banking Act.
7 Section 47(6)(a) Banking Act.
8 Section 47(6)(b) Banking Act.
9 Section 66 Banking Act.
10 See *www.creditbureau.com.sg/CodeofConduct.htm*

Case Reports

FRANCE

■ ECHR RULES ON "ANONYMOUS BIRTHS"

Odièvre v. France

European Court of Human Rights, February 13, 2002

In a judgment dated February 13, 2002,[1] the ECHR rejected by 10 votes to seven, the request of a French national abandoned by her parents, for the name of her birth mother to be disclosed.

The applicant was born in 1965 in Paris. At this time, the applicant's mother requested that her name remain confidential and completed a form at the Health and Social Security Department by which she officially gave up her daughter. After being placed at the Children's Welfare and Protection Service, the applicant was eventually adopted at the age of two by the Odièvre family.

The applicant first brought a petition before the *Tribunal de Grande Instance* of Paris, which was rejected for lack of jurisdiction to the benefit of the Administrative Court. Following this decision, she submitted the case to the ECHR. The applicant claimed that because the French legal system admitted anonymous birth it was impossible for her to trace her origins, which constituted a violation of the rights guaranteed by Article 8[2] and Article 14[3] of the Convention.

Anonymous Births Under French Law

In France, legislation has authorised anonymous births since the time of the French Revolution. French birth certificates include a line where the mother may put an X instead of writing her name. This means that the child can be adopted. Every year, approximately 600 women choose this option and give birth anonymously. On January 22, 2002, a new statute relating to "the Access to information about their origins by adopted persons and people in state care"[4] was passed. The new statute created a new institution, the "National Council for Access to Information about Personal Origins" which will be in charge of centralising all paperwork relating to anonymous birth and communicating the mother's identity, provided that the mother and child agree. The creation of this institution has not however, resolved the right for children to access data on their origins, since such access remains subject to the mother's consent.

Violation of the European Convention on Human Rights

Article 8

The applicant complained that she had been unable to obtain details identifying her natural family. She alleged a violation of Article 8 of the Convention considering the establishment of her basic identity as an integral part of her private and family life. Her counsel stated that "everyone has the right to a private life, and knowledge of one's origins is an essential element of this".

The Court admitted that:

> "birth and in particular the circumstances in which a child is born forms part of a child's and subsequently the adult's private life guaranteed by Article 8 of the Convention".

However, the Court decided by 10 votes to seven that there was no violation of Article 8 of the Convention, since the French legal system sufficiently took into account and attempted to balance all the interests at stake. The Court considered that there were three points in particular which needed to be considered:

- first, the child's right to know its origins versus the mother's right to remain anonymous;
- secondly, general interest, *i.e.*, the health of both the child and the mother (giving birth in appropriate medical conditions to avoid for example, illegal abortions). In this respect, Judge Ress[5] observed that:

> "While recognising the child's fundamental right to receive information about its biological origins and ascendants under Article 8 of the Convention, the State authorities may, in accordance with Article 8 § 2, nevertheless implement measures that are designed to protect the rights of others and the general interest. It is clearly in the general interest for appropriate measures to be taken to improve the situation of mothers in distress and to protect children's lives by reducing so far as possible the number of abortions. That, to my

mind, is an overriding consideration that may prevail over the child's right to know its origins".

In a joint dissenting opinion, Judges Wildhaber, Bratza, Bonello, Loucaides, Carbal Barreto, Tulkens and Pellopää,[6] however, considered that:

"it has not been established, in particular by statistical data, that there has been a rise in the number of abortions or cases of infanticide in the majority of the countries in the Council of Europe that do not have legislation similar to that existing in France"; and

- finally, third party interests, *i.e.,* essentially the adoptive parents, the natural father and other members of the natural family.

In view of these interests, the Court explored the issue "[does] the right to know imply an obligation to divulge"? The Court observed that the applicant had been given access to non-identifying information about her mother and natural family that permitted her to trace some of her roots, while ensuring the protection of third party interests. Furthermore, the Court noted that the 2002 Statute improves the prospect of mothers agreeing to waive confidentially. Consequently, after reinforcing the Member States' margin of appreciation in balancing all the interests at stake, the Court concludes that the French legal system does not violate Article 8 of the Convention.

Article 14

The applicant alleged that anonymous births constituted a violation of Article 14 of the Convention since it took away her right to inherit from her natural mother and therefore discriminated unfairly against her. By being prevented from establishing her basic identity, she was prevented from claiming any inheritance she might have been eligible for.

The Court rejected this argument, observing that there was no discrimination under Article 14 of the Convention because the applicant could inherit from her adoptive parents.

1 *http://hudoc.echr.coe.int* case of *Odièvre v. France*, application no. 42326/98.

2 Article 8 provides that "Everyone has the right to respect for his private and family life".

3 Article 14 provides that "The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any grounds such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status".

4 Law no. 2002-93, January 22, 2002, JO no. 19, p. 1519.

5 *http://hudoc.echr.coe.int* case of *Odièvre v. France*, application no. 42326/98, p. 24, no. 1 "Concurring opinion of Judge Ress".

6 *http://hudoc.echr.coe.int* case of *Odièvre v. France*, application no. 42326/98, p.28, no. 9.

By Laurent Szuskin and Myria Saarinen, Partner and Associate respectively, Latham & Watkins, Paris. The authors may be contacted by e-mail at: laurent.szuskin@lw.com; or myria.saarinen@lw.com

FRANCE

WEBMASTER CONDEMNED FOR UNLAWFUL TREATMENT OF DATA

Ministère Public et M. Philippe A. v. M. Roger G

On February 18, 2003, The Correctional Tribunal of Villefranche-sur-Soane, condemned a net user for the non-declaration of the disclosure of personal data (of others) on his website to the competent French authorities.

Decision

Mr Roger G, an Internet user, set up his own website. From March 1997 to August 2001, he published nominal information without having declared such disclosures to the *Commission Nationale de l'informatique et des Libertés* ("CNIL").

Amongst the data being published was the name of the victim, M. Philippe A., who decided to sue for damages and to obtain a criminal conviction against Mr Roger G.

The webmaster admitted that he was delayed in declaring his website to the relevant authority (the CNIL), because he was unaware of this legal requirement. He claimed that this was due to a lack of information in the media and from the access providers. The Tribunal rejected this argument.

The Correctional Tribunal fined the webmaster EUR450 and awarded EUR1.00 in damages to the victim on the grounds of the civil action.

Comment

Data protection in France is governed by a 1978 Act known as "Loi n°78-17 *relative à l'informatique, aux fichiers et aux libertés*". This Act protects nominal data, that is to say, data in whatever form, which will allow, directly or indirectly, the identification of physical persons, whether physical or legal persons execute the treatment (Article 4). The application of this Act is controlled by the CNIL, which is also responsible for agreeing to treatment submitted for its approval. As of April 2003, the 1995 European Directive still has not been implemented into French law and despite the introduction of a Bill before Parliament at the start of 2002, the 1978 Act still applies. (The Bill was suspended due to presidential elections last Spring.)

Article 16 of the 1978 Act requires that webmasters undertake a declaration to CNIL before their website is launched.[1] This declaration contains a commitment that the treatment of data will conform to the legislation applicable.

Failing to undertake the declaration constitutes a criminal offence, punishable by Article 226-16 of the French Penal Code. Article 226-16 stipulates that proceeding to disclose or process nominal data without ful-

filling the formalities required, prior to the start of the treatment of such data, is punishable by a three-year prison sentence and a EUR45,000 fine. The offence is constituted even when the non-declaration does not occur maliciously but as the result of negligence.

It was on this basis that the judge from the Correctional Tribunal of Villefranche-sur-Soane condemned Mr Roger G. The fact that he did not proceed to the declaration was not disputed and it is logical that the Tribunal applied Article 226-16. It is important to note that the sentence in itself does reflect the fact that Roger G did not maliciously refrain from making the declaration and that the damage caused by the absence of declaration was minimal. Indeed, out of the criminal sentence available to the judge (three-year imprisonment and a EUR45,000 fine), Roger G was condemned to a fine of a mere EUR450. Besides, the civil damages requested by the victim, Mr Philippe A were of the sum of EUR15,000. The Tribunal recognised the damage but refused to follow the victim's stance that any substantial damage had occurred as a result and awarded only EUR1.00 in damages.

But the amount of damages or the size of the fine is not the significant part of the decision here. Indeed, what needs to be noted from this case is the attempt to reinforce the application of the 1978 Act to the treatment of nominal data by physical persons outside business purposes.

This decision is not the first in the area of data protection to make application of the 1978 Act to situations where a non-professional is disclosing nominal data on his personal web pages.

Article 226-19 of the Penal Code also relating to data protection has already been applied by the French jurisdictions. This article states that outside cases enumerated by the law, the storage or conservation of nominal data, without the agreement of the data subject, which is directly or indirectly showing racial origins, political, philosophical or religious opinions, membership to a union, or the morality of a person is prohibited. Violation of this rule is subject to a five-year imprisonment and a EUR300,000 fine.

This ground was not used as a basis for the *Ministère Public et M. Philippe A. v. M. Roger G* decision, but was referred to by the judgment as a possible ground for action in the case.

In 1997, this Article 226-19 was used successfully in the case of *Ministère Public et Mademoiselle S v. Monsieur F*.[2] In this case, the creator of a website was condemned to a suspended sentence of eight months imprisonment and to a EUR760 fine and ordered to pay EUR3,058 in damages. Mr F, the website creator, was condemned for having published some pornographic pictures of his ex-girlfriend on his personal website without her consent, as revenge for their separation. The pictures were accompanied by unflattering comments on the morality of Mademoiselle S.

The judge in this instance considered that the pictures were protected by the 1978 Act as they allowed the identification of the person concerned. Mr F's actions were therefore, in violation of Article 226-19 since Mr F did not have the agreement of Mademoiselle S for the publication.

Application of 1978 Data Protection Act is Reinforced

With this latest decision from the Correctional Tribunal of Villefranche-sur-Soane, the application of the 1978 Data Protection Act is reinforced, reminding every website user that however little the disclosure or however misinformed, criminal sanctions can be applied. If the sum involved was fairly small in the case of Roger G (although we are unaware of his financial situation), it is important to highlight that the condemnation will appear on his criminal record. In France this can have important implications, as employers tend to require a copy of any criminal records held by potential employees and may base their selection on the necessity for potential employees to have a clean criminal record. This could jeopardise Mr Roger G's chances of securing a new job should he be required to do so. Furthermore, depending on Mr G's profession, his future career prospects may also be undermined.

We agree with the trend to treat any non-declaration of nominal data disclosure harshly, as it is an important tool to fight data misuses and afford a data subject sufficient rights on the disclosures executed. Moreover, the application is only the strict application of Article 4 of the 1978 Act that includes disclosure executed by physical persons as well as legal persons.

However, the strict application of the criminal sanctions of the 1978 Data Protection Act creates some objections.

Indeed, it is only in scarce circumstances that the Act is enforced in situations where persons are acting outside their professional activities. As the two cases mentioned also illustrate, it is only due to the victims' own initiative that an action was launched and not as a result of proceedings brought by the CNIL. (N.B., although the CNIL has the right to pass on cases to the criminal apparel (even in cases involving professionals handling nominal data), it has only used this privilege on rare occasions.[3)]

Equally it is striking to note, as the *Forum des droits sur l'Internet*[4] observes, that out of 3.2 million personal web pages registered in France with different hosts (mainly access providers) only 23,000 are declared to the CNIL. This statistic seems to illustrate that the French data protection system is inefficient when dealing with the Internet and the disclosures made online.

