Privacy Laws & Business International Data Protection Roundup

THE DATA PROTECTION ROUNDUP has now been divided into two parts because it has become too large to fit into one newsletter. A future international newsletter will feature more countries.

Anyone with comments on the information published here, or who wishes to write a report on a country which is not featured here, should contact the Associate Editor, Eugene Oscapella at eugene@privacylaws.com.

ARGENTINA

New legislation on personal data protection was enacted in November 2000 after the Executive Branch vetoed a regulatory law approved by Argentina's Congress in 1996. The new law (no. 25.326) on Personal Data Protection, also known as Habeas Data, provides personal data with greater protection than already granted by article 43 of Argentina's Constitution.

Although some provisions of law no. 25.326 are not self-executing (they must still be regulated by a proposal recently forwarded to the President by the Minister of Justice and Human Rights), others took effect when the statute was enacted.

The Habeas Data law applies to public databases (owned by federal, state and municipal entities) as well as to private databases that "provide information to third parties."

Several features of the law are compatible, but not identical, with the EU Data Protection Directive:

• Permits processing of sensitive data only in the public interest, as provided by law;

• Requires an opt-out option for consumers from marketing lists and databases;

• Obliges entities to maintain data only for the purposes described;

• Provides individuals with a right of access to personal information kept by companies;

• Permits data to be transferred outside Argentina, contingent on the recipient country having an adequate protection law.

Innovative provisions also provide consumers with new rights. However, the requirement for companies maintaining databases to register with a national Data Protection Authority has not yet been created by these regulations.

Cristiane Marrey Moncau (cristiane@mattosfilho.com.br) and Ignacio María Bérèterbide (imb@allendeebrea.com.ar)

AUSTRALIA

The last year has seen many developments in privacy regulation in Australia.

Federal issues: Extending the Privacy Act to the Private Sector

In December 2000, the Privacy Amendment (Private Sector) Act passed the Federal Parliament, and took full effect in December 2001. This Act has extended the Privacy Act 1988 to cover larger businesses in the private sector, subject to some major exemptions such as the media and political parties, and employee records. Organisations are required to comply with ten National Privacy