In the light of such statistics, one can ask if it is fair for a few net users to be targeted so heavily and bear the weight of criminal convictions, particularly when it appears that the authorities concerned are doing little to stop the real offenders[5] who decide out of malice or for professional purposes to abstain from a declaration and treat nominal data for marketing purposes.

Is it time to rethink the declaration method for Internet sites and modernise French data protection legislation? Even before attempting to answer this question, it is clear that the 1995 European Directive on Data protection must be transposed into French law as soon as possible. It is unwise however, to try and guess when the transposition will come about!

1 The declaration contains information relating to the person responsible for the disclosure; the characteristics, object and name of the disclosure; the service responsible for dealing with any data subject rights and queries; the nature of the data dealt with; the measures taken to ensure the security of the data; the disclosure of the data abroad; *etc.*

2 TGI Privas, Septembre 3, 1997.

3 Valerie Sedallian, *"La loi informatique et Libertés vue par la France d'en bas, ou le récit de candide au pays des merveilles"*, *www.juriscom.net*, December 17, 2002. According to the author, the CNIL made only 20 denunciations in 22 years at the date of July 15, 2002. It is also added that it is because the CNIL prefers consultation to repression.

4 *www.foruminternet.org*, Actualités du March 26, 2003, *"Un internaute condamné pour absence de déclaration de son site à la CNIL"*.

5 Jean Frayssinet refers to the CNIL as a *"Tigre de papier"* (which translate literally as a *"Tiger made out of paper"*) to illustrate the position this institution is in and its lack of efficiency in enforcing the applicable legislation (in *"Le projet de loi relatif a la protection des personnes physiques a l'egard des traitements de donnees a caratere personnel: constantes et nouv. nouveautes"*, Communication – Commerce Electronique Janvier 2002, p. 13).

By Dr Christine Riefa, Senior Lecturer, Faculty of Law, University of Hertfordshire. Dr. Riefa may be contacted by e-mail at: c.riefa@herts.ac.uk

News

THE NETHERLANDS

DPA Says Blacklist to Fight Fraud in Retail Trade is Illegal

The Dutch Retail Trade Council (Raad Nederlandse Detailhandel – RND) has been planning to set up a warning list with the names of retail personnel who have been dismissed for fraud or misconduct, in order to warn potential employers in the sector.

After conducting an investigation, the Dutch Data Protection Authority (CPB) came to the conclusion that such a blacklist is unacceptable in its current form, since it does not provide satisfactory guarantees for the careful handling of personal data and the protection of individual rights. In particular, it found, the inclusion criteria are too vague, and the definition of fraud is too broad, which may result in individuals being unfairly barred access to employment in the sector.

In a letter dated March 25, 2003, the CPB urges the RND to amend its warning list so as to meet the Dutch legal data protection requirements. This letter is available (in Dutch only) on the CPB website at: *www.cbpweb.nl/structuur/pag_nieuws.htm*.

Banks Rebuked for Non-Fulfilment of Information Obligations

In 2002, ING Bank, Postbank and RVS, which all belong to the Dutch ING Group, notified their clients in writing of their plan to store all client data in a centralised system. This was mainly to be done for marketing purposes. Numerous questions and complaints from clients prompted the CPB to conduct an investigation. At the beginning of April 2003, the CPB found that the three financial institutions failed to fulfill their obligations under the law, since

- it was not clear which data were to be shared; and
- the clients were misled into thinking that centralisation of the data would occur in compliance with an approved code of conduct for the processing of personal data by financial institutions, although the code still had to be approved at the time of the mailing.

The text of the conclusions is available (in Dutch) on the CBP website at: *www.cbpweb.nl/structuur/pag_nieuws.htm*.

By Christopher Kuner, Hunton & Williams, Brussels; e-mail: ckuner@hunton.com

Entitlement cards: Do the U.K. Home Secretary's Proposals Comply with Data Protection Principles? Part II

By Dr Perri 6, Director, The Policy Programme, Institute for Applied Health and Social Policy, King's College, London

The first part of this article considered a number of data protection problems with the recent British government proposals in their consultation for an "entitlement card" and the population register that will stand behind it (see *WDPR*, March 2003). In particular, it dealt with the application of the Article 8 necessity test, fair processing, and the appropriateness of the purposes, function and risk of excessive and irrelevant information. In this second part, issues of accuracy, disclosures from that central register, and security are considered.

Accuracy

Accuracy of data is the fourth and very important principle of data protection law in the United Kingdom.

In the consultation paper, the government makes some substantial claims for the improvements in the accuracy and quality of personal data that can be achieved through the implementation of the entitlement card system ("EnC") and the population register. The Home Office consultation paper, *Entitlement cards and identity fraud* ("ECIF") claims that the standard of accuracy of entries in the central register will be sufficiently greater than that of other government databases (2.26), that it will become the key tool in combating fraud (4.12), that overall efficiency in public services will rise (2.36), and that it could, in time, actually replace other registers such as the electoral register (2.36).

If these claims could be substantiated, then they would represent an important benefit from an EnC scheme, and one that would weigh with the Information Commissioner. However, it is not wholly clear from ECIF just what these claims are based on.

Accuracy of the central register for the EnC system would, if this is possible, be even more important than accuracy for other databases used to administer public services, if the intention is that it should be used to correct those other databases. Otherwise, it will present significant risks of "error infection" or the transmission of errors to other databases, making them harder to eradicate.

Most databases contain significant numbers of errors. The levels of errors in the Criminal Records Bureau databases were a major scandal during 2002. At various times in its history, the Child Support Agency has been in the news for the high rate of errors in its databases leading to inappropriate decisions. The Audit Commission has recently reported in a study of health records that it has found "obvious errors", some minor and some less so, without detailed checking, on the face of some 40 percent of health records (according to Dr Marion Chester, Association of Community Health Councils in England and Wales, in a presentation to the Privacy International, Liberty and Foundation for Information Policy Research meeting at the London School of Economics, December 11, 2002). The Audit Commission (2002, 5) also recently stated that NHS bodies still "have a long way to go" to improve the quality and accuracy of patient-based information). The Driver and Vehicle Licensing Authority's own study of the accuracy of its databases suggests that between 24 percent and 30 percent of all records contain at least one error – mostly in postcode and address fields and also in names – even on the narrowest definition of an error, and 91 percent of all forms submitted contained some error (National Audit Office, 2002, 13-14).

Data will accrue to the central register for the scheme in several ways:

- some data will be internally generated: for example, the unique personal identifier will be generated by some algorithm internal to the system;
- individuals will voluntarily supply data at the point of application in the form of their own written information and in the form of any supporting documentation they must submit with their application, and at various times thereafter if they provide updating information;
- information will be obtained through checks made in the course of making decisions on applications, and this may involve some data matching and data sharing across the public sector, and may also involve buying data from commercial credit reference agencies and other private bodies; and
- some data will be captured automatically, for example, at the point of card validation, and in the construction of any audit trails of the use of the card.

Data accrued to the register may then reach the record for an individual in a variety of ways:

- it may be entered manually by a data entry clerk into fields in the record;
- it may be read from some analogue source by machine and transformed into digitised material and those data routed into fields in the record; or
- it may be collected from another digital source, its classification taken or else checked and corrected, and then routed into fields in the record.

Finally, there may be combinations of these methods for certain kinds of information that must be assembled from several sources. Having been entered, the data may then be checked either manually by a human being reading them and checking them against other sources, or they may be checked by using data matching. A data matching algorithm, having identified any items of discrepancy that could be errors, may simply flag up those discrepancies for a human being to make a decision upon, or may use some recommendation-generating system to identify a proposed correction, or could be programmed in some circumstances to make changes automatically.

Each of these methods of data accrual carry certain types of risk of generating errors at the stage of data gathering, data entry and data checking. In general, any system for reducing the numbers of errors in databases will only achieve those reductions if additional expenditure can be supported to enable additional manual and automatic checks, and at the cost of additional time taken between the date of data acquisition and the date at which a record is signed-off as correct.

The response to the recent consultation paper published by the British Computer Society (2003) points out that a critical element in ensuring accuracy will be the process by which new applications for cards are checked against the central database of those who have already applied and been granted a card. If an entry already exists on the database for an individual and a new application is made for a card for that individual, this will, as the Society notes, be a *prima facie* indication that something has gone awry. However, it is quite possible that the first applicant, who may have been successful in securing the issue of card, is the fraudster, and therefore the existing record is the inaccurate one. Indeed, fraudsters are likely to recognise that it is to their advantage to make applications early, if they intend to apply in the names of other individuals who are alive and resident in the United Kingdom (as opposed, for example, to applying in the names of deceased persons). This raises a number of issues for the management of the database to ensure the highest levels of accuracy. For example, should the burden of proof and the presumption of innocence lie with the first applicant or the new applicant? If the issue of a card to the new applicant is delayed until investigations are completed into the possibly wrongful prior issue of a card to someone who turns out to have applied fraudulently, then how long a delay would be acceptable? How costly will it be to detect inaccuracy after the fact where this arises from successful fraud in securing an entry in the central database early? On these questions, ECIF is largely silent. Some can and perhaps would have to be dealt with in a code of practice, but ECIF does not set out this fact clearly.

The cost estimates presented in Annex 5 of ECIF do not include a detailed breakdown of the costs for improving accuracy, nor indeed does the document as a whole include any specific targets for levels of errors. It notes that the process will require the hiring of staff and the investment in and installation of hardware and software including systems to support biometric recording and recognition. But little is said that is specific about how the aspirations for greater accuracy will be met. In general, in order to improve accuracy in the handling of biometric data, and to reduce false positive and false negative results, it is necessary to use more expensive systems.

Moreover, some of the ways in which the document as a whole discusses processes, which would impact upon possibilities for error reduction, do give rise for concern.

For example, Paragraph A5:21 suggests that additional investment in capacities for biometric checking and other automated checking systems will reduce the need for staff. The history of large information technology projects is that net reductions in the demand for labour take a very long time to show up, and that in the short and medium run, additional staff are often required, albeit in very different roles from those which such organisations may have required before the new investment.

ECIF also stresses that the government will seek to simplify and speed up the application process. The Home Office "Frequently asked questions" document (Home Office, 2002), for example, states that few additional calls for information will be made over and above those required for passport and driving licences today, save for at most a single face-to-face meeting with the applicant (Q.23). Such a meeting would certainly increase the complexity of the application process, but would do little in and of itself to reduce the error rate in entries in the register, not least because meetings at the point of application would take place before much of the data to be entered had been acquired by the central registration body. If delays in handling applications are to be reduced in order to achieve the ambitious roll-out targets, and the goals for reductions in identity fraud also achieved, and the rate of errors in the register database at the same time reduced to levels significantly below those of other government databases, then substantial additional resources must be spent on checking. Only significantly increased resources can mitigate the trade-off between simplicity and speed on the one hand, and error minimisation on the other.

Many of the accuracy problems will arise after the initial application stage. ECIF states (6.13) that card-holders would be legally required to inform the central register authority of changes to information held about them, including a change of address. This is already a duty for holders of driving licences, but in practice significant numbers of people do not comply with the duty, and this has resulted in serious levels of inaccuracies on the database. It is often found to be disproportionately costly, given the benefits of the scheme, to police non-compliance very actively. It is hardly possible to apply drastic sanctions for failure to provide up-to-date information in all but the most egregious cases, since most failures are the result of absence of mind rather than any deliberate attempt to defraud or deceive. Updating changes of address might become a

less severe problem for those people who have reasons to access a number of public services, if data sharing between those services and the central register is permitted. However, that would require a number of specific "gateways" to be authorised in the statute, and ECIF does not set out adequate proposals for this. However, many people who work in the private sector and claim no means-tested benefits and are in good health may use few public services other than the Inland Revenue. Updating of information from the Inland Revenue to the central population register would raise a number of problems in the minds of the public, because personal financial details are regarded by many people as a category of personal information that they want to feel is kept strictly separate from other kinds of information held about them. Even if this were to be overcome, it also has to be recognised that the Inland Revenue databases are not always accurate or fully up-to-date: indeed, recent press reports have suggested that the number of errors in Inland Revenue databases may be increasing. In general, this method of updating by taking data from other public services itself raises accuracy risks by way of "infection" with data that are wrongly believed to be correct and up-to-date. These risks can be reduced only at greater expense per case, by providing for investigation and checking. Perhaps more fundamentally, it undermines a goal that ECIF sets out for the scheme, that the central population register should be so accurate that it will be used to update other public services' databases, and not the other way around.

It *may* be possible to produce a database of this kind that will be systematically more accurate than most databases currently in use in the public sector. However, it must be realised just what an undertaking this would be. To achieve greater accuracy than is achieved by other databases, and to sustain it over time is extremely ambitious in a scheme that has the following characteristics:

- it is expected to be a register of almost the entire adult population, but one in which many people will hold more than one card;
- it is to be assembled and in use in a period of just a few years;
- it is to be assembled using a variety of distinct sources of information, each of which may contain errors;
- it is to be constructed using a variety of entry systems each of which runs risks of errors; and
- it is to interface with a wide variety of other databases for public and possibly commercial services.

The consultation paper does not really substantiate its claim that this is achievable, for it fails to set out a sufficiently clear and structured set of methods and costs for this. Moreover, the consultation paper does not explain how the three-cornered trade-off between controlling cost, reducing delays and complexity at the point of application and improving accuracy is to be managed.

This conclusion has, I believe, some important consequences for the whole EnC programme. If significantly greater accuracy than other public service databases cannot be achieved, then many of the programme's expectations, that it will enable officials to identify people who are not entitled to services and to deny services to those people more accurately and cost-effectively and with fewer "false positives" than current systems can, will in turn not be met. In that case, a significant part of the economic justification for the programme must be called in to question, for in part that argument rests on the claim that the costs of administering the programme will be offset and even outweighed by the savings made from improved targeting of services and detection of illegal immigrants and people working illegally. If it is true that accuracy can be improved only with substantially greater expenditure on the programme, then the question must be asked afresh about the cost-benefit assumptions that lie behind the argument in ECIF.

Disclosures

Data Protection law regulates and limits permitted types of disclosures in a variety of ways. The most general is part of the fair and lawful processing condition, and this is interpreted (Information Commissioner, 2001, paragraph 3.1.4) to mean that disclosures must be limited by duties of confidentiality, the *ultra vires* rule and the scope of specific powers, legitimate expectations of the data subject, and Article 8 of the European Convention on Human Rights which provides for the right to private life. Secondly, the general conditions for processing impose a series of necessity tests on disclosures, and the limb which permits disclosures in the legitimate interests of the data controller or the third party to whom the data are to be disclosed is also limited by a test of necessity; necessity here must be read in the light of the specified and limited purposes.

Regrettably, ECIF does not contain a clear and fully integrated discussion of the disclosures envisaged from the central register to other databases used to provide public and private services. What follows therefore, is based on what can be gleaned from several paragraphs scattered across the document. The following are types of disclosures that would be made without specific consent.

- Disclosures are made visually, when the information displayed on the face of the card is read manually, whenever it is presented.
- Disclosures are made at the point of card validation. At the very least, at this stage, the card reader device receives the information that a valid card has been presented; the reader device may retain some kind of audit trail of card numbers, which could be retained by the particular service and, at least in principle, later be correlated with individuals.
- Disclosures are made at the point of biometric identification. At the very least, the card reader device receives the information that the person presenting the card is indeed, on the biometric

evidence, the person entitled to hold it; again, this may be retained by the particular service.

- Disclosures are made at the point of face-to-face contact with service providers. In one scenario set out in ECIF, the cardholder is asked for, say, the second word of a passphrase in order to enable a check with the central register: the whole passphrase is not revealed. However, if a different word were demanded on each occasion of face-to-face contact by a service used frequently, it would quickly become possible to assemble the phrase. The other principal example in ECIF of disclosure at the point of face-to-face contact is that of emergency medical care, where a person has consented in advance to the holding of some health information either in their card or accessible through it, and a paramedical officer uses their card to access that information.

There would in addition, be a number of disclosures that could be made with consent. Where the information sought is not statutorily required or deemed implicitly necessary for fulfilling a statutory requirement, the service provider might ask the cardholder for permission to download those pieces of information from the central register (and perhaps retain them on the service provider's database). The system might use the digital signature on the card, perhaps with a word from the passphrase, to record with the central database that consent had been given.

This will raise some complex issues which are not really addressed in ECIF, but which would have to be clarified, about the later withdrawal of consent. How would the cardholder communicate their withdrawal of consent? Could it be retrospective? How would this be processed?

However, where giving that consent became effectively a condition of accessing services at all, and where the services in question were basic and essential (*e.g.*, NHS healthcare, income maintenance benefits, perhaps certain types of commercial credit) the meaning of consent would be eroded.

Thirdly, ECIF envisages data sharing from the central register, not so much on a case-by-case basis at the point of presentation of a card by an individual, but

- on an automated basis: For example, a person might provide updating information on a change of address to the central register, and the central register would then provide that updated address to other public service databases, in order to reduce duplication in demands for this information.
- on an individual basis: In the course of investigating persons under suspicion of being illegal immigrants, or working illegally, or not being entitled to services that they have claimed, fraud investigators or law enforcement officers would secure access to the records on the central register of the individuals under suspicion. This would typically involve data matching.
- on a routine basis: ECIF speaks of the routine links between the two constituent databases of the central register – namely, the DVLA and the Passport Agency – as being "gateways". However, these are not the only gateways. Databases for other services would have gateways that are described as being subject to "rigorous access protocols" (5.32), but these protocols are not defined in the paper. Annex 4, paragraph 22, speaks of gateways to databases run by private sector services, mainly in the context of the central register obtaining data from credit reference agencies, and says that these would be operated in compliance with data protection law. However, it neither specifically rules out nor clearly defines and limits any disclosures from the central database on a routine basis through these gateways. Presumably what is meant by a gateway here is the same as is meant by the term in the Performance and Innovation Unit (PIU) report (2002, paragraph 3.50) – namely, both legal powers to construct links and those links themselves between databases, enabling data sharing between agencies, where the legal powers typically specify the uses and purposes for that sharing and in some cases specify the types of information that may be shared. Chapter 11 of the PIU report set out recommendations for a number of new gateways. Several of those involve the DVLA and the Passport Agency sharing information on a routine basis with other agencies including the Criminal Records Bureau, several criminal justice agencies, the Motor Insurance database, and perhaps the civil registration system.
- on a bulk basis: in the course of specific exercises to identify potential fraudsters or criminals, a number of records, or fields from a number of records might be transferred from the central register to databases run by particular service-providing or investigation agencies; and
- by substitution: ECIF envisages that the central register itself might substitute for other registers, such as the electoral registers.

Finally, Annex 5, paragraph 12, gives a brief list of links with other databases across which the flows of data expected are principally from the third parties into the EnC central register for checks at the point of application, rather than disclosures from it. However, the paragraph does not rule out disclosures to these databases. They include:

- the Passport Service;
- the FCO passport database;
- DVLA and DVLNI registers;
- the online civil registration system if implemented by the time the EnC is introduced;
- the National Insurance central index;
- the Immigration and Nationality Directorate database; and

- databases held by one or more credit reference agencies.

In addition, there are already powers in law that would provide for disclosures, for example, in the course of investigations for fraud in relation to benefits, taxes and fees and charges, and general criminal investigations.

The information that can be gleaned from ECIF, even when read together with the proposals in Chapter 11 of the PIU report, does not suffice to enable one to be clear that the disclosures from the central register would in fact comply with the restrictions on lawful disclosures in data protection law.

The statement of the purposes is not sufficiently specified to enable any determination of what the legitimate expectations of confidentiality are. Secondly, it is not clear just which pieces of information that might be stored in the card but not on the central register – apart from emergency health-related information – would be subject to specific duties of confidentiality.

Most important, however, is that in order to meet the necessity tests in the conditions for processing, it would be critical to spell out just which pieces of information that will be held on the central register would be the subject of which types of disclosures to which agencies under which gateways and for which purposes. This would require a detailed tabulation of services, gateways and fields that could be shared with and without consent and under which circumstances. ECIF provides no such set of tables.

Investigating fraud and crime is clearly a legitimate interest of governmental data controllers and third parties providing public services. It may be that almost any of the fields listed in ECIF as intended to be included in records on the central register might be relevant in a fraud or a criminal investigation.

However, matters are much more complicated where the benefit at issue is either the reduction of duplication in demands for information such as change of address information, or any of the efficiency improvements or improvements in the effectiveness of co-ordinated service provision that lie behind the PIU report's proposed additional gateways. For in these cases, the imperative for data matching and sharing is of a rather different order of "legitimate interest". Therefore, not every field may be necessary for every type or occasion of matching or sharing, and in some of these cases, as the PIU report itself notes, the Information Commissioner has already held that the consent of the data subject would be required before sharing could proceed lawfully. The Information Commissioner's legal guidance on the "legitimate interests" clause in the processing conditions states that those interests must be weighed together with the legitimate interests of the data subject (Information Commissioner, 2001, 3.1.1). In the case of convenience, efficiency and effectiveness justifications for sharing being claimed as legitimate interests of the data controller and third parties, the relevant interests of the data subject would include those in privacy, which might well militate against unrestricted sharing or at least would call for individual consent, and that could not be overridden so readily as in the case of the imperative for law enforcement.

Perhaps, although the Commissioner's guidance does not put it in these terms, there might be implicit in this argument, a conception that the benefits to be obtained from the legitimate interest in data processing must not be *disproportionately* small when weighed against the relevant interests of the data subjects and the risks that the processing might run of violating the data protection principles from the intended disclosures. The crucial question to be addressed is by what standard proportionality is measured. If the benefits are measured as a proportion of the total expenditure on the service by the data controller, a very different answer would be obtained than if they are measured for the individual data subject. The logic of the Commissioner's guidance and of the law would lead us to think that the latter is the more relevant standard.

Security

The seventh principle provides that data must be secure against accidental loss, destruction damage, disclosure, and unauthorised processing. I am not competent to comment upon technical aspects of security in smart card systems, card reader devices, or in online databases of the kinds proposed in ECIF. However, in a paper of this nature, it is appropriate to pass some comment on the range of security issues that are raised by the argument as a whole.

The justification for the EnC at all rests heavily on the ability of the system to achieve very high levels of security, and to sustain them over time. For if the purpose of the scheme is one of securing for citizens a means of identification for the demonstration of entitlement, then the cards must be secure against counterfeiting both of the kind that creates an identity for an otherwise fictitious person and of the kind that steals the identity of a real person, either currently living or recently deceased. ECIF admits that the EnC will be the target of counterfeiters. There have been cases in recent history in which criminals have successfully counterfeited smart cards. Satellite digital and cable television companies have particularly suffered from this. Because those cards had a single use, the incentive for criminals to counterfeit them might well have been *less* than the incentive to counterfeit an EnC, because an EnC could in principle, provide access to a great many services at once.

The most important element of the security of the data held in the card is probably the strength of the encryption used. There is, however, a trade-off between increasing security by increasing the key-bit length and improving convenience of use, for longer key bit strings take longer to conduct processing at the point of use.

The central register must also be secure against attack. There seems little doubt that there will be incentives for many organisations, both legitimate and criminal in the

nature of their main business activity, to want to gain access to a register of details on all adults in the United Kingdom, and so to be tempted to use hacking methods to gain access to it. The central register will hold records employment status and a digitised photograph; it may hold a PIN and a digitised image of a hand signature and even an individual's electronic signature. Even more valuably, the card or the register may be linked with other databases, which in turn may hold medical information, financial information and a wealth of other service use and transaction data. While hacking may not be the most important risk, there are plenty of ways in which errors in the management of the database can result in inadvertent disclosures. In recent scandals, a utility company, a joint commercial loyalty point scheme based on a smart card, and the Inland Revenue have all experienced problems that resulted in people being able to access personal information about other people over a website, as a result of incompetent management rather than external attack.

Security, within the meaning attached to it in the Data Protection Act, is not only a technical matter to do with firewalls, encryption, passwords, PIN numbers, levels of authorisation and so on. The Commissioner's legal guidance makes it clear that organisational and management issues are a key component in ensuring that human failures, incompetence and corruption are minimised. In particular, the guidance notes that "sufficient resources and facilities" must be in place to ensure that the duty is fulfilled. Apart from the office management routines identified in the guidance, this will involve ongoing programmes of staff training. Given the scale of the proposed EnC scheme, encompassing as it would a huge range of public services, this would be a costly endeavour. Unfortunately, the ECIF cost estimates do not seem to include budgets for this: the staff costs identified relate only to those for the central registers at DVLA and the Passport Agency, and not to the costs of training for public servants who will access the data systems.

Security is also a crucial issue in the technical basis by which rules are policed against disclosure at the point of use of the card. For when citizens present their cards at the point at which they apply for a public service, they will want to be assured that the public service – or, perhaps of greater concern, the commercial body contracted to provide that service – is accessing only those fields upon their record on the central database or in the card (*i.e.*, neither in fields nor even in directories other than the ones they are authorised to access), or only those data held in other public services accessible through secondary gateways from the central register, that (a) they are authorised to do and (b) that the citizen has been informed that they are accessing, and that any audit trail or retained data meet the same criteria. They will also expect that no data will be captured from the central register and retained by the service provider, other than those about which they have consented or at least been informed, and which the service provider is permitted to store, within the purposes of the scheme.

Security is a technological arms race. The speed with which improvements in the capability to decrypt or to work around blockages and firewalls become available is such that no smart card can remain in circulation for very long without becoming insecure. In the case of systems that use encryption of today's typical key bit lengths, it is quite possible that they would become insecure before such time as they would begin to wear out through use in any case. In the same way, it would be necessary to upgrade the security systems of the central register on a constant basis.

To ensure all this requires significant and sustained investment. ECIF does not detail just what the full estimates would be, mainly focusing instead on the costs of biometric infrastructure, which are at most, part of the card level security.

Conclusion

There are, then, a wide range of concerns from a data protection standpoint about the scheme proposed by the Home Secretary, quite apart from the wider social considerations about the possibilities for the declining availability of anonymity in transactions with organisations, and about the true costs of the scheme which, it has been argued (see *e.g.*, 6, 2003) are likely to be greater by an order of magnitude than the Home Office has estimated.

If the Home Secretary does decide to proceed with a scheme, and can secure the funds required for it from the Chancellor, then at the very least, a much more specific set of purposes should be set for it; detailed codes of practice should be developed governing how, why and when public officials might demand a card and process information using it; a system of regular audit should be put in place to identify misuses; only disclosures of defined list should be permitted. Without these minimum measures, it would be very difficult for the government to claim that the present scheme to be in full compliance with both the letter and the spirit of the data protection principles. It is against these very modest standards that, in the first instance and even before considering all the wider issues of the social impact and the costs and the likely real impact upon identity fraud, we should judge any revised proposals that the Home Secretary presents later in 2003.

References

6 P, 2003, "Entitlement cards: benefits, privacy and data protection risks, costs and wider social implications", Office of the Information Commissioner, Wilmslow, published at *www.dataprotection.gov.uk/dpr/dpdoc1.nsf/24afa328dcbf83d8802568980043e730/2924d87f53cb414180256cc5003fcd96/$FILE/perri6_annexb_ecards_paper_ic_rvsd_final_ver.doc.*

Audit Commission, 2002, "Data remember: improving the quality of patient-based information in the NHS", Audit Commission, London.

British Computer Society, 2003, "Response from the British Computer Society to the government consulta-

tion paper on entitlement cards and identity fraud", British Computer Society, Swindon.

Home Office, 2002, "Entitlement cards and identity fraud: frequently asked questions", Home Office, London, available at *www.homeoffice.gov.uk/ccpd/faqid.htm*.

Information Commissioner, 2001, "Data Protection Act 1998: legal guidance", Information Commissioner, Wilmslow, available at *www.dataprotection.gov.uk/dpr/dpdoc.nsf*.

National Audit Office, 2002, "Report by the Comptroller and Auditor General - Class III Vote 8 - Driver and Vehicle Licensing Agency", HC 335-III Session 2001-02, National Audit Office, London.

NHS Information Authority, 2002, "Caring for information: model for the future", NHS Executive, London and Leeds.

Performance and Innovation Unit, 2002, "Privacy and data sharing", Performance and Innovation (now the Strategy Unit), Cabinet Office, London, available at *www.strategy.gov.uk/2002/privacy/report/index.htm*.

Secretary of State for the Home Department, 2002, "Entitlement cards and identity fraud: a consultation paper", Cm 5557, The Stationery Office, London.

U.K. Consultation Proposals on Communications Data Retention and Access

By Sally Annereau, a Data Protection Analyst in Taylor Wessing's Privacy and Data Protection Group. The author may be contacted at s.annereau@taylorwessing.com

On March 11, 2003 the Home Office published two long awaited consultation documents. The first consulting on a draft voluntary code of practice on the collection and retention of communications data and the second consulting on proposals for greater access to communications data by law enforcement authorities.

The origins of both proposals go back to the September 11 terrorist attack on the twin towers when in common with other governments around the world, the U.K. Government rushed through new anti-terrorist legislation, the Anti-Terrorism, Crime and Security Act 2001 to give law enforcement agencies in the United Kingdom additional powers to combat the perceived increased terrorist threat.

The speed with which the legislation passed through Parliament, meant that there was no time to put in place a regime within the legislation under which communications data could be stored for consistent periods of time and in a way that would not conflict with other legal requirements, in particular the Data Protection Act 1998. Sections 102 and 103 of the Anti-Terrorism, Crime and Security Act 2001 therefore dealt with this issue by giving the Home Secretary the power to introduce a voluntary code of practice to cover this area at a later date.

In a separate initiative the Government has also sought to extend the current number of authorities able to obtain access to communications data through another, earlier piece of legislation, the Regulation of Investigatory Powers Act 2000. An earlier attempt to expand the categories of authority entitled to have access to communications data under this legislation were hastily withdrawn by the Home Office for review, following a public outcry over the scope of the proposals.

For the purposes of both consultation documents communications data consists of:

Traffic data: Information relating to the sender or recipient of a communication. This may be the telephone number of the sender or recipient in the case of a phone call or an Internet e-mail address.

Service data: Information about what telecommunications services are used, and when.

Subscriber data: Information about the user of the service that is held by the service provider such as the name and address details of a subscriber held by Internet Service Providers (ISPs) or by telecommunications service providers.

It is important to note that the definition of communications data here does not include the content of any communication.

The key issues arising from each of the consultations is summarised below:

Retention Consultation Proposals

The draft code published with the consultation document includes proposals as to how the processing and retention of personal data under the draft code can be conducted in a manner that will also be lawful under the Data Protection Act 1998. In particular, the draft code proposes that:

- Data no longer required for business purposes but retained under the code will be retained specifically for national security purposes only and no other.
- Communications providers will need to ensure that their entry in the register of data controllers maintained by the Information Commissioner is updated to describe the processing of personal data for national security purposes.
- Subscribers should be notified of the new purpose for which data is being retained by sending out a general notice to all customers and by making the national security purpose for retaining personal data clear to any new subscribers at the time they subscribe.

The draft code further proposes the following specification for the different types of communications data retained for national security purposes.

Type of Data	Description	Retention period
Subscriber information	Subscriber details Contact information Services subscribed to	12 months
Telephony data	All numbers associated with each call Date of call Time of start/end of call Duration of call Location data at start/end of call	12 months
SMS, EMS, and MMS data	Calling number Called number Date and time of sending Delivery receipt (if available) Location data where message sent Location data where message received	6 months
E-mail data	Log on (user name, date/time log on and log off, IP address logged on from) Sent e-mail (user name, to/from/cc e-mail address, date/time sent) Received e-mail (user name, to/from e-mail addresses, date and time received)	6 months
ISP data	Log on (user name, date/time log on and off, IP address assigned) Dial up (caller line ID and number dialled)	6 months
Web activity	Proxy server logs (date/time, IP address used, URLs visited services)	4 days

Provided the data is not required for other lawful purposes, the data must then be either anonymised or erased when the retention period has expired.

The draft code further proposes that where the data retention periods specified are significantly longer for national security purposes than for the service providers own business purposes, the Secretary of State will contribute a reasonable proportion of the marginal cost involved, (such as the design and production of data storage and searching facilities).

Access Consultation Proposals

The separate access proposals identify those bodies to which access to communications data should be extended. The consultation document addresses the scale of this access and also deals with the supervision of these arrangements. Broadly speaking the bodies proposed access to communications data fall into three separate categories:

1. A number of specific police bodies that were left out from the original access arrangements provided under the Regulation of Investigatory Powers Act 2000.

2. The emergency services (fire and ambulance).

3. Other agencies or public bodies that are responsible for investigating and sometimes prosecuting certain specific types of offence. For example trading standards offences investigated by local authorities.

The full list of bodies proposed access under the consultation is:

	Identity of Body
1	Scottish Drug Enforcement Agency U.K. Atomic Energy Authority Constabulary
2	Fire Authorities Ambulance Authorities Coastguard
3	Financial Services Authority Office of Fair Trading Department of Trade and Industry Radio Communications Agency Serious Fraud Office Home Office (Immigration Service) Health and Safety Executive Environment Agency Department of Environment, Food and Rural Affairs Department of Health (Medicines Control Agency, Medical Devices Agency and anti-fraud agencies) Department of Work and Pensions Information Commissioner Royal Mail Postcomm Gaming Board Charity Commission

Access to communications data is already limited under the Regulation of Investigatory Powers Act 2000 to certain specified purposes. The latest proposals go further to include "restricted access and double lock" options whereby there would be a restriction on the purposes for which a given authority could have access to communications data and further restrictions on the type of data to which that access would be allowed. Finally there would be an additional level of oversight in relation to access by some authorities. This would require, for example, an authority to obtain the prior approval by an independent third party such as the Office of the Interception of Communications Commissioner, before being able to obtain access to communications data.

Overall, both sets of consultation documents indicate that the Home Office have taken on board a number of the public and industry concerns about earlier proposals on retention and access to communications data however there remain a number unresolved issues including:

- The list of public bodies proposed access to communications data remains extensive.
- The supervision arrangements for certain government agencies are limited to the agency itself or to supervision by another government agency rather than the courts.
- There are likely to remain practical difficulties with implementing the retention and access rules in practice.
- The limited prospect of government financial assistance to service providers in putting place the necessary collection and storage facilities.
- The lack of recognition for the cost of hiring staff to fulfil what for some may be a full time job of supervising the collection, storage, access and deletion of the data.

Both papers are now open to consultation until June 3, 2003.

The Government's consultation on Access to Communications Data under RIPA can be found at: *www.homeoffice.gov.uk/ripa/part1/consult.htm*

The Government's consultation on the Voluntary Code of Practice for Data Retention can be found at: *www.homeoffice.gov.uk/oicd/antiterrorism/consult.htm*

Developing E-mail and Internet Policies for Employers in the United Kingdom

By William Downing, partner, and Cara De La Mare, Barrister, Trowers & Hamlins, London. The authors may be contacted by e-mail at yperlinkwdowning@trowers.comHyperlink; or cdelamare@trowers.com

The specific legislation which governs all U.K. employers' rights on the use of e-mail and the Internet by their employees includes:

- the Data Protection Act 1998 (DPA)and the Employment Practices Data Protection Code of Practice;
- the Regulation of Investigatory Powers Act 2000 (RIPA); and
- the Human Rights Act 1998.

This article analyses the key legal obligations on employers who provide e-mail and Internet access to their employees, and details how employers can effectively manage their employees' use of online facilities through the implementation of properly drafted e-mail and Internet policies.

Vicarious Liability

Vicarious liability describes the principle of law by which an employer can be held liable for the acts of its employees committed in the course of their employment, including their use of e-mail and the Internet.

The essential pre-condition of vicarious liability is that the act complained of should have been done in the course of employment. This concept has been widely construed and can include acts which employees are instructed or authorised to perform, unless it can be said that they are on "*a frolic of their own*". Where there is sufficient connection between the act committed by the employee and employer, the employer may be liable for it. It is therefore, sensible to regulate employees' conduct in using the Internet and e-mail.

Regulation of Investigatory Power Act

The Regulation of Investigatory Powers Act 2000 came into force on October 24, 2000. The Department of Trade and Industry has also issued the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 ("the Regulations") under the Act.

The key provisions of RIPA which apply to employers include the provisions by which it will be an offence for a person (including an employer),

> "intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of a private telecommunications system".

It is beyond doubt that the definition of "private telecommunications system" includes an employer's use of external e-mail and the Internet.

However, the Act provides that interception by an employer can be lawful where it occurs with consent which means: the employer has the consent of the sender and the recipient to interception; or the employer has reasonable grounds for believing that both the sender and the recipient consent to the interception. Thus, an employer can lawfully intercept communications without consent where the interception is:

- to establish the existence of facts relevant to the business, (*e.g.*, keeping records of transactions and communications);
- to ascertain compliance with regulatory or self-regulatory rules or guidance (*e.g.*, financial services call monitoring);
- to ascertain or demonstrate standards which are or ought to be achieved by persons using the system in the course of their duties (*e.g.*, training on the system);
- to prevent or detect crime (*e.g.*, to prevent fraud or corruption or to detect use of unsuitable material);
- to investigate or detect unauthorised use of telecommunications systems. This can cover both internal use (*e.g.*, monitoring to ensure that there is no breach by employees of the employer's procedures), or external use (*e.g.*, to check for viruses or inflammatory content); and
- to ensure the effective operation of the system.

All monitoring must be necessary and relevant to the business; this is quite wide, but employers should act with circumspection. Also, employers must make every reasonable effort to inform those involved that interception may take place. The sensible place to do this is in an employment policy.

Data Protection Act 1998

In addition to the obligations placed on employers under RIPA 2000, the DPA imposes obligations on employers in relation to the processing of personal data and sensitive personal data held on their employees. Under the DPA, "Personal data" is defined as any data which relates to a living individual who can be identified from the data or from the data together with other information which is in the possession, or is likely to come into the possession, of the data controller (*i.e.*, the employer). As such, personal data includes any expression of opinion about the individual and any indication of the intentions of the employer or any other person in respect of the individual.

The DPA defines "Sensitive Personal Data" as personal data consisting of information as to the racial or ethnic origin of the data subject, political opinions, religious beliefs, other beliefs of a nature similar to religious beliefs, trade union membership, medical records, sexual life, as well as commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed. Moreover, "data" is

used to mean any information held on computer or in a paper-based filing system.

The DPA places limits on how employers process data on their employees by requiring that "consent" (as opposed to explicit consent) be required for processing personal data unless the employer can meet one of the exceptions set out in Schedule 2 of the DPA. Also, where an employer wishes to process sensitive personal data, it must have the "explicit consent" of the person to whom the sensitive personal data relates, or the organisation must rely on one of the other limited grounds set out in Schedule 3 to the DPA.

Data subjects, including employees, also have the right to have all data held by a Data Controller (*e.g.*, an employer) processed in accordance with the data protections principles. The standards which must be met if the requirements of the DPA are to be complied with are broadly that the data must be:

- fairly and lawfully processed;
- processed for limited purposes and not in any manner incompatible with those purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept for longer than is necessary;
- processed in accordance with the individual's rights;
- secure; and
- not be transferred to countries without adequate protection.

This will have an impact on any data that are held for monitoring purposes. Data subjects have various rights under the DPA, including the right to have access to the data held on them, and a right to information about the processes used.

The Employment Practices Data Protection Code

The Office of the Information Commissioner has the power to issue enforcement notices where it considers that there has been a breach of one or more of the Data Protection principles. One of the duties of the Information Commissioner is to prepare and disseminate Codes of Practice for good guidance detailing good practice (Section 51(3) of the DPA). Thus, in performance of this duty, in March 2002, the Information Commissioner issued the first part of a four-part Code of Practice entitled the Employment Practices Data Protection Code. Part 1 relates to recruitment and selection. Part 2 covers employment records including the collection, storage, disclosure and deletion of records. The final two parts on monitoring at work (such as monitoring workers' use of telephone or e-mail systems and vehicles) and medical information (including occupational health, medical testing, drug testing and genetic screening) will follow when completed. The Code will not be formally published as one Code until all four booklets have been completed, but the various parts will appear on the Information Commissioner's website as they are released.

Part 3 of the Data Protection Code deals with monitoring at work. It has only been issued in draft form so far, but it is expected that it will be finalised in the coming months. Part 3 expressly recognises that monitoring (including e-mail, Internet and telephone usage) should be designed to operate in such a way that it does not intrude unnecessarily on the right of workers to respect for their private lives and correspondence. Thus, although employers might have good reasons for workplace monitoring, in all cases this is to be balanced against the impact on employee privacy. The Code recommends that an employer undertake an impact assessment in order to determine whether the impact of monitoring on workers is justified by the likely benefits, which requires consideration of the possibility of less intrusive methods or more closely targeted monitoring. In short, monitoring should only take place if it is a proportionate response to the employer's problem. The basics of the Code can be summarised as follows:

- covert monitoring of employees' e-mail should be avoided except in exceptional cases;
- an e-mail monitoring system must not entail routinely reading an individual's e-mail account; and
- the Information Commissioner is in favour of setting up private e-mail accounts for employees, thereby making it clear to employers which e-mail accounts are private and which are not.

Access Requests

One area that causes employers difficulty is access to e-mail. Workers are entitled, and may request copies of e-mails about them, however, employers are not required to search through all e-mail records merely on the chance that somewhere there might be a message that relates to the worker. For information to fall within the DPA subject access provisions, the worker must be the subject of the information. This means, for example, that an e-mail which merely mentions a worker, perhaps because his or her name appears on the e-mail address list, need not be provided.

Information released to a worker could include information that identifies another person, for example a fellow worker. This other person is referred to as a third party. Responding fully to a subject access request could lead to the third party's rights under the DPA being violated. One example is where a complaint is received about a worker and releasing information on the complaint, in its entirety, will identify the complainant to the worker. In many cases, simply removing the third party's name from the information before it is released to the worker will solve the problem. However this will not always be the case as sometimes the worker might be able to work out the third party's identity from the information itself, for example "*only x could possibly have written that about me*". In such circumstances, the employer has to strike a balance between the right of the worker to access and the right of the third party to privacy. Before releasing information to the worker the employer

should follow a clear decision-making process to ensure it gets the right balance.

In addition, workers have a right, under the DPA, to know the logic behind any automated decision. If a separate request can be made, or if specifically stated, the request can be included in a general subject access request.

Privacy

Privacy has become an important issue in cases before the U.K. courts as a result of the Human Rights Act 1998 (HRA), which came into force in the United Kingdom on October 2, 2000. Although the HRA makes it unlawful for a "*public authority*" to act in a way which is incompatible with the Convention, it is only of relevance to all employers because any employer whose functions include public functions will be caught, and any court or tribunal (public authorities), is obliged to interpret the law in the light of the rights.

The case of *Halford v. United Kingdom* [1997] IRLR 471 is an important decision on the right to respect for private and family life, and was a case arising from a complaint by Alison Halford against the Merseyside police. During the course of her complaint it became apparent that the police had been intercepting her calls on the office telephones. The European Court of Human Rights held that the interception by her employers of calls made on her office telephone was a violation of Article 8 of the European Convention on Human Rights.

Following the case the Home Office issued a circular entitled "*Interception of Non-public Telecommunications Networks*" which was addressed to all Government departments and Chief Police Officers (HOC 15/1999 issued March 23, 1999). The Oftel circular detailed the requirements for complying with the Halford judgment and those were summarised as follows:

- *Expectation of privacy*: If the person making the communication is fully aware that monitoring or tape recording of communications may take place then an expectation of privacy can, in principle, no longer exist. However, warnings to this effect may not, on their own, be sufficient to dispel the legitimate expectation of privacy. It is not reasonable to expect that employees will never be contacted on a domestic matter in work time, or that the employee will never have reason to make personal calls from the office.
- *Adequate warning that interception may take place*: Where written consent can be obtained this is clearly the best way, but in the absence of that, an employer could possibly seek to rely on implied consent. The onus is on the operator of the network to ensure that the message is advertised clearly enough to ensure that no user is left in any doubt that interception may take place. This can be achieved by including a clause in the terms and conditions of employment and through publicity within the office. It will also be good practice for operators to make every reasonable effort to inform all potential users that not only speech, but also any other form of communication passing over the network may be monitored or recorded.
- *Monitoring*: It is important that monitoring is used only where necessary, that the level of intrusion is proportional to the offence to be investigated, and that monitoring is the appropriate method of investigation. For instance, if an employer suspects an employee has been misusing the office telephone to make a large number of personal calls, evidence of this activity can be gathered simply by obtaining an itemised billing print.

This guidance, although directed at telephone monitoring, is also relevant to other forms of monitoring, including e-mail and Internet monitoring.

E-mail/Internet Use – Drafting an E-mail Policy

An e-mail/Internet use policy should outline:

- the issues involved in the use of e-mail and the Internet. The employee should be made aware that use of the e-mail system (or misuse/abuse of the e-mail system) can give rise to such matters as race and sex discrimination, defamation, criminal prosecution and internal disciplinary offences;
- what is not appropriate use. This includes detailing what employees must do and what employees must not do. The "*musts*" will include attaching disclaimers, obtaining authority where necessary and retaining a paper trail during contract negotiations *etc.* The "*must nots*" will include discriminating (harassing) criminal activities (including fraud) and breaches of confidentiality;
- the issues in relation to the Internet are essentially the same also, the accessing of obscene material and any material which may give rise to offence should explicitly be forbidden;
- state which systems will be monitored. This will make it difficult for an employee to argue that his/her correspondence is private. Furthermore, it will assist in arguing that the individual has given his/her consent to the monitoring; and
- state that a failure to adhere to the policy could amount to a disciplinary offence.

It is sensible for all employees to have training on e-mail policies.

Policing the Policy

Once the employer has drafted and implemented a policy or updated its current policy, it needs to bear in mind the parameters in which it can be enforced. There will be some constraints on an employer's freedom to monitor e-mails, in particular as set out in RIPA 2000 and the Human Rights Act 1998 which have been précis'd above. The employer must:

- notify all employees where monitoring and surveillance takes place;

- include a sentence in the disclaimers attached to all external e-mails that monitoring and surveillance of incoming information is carried out;
- make a regular periodic review of the technical screening measures in operation to ensure that they comply with the legislation (and keep records of those reviews);
- when information is intercepted given preliminary consideration to whether there is a "power argument" for its interception and for any further action (note that the draft Regulations may be altered in this regard);
- obtain employee's consent to processing data for the purposes of the DPA including a clause in the new employee's contract of employment;
- have all new starters trained at their induction and sign a document confirming their training, publishing of information on the notice boards; and
- consider the Data Protection principles in deciding whether to store intercepted information if building a case.

Disciplining

Employers are reminded of the requirement to carry out as much investigation as is possible in all the circumstances prior to taking any disciplinary action against an employee. The following tips are worthy of note:

- remember the requirement to carry out as much investigation as possible;
- at the same time remember the requirement for privacy and consider at an early stage whether it is necessary to reveal the details of the messages themselves (or whether it is necessary to reveal all of them as opposed to a few);
- consider the severity of the offence which is alleged and the appropriate action;
- include examples within the disciplinary procedure about use of the e-mail system and the Internet; and
- follow the organisation's own procedures.

GENERAL

Under the Gaze, Privacy Identity and New Technology (Part I)

This is the first of two parts of a paper by Malcom Crompton, Australian Federal Privacy Commissioner, presented at the Privacy Issues Forum in Wellington, New Zealand. The Forum was hosted in March 2003 by the New Zealand Office of the Privacy Commissioner.

Introduction

Privacy is an important human right, which has been recognised in statute law and common law in most Western nations. Developments in information and communications technology have posed considerable challenges for the protection of privacy in recent years. This paper will consider some of the challenges posed to personal privacy in the context of technological change, with a focus on questions of identity.

New technologies have vastly increased the capacity to collect, store, transmit and manipulate information. The increasing interconnections between information networks allow personal information to be collected, matched, traded, and profiled by both public and private institutions. The rapid pace of digitisation of information increases the access, transmission and retrieval speed and allows for comprehensive personal information files.[1] There has also been a significant increase in surveillance and tracking devices.

The increase in the ease of movement and levels of connection of information clearly creates benefits in greater efficiencies in business and government. It can also pose risks to privacy. Threats to privacy arise through the ways all this information about each person's activities, transactions and communications is used. The capacity to link and match different data trails left by electronic transactions for example, can bring together a comprehensive digital picture of one's activities, purchases, preferences, habits, likes and dislikes. Compilations of personal information can result in rich data portraits capable of revealing character, identity and lifestyle.

Technologies have the potential to be more privacy invasive where they involve the identifying organisation holding large amounts of information about individuals that they may or may not need, or that individuals may or may not know about. Aggregation of personal information almost always means shifting information to a different context. Some of the greatest risks to privacy can occur when personal information is taken out of context.

Effective privacy protection will require the interaction of law, technology and market pressures.[2] Privacy laws alone may not be sufficient to ensure adequate privacy protection. Technical capacities of new technologies can either constrain or enable the protection of personal information. Privacy laws can be a powerful tool for establishing public policy objectives, providing incentives for technological developments and to influence market behaviour.

To illustrate the interactions between the law, technology and the market place, the paper will explore the relevance of identity to privacy and then consider the impact of new technologies, and the market, on identification and the role of law in finding the right balance between privacy and other considerations such as law enforcement, efficiency of government and business transactions and the development of new services.

The Value of Privacy

Privacy is an important component of human dignity, it is related to respect and freedom from interference or intrusion. There have been numerous and varying attempts to define privacy. Some definitions focus on the relationship between privacy and autonomy and the right of individuals to determine for themselves how, and to what extent information about them is communicated to others. Other definitions focus on the inviolability of the person where an invasion of privacy constitutes an offence against individuality, dignity and freedom.[3]

Perhaps the most simple and meaningful definitions of privacy come from a key early modern writing, which describes privacy as "the right to be let alone".[4] Let alone to contemplate, to question, to grow, to develop, perhaps to make mistakes, to try out new ways of being or to experience intimacy.

Some privacy sceptics have argued that only those with something to hide need privacy. This view assumes that it is possible to live a wholly transparent life where nothing about a person is inaccessible to others. However, every person needs some space away from the scrutiny of others. Just contemplate the all-seeing world described by Brin[5] with ubiquitous cameras on every vantage point, accessible to every citizen. For growth and development an individual needs some solitude and anonymity. Thoughtful action requires time to think, reflective behaviour relies on time to reflect. Each individual needs a balance between solitude and companionship, between anonymity and responsible participation in society. A free society allows the individual to choose that balance.[6]

In a free society, we need to be free to make our own decisions according to our own belief systems. We need to build a society where good decisions are motivated by the common good, rather than motivated by compulsion and oppression. The second path leads inevitably to totalitarianism. Privacy gives each individual the space

to make their own decisions according to their own conscience. If we build and nurture our society well, these decisions will, in the main, be for the common good. Without privacy, every decision is observed, and in a sense forced by the public gaze, not the moral code of the individual. This is not a good foundation for a society.

Privacy is not an absolute right. Rather it must be balanced against other competing human rights and social interests. A measure of accountability is necessary in a free society, under the rule of law. An individual's right to privacy is tempered by other competing needs for individuals to be accountable.

There may be conflicting interests for example, between privacy and:

- maintaining order, the stability and security of the nation state;
- social ends such as the efficiency of business, compliance with taxation law, freedom of speech;
- personal ends, such as advancement of the individual, which may require relinquishing some privacy.

Individual privacy is not a new or exclusively Western notion. All human societies have allowed for some areas of human life to remain private. Privacy has taken different forms in different societies. Similarly, the balance between privacy and other social interests has been found in different ways. In some societies there was little or no anonymity. In a tribe, or even in a village, the individual is identifiable to most people they encounter.

This lack of anonymity in such societies is balanced to some extent by experience of greater trust, permission and control that the individual experiences in that environment. The mutuality, interdependence and shared background associated with a small community promotes trust. Individuals may well have more influence over their world (unless, for example, they lived in slavery). They certainly have more awareness of the extent to which they are under the gaze of others that in turn enables them to take appropriate protective steps. The social conventions of small communities also provide for some degree of privacy.

In contrast, privacy takes very different forms in the large anonymous cities of the nation state. In this environment, an important distinction emerges between the public and private sphere of life. The family or household domain became the place for "private life" where the individual is known and is intimate with others. In this sphere, the individual can be expected to experience greater trust, permission and control. In the public sphere many transactions were conducted with relative anonymity. One of the freedoms of the big city was the capacity to move about in passing crowds with relative anonymity. This escape from the sense of being under the gaze allows individuals the opportunity to explore different ways of being and enables greater diversity.

The extent to which an individual can be identified or anonymous is an important factor for the individual's privacy.

Privacy: Identity, Anonymity and the Places In-Between

Identity and anonymity are not binary opposites, but rather different ends of the same spectrum and there are many shades of grey between them.

An important distinction needs to be made between identity and identification. Identity is a complex, multi-faceted notion. Each of us has a range of different identities defined through relations with others, position, status, actions, behaviours, characteristics, attitudes and the circumstances of the moment.

A person may be a corporate lawyer, a steam train enthusiast, a doting father, a lapsed Catholic, a proud migrant, an estranged son, a polio survivor, a music lover and so on. Each of those identities is valid in its own context, but personal information relevant to one identity may be inappropriate or embarrassing when taken out of context. One of the values of privacy is the "ability to maintain different sorts of social relationships with different people".[7]

In addition to these relational dimensions of identity, there is also the question of self-identity. An individual's perceptions of himself or herself include personality, degree of happiness, fears and aspirations. People need an environment of trust to reveal themselves to others. An important aspect of privacy is allowing individuals to have some control over when and to what extent they identify themselves.

Identification is the action of being identified, of linking specific information with a particular person. An individual's identity has a degree of fluidity and is likely to change over time. The extensive linking of different information about an individual may restrict or limit this fluidity. To allow for growth and development, individuals need to be able to let life flow by. Few of us would want to be defined forever by all the attitudes we may have held at the age of 17.

Identification can potentially relate a wide range of elements of an individual's identity. In practice, identifying an individual generally involves focusing on those things that distinguish that individual from others including, legal name, date of birth, location or address and symbolic identifiers such as a drivers license number. The basis for identifying a person can also involve such characteristics as:

- the person demonstrating that they have knowledge of something (*e.g.*, a password); or they possess a token (*e.g.*, drivers license);
- a person's physical appearance, actions or characteristics (*e.g.*, facial features, signature, fingerprint); or
- social characterisation (*e.g.*, gender, ethnicity, education, employment and leisure activities).

One of the impacts of new technologies is the emergence of "identity creep" or the capacity for gradual identification of "non-identified" information through data mining or linkages of data.

Anonymity is not synonymous with privacy, but is one means by which individuals can attain a degree of privacy. On one view, privacy has three elements:

- what is known about the person;
- whether there is physical access to the person;
- whether attention is paid to the person.

The last of these is also relevant to anonymity. Anonymity can mean being unacknowledged as well as being unidentified.[8]

Complete privacy and complete anonymity are neither possible nor desirable in human society. However, a free society generally allows individuals to make appropriate choices about when, and to what extent they reveal themselves to others. Requiring individuals to be identifiable when it is not necessary can be a form of privacy intrusion. There are circumstances where it is necessary and appropriate to ensure that a person is who they say they are. However, there is also considerable confusion between when an individual needs to identify him or herself, and when he or she needs to authenticate something else about him or herself.

There is a significant distinction to be made between the process of identification and authentication.[9] Processing a transaction may involve a number of elements including authorisation, identification and authentication.

The terms "identification" "authentication" and "authorisation" are sometimes used in different ways depending on whether the transaction is being considered from the perspective of the individual or the organisation with which they are transacting. This paper uses the term "identification" to mean the process of accurately identifying a person, ensuring that a person is who they say they are. This generally involves checking documentation such as records of the bases of identification listed above.

In contrast to identification, "authentication" involves checking an assertion made by the person. Authentication could include an assertion relevant to identity, such as confirming that a person seeking to make the transaction is the same person who opened the account. However, authentication may also include other assertions such as, the fact that the individual holds a valid drivers license, or is offering a valid payment. Often the individual's identity is not at issue, but rather some other claim that the person makes.

For the organisation, we take authorisation to have two stages. The first is the initial allotment of privileges to the individual, for example the allocation of a user representation such as a bank account number. The second stage can also be called "access control" where the organisation's information system checks whether the user representation is authorised for each service provided. The structure of the transaction for the organisation generally involves: prior authorisation and then a process of authenticating the user representation, for example checking a PIN number against a particular automated teller card, and then access control or a specific authorisation for the particular transaction. Authentication may or may not require identification of the individual.

From the individual's perspective, authorisation is the act of authorising the transaction. This may or may not involve or require revelation of identity. Paying for goods with cash need not require any identification whereas the same purchase with a credit card can involve a very strong from of identification and linkage of data.

Distinguishing between identification, authentication, and authorisation involves getting clear about the real purpose for the information. New technologies have the capacity to enable the authorisation and authentication without revealing identity in transactions where it is not needed.

Identity and New Technologies

New technologies are not necessarily destructive of privacy. They can be privacy enhancing technologies or privacy intrusive technologies, depending on how they are designed and the uses to which they are put.

Technologies have the potential to be more privacy invasive where they involve organisations holding large amounts of information about individuals that they may not need, or that the individual may not know about. This can distort the balancing act between individual privacy and other social needs.

There are a number of technological developments relevant to questions of identity, including:

- biometrics;
- tracking and monitoring technologies;
- data mining;
- electronic transactions;
- encryption and digital signatures.

The capacity for technological developments to impact on identity may not necessarily be the initial or primary purpose in developing the technology. In some cases this capacity is simply an artefact of another process, albeit sometimes very powerful. A mobile phone, for example is also a persistent and accurate location tracking device.

Numerous biometric technologies are in development using; fingerprints, hand geometry, face recognition, voice recognition, iris and retinal scanning, keystroke recognition and DNA. These digitised measures of biological data create powerful authentication and identification tools. Biometrics designed to operate as one unique identifier to be used in whole range of different context can raise significant privacy risks. Alternatively, they can be designed to operate in a privacy protective manner.

Tracking and monitoring technologies cover a wide range of technologies from increasingly sensitive video and audio surveillance tools, through to recording the movement of mobile phones in real space and online interactions in virtual space. These have the potential to reduce the scope for anonymity as more individuals are increasingly under the gaze of others.

Data mining involves the use of generic algorithms to optimise searching and combine information on different databases and generate new information in the

process, including identification of de-identified information.

One of the impacts of new technologies has been a loss of anonymity in many transactions which are now conducted electronically. Many electronic transactions, as currently designed, leave digital trials and transactions that were once anonymous are now becoming increasingly identifiable as more information can be gathered, collated and linked to an individual. Despite this tendency, loss of anonymity is not inevitable. It is technologically possible to conduct anonymous or near anonymous electronic transactions and much work is going into developing these alternatives.

Cryptographic tools allow for more security in electronic transactions. Asymmetric encryption systems such as public key technology involve a pair of encryption keys, a public key and a privacy key. The subscriber must keep the private key secret. The public key can be made known to others and made publicly available.

Public Key Infrastructure is a system to enable the widespread and open use of public key certificates. It can be used to deliver a number of goals:

Authentication of the identity of a subscriber in online transactions can be achieved by the subscriber "signing" an electronic communication with their private key. This authentication is performed by the application of the public key to the digital signature.

The integrity of the message can be checked. Where a subscriber signs an electronic document a message digest or hash of the message is produced, this is essentially a number (hash value) derived from the text of the message, any other message will produce a different number. If the hash value remains the same after the message has been received then the message integrity is assured. That is, the message has not been altered in transit.

Non-repudiation can be achieved. Where an electronic message is signed with a digital signature, the fact that it was signed with a particular key cannot be repudiated or denied. In practice, this means that there will be irrefutable evidence of this, unless it can be shown that the private key was applied by other than its unique and rightful owner.

Confidentiality of messages can be assured. This is achieved by encrypting a message with a subscriber's public key. The message can only be decrypted with the subscriber's private key.

Three of these elements, authentication, integrity, and confidentiality are particularly pertinent to privacy protection.

Technologies relevant to identification could potentially be privacy enhancing technologies (PETs) or privacy intrusive technologies (PITs). Whether a technology is a PIT or a PET depends not only on how it operates, but also on how it is structured. One key factor is whether or not it involves the collection of unnecessary information, including a greater degree of identification content than required for the system to function.

An individual's identity is only really necessary for particular parts of an information system, the authorisation and accounting processes. One way to protect privacy is to introduce an "identity protector" and use encryption and digital pseudonyms to separate an individual's true identity from the details of one's transactions and communications. This would result in a significant reduction in the collection of identifiable information and therefore enhance the protection of privacy.[10]

Technologies that may often be PITs include systems that involve the use of a single identifier for each individual, which is linked to a single set of demographic and identifying information that is used in a wide range of situations. This was the basis of the infamous "Australia Card" proposal in the late 1980"s. More recently, in 2001 the Malaysian government began issuing a multi-application ID card. The card has an embedded microchip and is used as a national identity card, driver's license, passport and electronic purse. Plans for additional applications include using it to withdraw cash from automated teller machines and storing health and immigration information. The cards have been criticised by consumer associations concerned that they make individuals' personal and confidential information too vulnerable.[11] The extensive linking of information has the capacity to significantly intrude on citizen's privacy. The extent to which it does would depend on how it operates in practice, and what protections exist technologically and in law against misuse and abuse.

Another PIT is the use of fingerprint scanning technology to purchase groceries. A system called SecureTouch-n-pay[12] developed by Biometric Access Corporation has reportedly been introduced into Kroger convenience stores in the United States. To enrol in the systems, customers must show a Kroger representative their driver's license and a credit card and have their fingerprints recorded. Customers then present their fingerprint and a PIN (typically their phone number) in place of a card payment at the check-out to validate their payment.[13] This system appears to require a disproportionate level of identification for such a simple, and potentially anonymous, transaction as purchasing groceries.

A technology on the drawing board that also carries the risk of tracking individuals through their grocery purchases is the replacement of bar codes with microchips and radio transmitters. This has significant potential to improve distribution mechanisms for goods and to speed up grocery check-outs. It also carries a privacy risk that goods could be tracked from the manufacturer all the way to the individual consumer's home.[14] In the development and design of new technologies, considerations need to be given not just to the intended uses of a product, but also potential unintended consequences that may adversely affect individuals' privacy. The intended effects in this case may greatly improve distribution networks and enable enhanced stocktaking. The unintended effects could involve tracking individual consumers and collection of information on individual purchases if linked to identifiable payment options.

Privacy intrusive technologies can also be inherently intrusive, for example Spyware products. An example is iSpyNow,[15] a computer monitoring product that allows for remote monitoring of another user. It logs all websites visited, logs both sides of chat conversations, captures information on every window the individual interacts with, tracks every application executed, captures text and images sent to a clipboard and tracks all keystrokes. It is installed by sending it as an e-mail attachment to the user to be monitored and is designed to be undetectable.

In contrast, PETs have the potential to bring some trust, permission and control into the equation. Information technology companies are currently investing considerable resources in developing new technologies which aim to provide the necessary functionality while protecting privacy. Technological means to protect privacy can involve restricting access to privacy related information or the development of systems that provide the necessary functioning without needing to reveal privacy related information. Restrictive tools include cryptographic encoding such as public key infrastructure and digital signatures or systems that simply do not generate the information in the first place. These can be supplemented with technical tools that specify the privacy preferences of individuals.

One new technology which claims to be a PET is IDEMIX[16] developed by IBM. IDEMIX stands for "identity mix". This enhanced public key technology tool claims to provide authentication functionality without revealing an individual's identity. In the IDEMIX system organisations only know users by their pseudonyms. The user can have a different pseudonym for each organisation and these different pseudonyms cannot be linked. A key part of IDEMIX is a "pseudonym authority" which users can access easily and which grants users "pseudonym credentials". Most online services generally require you to provide a user name and password to use them. With IDEMIX the user first selects a pseudonym and registers that pseudonym and then receives the corresponding credentials and an electronic signature. If the user then wants to access the service, he or she need only provide proof to the service that the corresponding digitally signed credentials are in his or her possession. The pseudonym and credentials are given to the online service in an encrypted form and the online service is not able to decrypt them, but they can verify the authenticity of the encrypted pseudonym with the pseudonym authority. A new encryption is used every time the user presents the credentials to another organisation. The system comes with other important controls, including prevention of re-use of information and self-destruction of the data on misuse.

This system and others like it allow for "pseudonymity" rather than anonymity. In many cases total anonymity may not be appropriate. If the identity of the individual is necessary, for example in an investigation of fraud, the pseudonym authority can uncover the individual user's identity.

Biometric encryption is another new technology with the potential to enhance privacy protection. Biometric encryption uses a person's biometric such as a finger pattern or iris scan and uses it as part of an encryption algorithm to encrypt a PIN number. The finger pattern is not stored and the PIN number cannot be decoded without your live finger pattern. Only the individual with a particular biometric can gain access to an account or computer system. With this system, the biometric cannot be used as a universal identifier as it is used to encrypt a different number or alphanumeric for each application. There is not one single link as each encryption is different and cannot be matched.[17]

Another example of a potentially privacy enhancing technology is P3P (Platform for Privacy Preferences)[18] – a technical standard developed by the Worldwide Web Consortium (W3C) designed to allow users to set privacy preferences in their browser and prevent access to sites that do not accord with the user's preferences. While this technology does not protect privacy itself, it can enable individuals to make appropriate privacy choices.

The availability of such technologies alone is not sufficient to ensure that PETs predominate over PITs. The technologies for digital cash and other anonymous and pseudo-anonymous online payment systems have been available for some years, but have not been widely implemented. While there may be other factors to account for this, one factor may be that existing online credit card payment systems also provide the vendor with a rich source of personal information about the purchaser. Market pressures are an important factor to address in promoting the development of adequate privacy protection in the context of new technologies.

The Market and Identity

There are a range of competing commercial pressures relevant to identification and privacy and new technologies. These include

- levels of identification needed for commercial transactions;
- the trend towards market customisation and customer profiling;
- the marketing benefit of privacy protective customer management;
- pricing mechanisms.

There is some commercial pressure to increase capacity of organisations to collect information about individuals. However, in most commercial transactions the identity of an individual consumer is actually less important than other assertions the individual may make. This is partly because the consumer often carries the transaction risk. This is generally the case in the credit card payment transactions where the customer is purchasing goods or services online, sight unseen. More importantly, in most commercial transactions the customer's claim to provide a consideration of a particular value is more essential than their identity. This may involve clearing credit card details, counting the cash offered for payment or checking the receipt of the item returned for refund

or exchange. Other assertions may involve checking if the person has a particular attribute, for example the individual is a licensed builder and therefore entitled to the trade discount. Here again, it is not the individual's identity as such, but rather the fact that they have the required attribute which is at issue.[19]

Consumer identity will be relevant to some commercial transactions where the consumer is undertaking to provide a guarantee or perform a function specific to that person, such as collect a credit card. For the majority of cases identity is actually not required.

However, there are commercial pressures to collect identifying information to enable closely targeted marketing and customer profiling. Customer profiling can improve the personalisation of customer services and increase marketing efficiency and significantly reduce advertising costs. This can involve some confusion of purpose. Some consumer research indicates that most users prefer to give out only information needed for a transaction.[20]

Identified information is often collected in the form of loyalty schemes and competition entries. The stated need for identity information may refer to distribution of prizes, but the company's intended purpose is to use the identified information for marketing purposes. This kind of mismatch between consumer and business expectations can lead to a breach of customer trust. On the other hand, customer relations management undertaken openly, with the agreement of the customer and under the customers control can, and has, markedly increased levels of trust between the customer and the vendor.

Retaining the consumer's trust is a key element in business to customer relations and an important market consideration. The importance of privacy to levels of consumer trust in electronic commerce has been one of the drivers to the development of the P3P technology, which allows computer readable privacy policies. Some industry players have adopted privacy protection as a critical business practice in response to the levels of public concern about privacy.

Early in 2002, Microsoft launched a multifaceted "trustworthy computing" initiative. "Trustworthy Computing" refers to ensuring that computing is available, reliable and secure.[21] Privacy was listed as a key element of the initiative including: allowing individual users to control how their information is used; clear policies on information use; and easy mechanisms to allow users to specify their preferences. One element is a new hardware and software architecture for the Window PC platform called Palladium.[22] This technology is to be included in a future version of Windows. It will enable applications to run only "trusted" code that is physically isolated, protected and inaccessible to the rest of the system. It is intended to reduce the risk of many viruses and spyware. Files within the Palladium architecture will be encrypted with secret coding specific to each PC with the intention of making them useless if stolen or surreptitiously copied. Palladium will also allow users to operate in different "realms" within their PC in order to keep public and private information separate. It could also allow users to protect their privacy online through the incorporation of P3P technology in Internet Explorer. This would allow individuals to set their own privacy levels and the browser will then compare any P3P compliant website's privacy practices with the user's privacy settings.

Microsoft's initiative is claimed to be in response to market demand to make computing more trustworthy. Interestingly, this Microsoft initiative is also being underpinned by law. On August 8, 2002, Microsoft entered into a consent agreement with the U.S. Federal Trade Commission ("FTC") to improve its practices including submitting some of them to external audit. The agreement was the resolution of an investigation by the FTC into a complaint made by the Electronic Privacy Information Center in July 2001.[23]

Market pressures include not only consumer demand and preferences, but also pricing mechanisms. Pricing mechanisms can also be an effective influence on the role of the market in respect to privacy. One example is the prevalence of spam in e-mail platforms compared to mobile phone text messaging ("SMS"). The cost of sending huge volumes of unsolicited e-mail marketing messages is very low. As a result, e-mail spam is a significant problem worldwide. In contrast, the level of SMS spam is relatively low in Australia. This could largely be attributed to the pricing mechanism. In this country, mobile phone text messaging was established on a pay-to-send basis. According, it is not commercially viable to send the same volume of SMS advertising messages as in some other countries. In contrast SMS spam is a significant problem in Japan which has a relatively open network architecture, that allows spammers to use IP-based services to send out bulk text messages that cost little or nothing. Under this system the customer pays for all the data they receive, including spam.[24]

Market pressures can promote both privacy enhancement and privacy intrusion. It will not be sufficient to leave privacy protection to the market, as there are too many areas where the privacy impact of different choices is not transparent. In many cases, consumers are unaware of the impact some industry practices have on their privacy and so cannot influence company behaviour through the marketplace.

The lack of information individuals may have about business information handling practices is a classic case of market failure. Laws are needed to enable individuals to make privacy choices where the market alone may not. Effective privacy protection also relies on the role of law to address broad public policy considerations.

This Paper was first delivered at the Union Internationale des Advocats (UIA), 75th Anniversary Congress held in Sydney on October 28, 2002.

1 C. Bennett & R. Grant (eds.) *Visions of Privacy: Policy Choices for a Digital Age* (University of Toronto Press, Toronto: 1999)

2 J. Reidenberg, Fordham University School of Law *Privacy Protection and the Interdependence of Law*, Technology *and Self-Regulation* prepared for the conference "On the Brink of New Evolutions in the Law of Information Technology" for the 20th Anniversary of the C.R.I.D., Nov. 7-9, 1999 available at *http://reidenberg.home.sprynet.com/Interdependence.htm*

3 A. Cavoukian, D. Tapscott, *Who Knows: Safeguarding your privacy in a networked world* (Random House, Toronto: 1995) p. 124

S. Warren and L. Brandeis, 1890, "The Right to Privacy",
4 Harvard Law Review 193, 1890 available at: *www.louiseville.edu/library/law*
5 D. Brin, *The Transparent Society – will technology force us to choose between privacy and freedom* (Perseus Books: New York, 1998) p.3
6 Z. Cowan, Australian Broadcasting Corporation Boyer Lectures 1969 "The Private Man"
7 J. Rachels "Why Privacy is Important" in F. Shoeman (ed.) *Philosophical Dimensions of Privacy* (Cambridge University Press: Cambridge, 1984) pp. 290-299 quoted in Helen Nissenbaum "Towards an Approach to Privacy in Public Challenges of Information Technology" in *Readings in cyberethics* by Richard A. Spinello and Herman T. Tavani (eds.) (Jones and Bartlett Publishers: Boston, 2001)
8 Ruth Gavison "Privacy and the Limits of Law" Yale Law Journal 1980, Vol. 89 pp. 421-471 quoted in Diane Rowland, " Anonymity, Privacy and Cyberspace" paper presented to the 15th Bileta Conference: *Electronic Datasets and Access to Legal Information* Friday 14 April 2000, University of Warwick, Coventry England available at *www.bileta.ac.uk/00papers/rowland.html*
9 Roger Clarke "The Mythology of Consumer Identity Authentication" (Paper for 24th International Conference of Data Protection & Privacy Commissioners, Cardiff UK September 9-11, 2002)
10 Registratiekamer, The Netherlands and Information and Privacy Commissioner Ontario, Canada "Privacy Enhancing Technologies: The Path to Anonymity" Volume II (August 1995) available at *www.ipc.on.ca/english/pubpres/papers/anon-e.htm*
11 Sarah Andrews "Privacy & Human Rights 2002: An International Survey of Privacy Laws and Developments" p. 266-267 Privacy International available at *www.privacyinternational.org/survey/phr2002/*
12 *www.biometricaccess.com/products/touchnpa.htm*
13 "Shopping at your fingerprints" p.14 in MX Melbourne on Wednesday, May 22, 2002.
14 "Check this out – the Jetson's Supermarket" Sydney Morning Herald October 1, 2002.
15 *www.coolspyproducts.com/ispy/?code=ispygc0709*
16 *www.zurich.ibm.com/security/idemix/*
17 George J. Tomko "The Privacy Threats Associated with Template-Based Biometric Identification" presented to the 24th International Data Protection Commissioners Conference, September 1012, 2002, Cardiff, Wales. Available at *www.informationrights2002.org/presentations/tomko_Workshop_4ppt.*
18 For more information on P3P see *www.w3.org/P3P/*
19 Roger Clarke (2002) op. cit.
20 Ann Cavoukian, Michael Gurski, Deidre Mulligan and Ari Schwartz *P3P and Privacy: An Update for the Privacy Community* (March 28, 2002) available at *www.ipc.on.ca/english/pubpres/p3p.htm*
21 Bill Gates "We can and must do better" e-mail sent to Microsoft employees on 15 January 2002 available at *http://news.com.com/2009-1001-817210.html*
22 *www.microsoft.com/PressPass/features/2002/jul02/0724palladiumwp.asp*
23 Federal Trade Commission "Microsoft Settles FTC Charges Alleging False Security and Privacy Promises" (8 August 2002) www.ftc.gov/opa/2002/08/microsoft.htm
24 Andy Polaine "Protecting the extension of your personal space" *The Age,* May 14, 2002 available at *www.theage.com.au/articles/2002/05/10/1021002428754.html*

"Under the Gaze, Privacy Identity and New Technology" was written by the Office of the Federal Privacy Commissioner (OFPC) and reproduced with their permission. © OFPC.

Part II of this paper, to be published in the May issue of World Data Protection Report*, will discuss the themes of Law and Identity and the challenge of retaining privacy against the demands and requirements of the marketplace.*

FORTHCOMING EVENTS

2003 World Computer and Internet Law Congress

May 2003 (Washington, DC) The 2003 World Computer and Internet Law Congress, produced by the Computer Law Association, will take place on May 1–2, 2003 in Washington, DC. For further information, please contact Barbara Fieser at the Computer Law Association, tel: (703) 560 7747; fax: (703) 207 7028 or visit: *www.cloa.org/claconfs.htm*

25th International Conference of Data Protection and Privacy Commissioners

September 2003 (Sydney) The 25th International Conference of Data Protection and Privacy Commissioners will be held in Sydney Australia, September 10-12, 2003.

The Australian Federal Privacy Commissioner will be hosting this year's event.

The theme of the Commissioners' Conference for 2003 is "Practical Privacy for people, government and business". In this, the 25th year of the Conference, the Australian Privacy Commissioner has created a stimulating programme, which provides a relevant forum for consumer, business and regulatory interests to debate privacy and to exchange their knowledge and experience of privacy and its implementation.

The emphasis will be on what has worked; what has not; why? – All from the different perspectives of participants. This Conference will also continue to build on some of the successful themes that were presented at the 24th International Conference held in Cardiff, Wales in 2002.

An event business leaders, advisors and privacy professionals cannot afford to miss. Registration will be available online. For further information on the Commissioners' Conference please visit the website at: *www.privacyconference2003.org.*

Review

Books

Please note that the correct title of Christopher Kuner's new book on data privacy and e-commerce in Europe is *European Data Privacy Law and Online Business. WDPR* apologises for the incorrect citation given in the March issue.

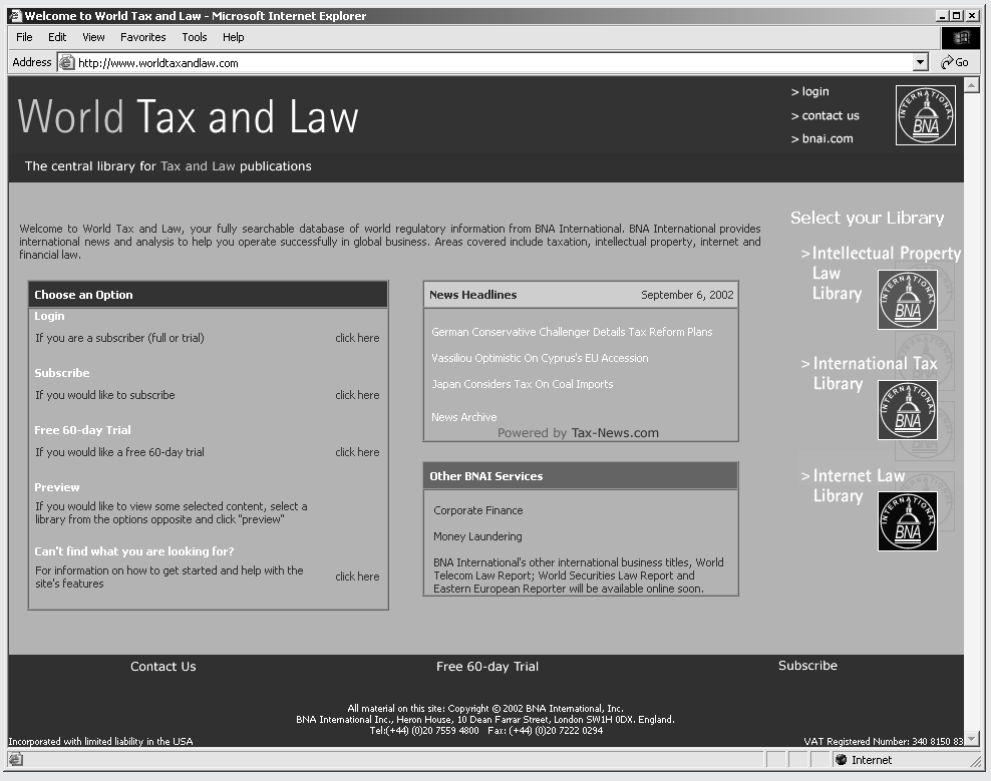
(*European Data Privacy Law and Online Business* is published by Oxford University Press, ISBN 0-19-924423-5, £85.00)

Upgrade your subscription today to include web access

Go straight to the article you're looking for

Have you ever needed to locate an article but can't remember which issue it appeared in? Or gone to the library only to find that the copy you want has disappeared?

World Data Protection Report is now available on the Web and for only a small additional amount you can upgrade your subscription to include Internet access and keep your print.



Add web access to your subscription and receive:

- E-mail notification every time a new issue is added to the website
- Immediate web access to each issue – no need to wait your turn on the circulation list

BNA International Inc., Sixth Floor, Heron House, 10 Dean Farrar Sreet, London SW1H 0DX, UK
Phone: + 44 (0) 20 7559 4801 Fax: + 44 (0) 20 7222 5550
Email: marketing@bnai.com Website: www.worldtaxandlaw.com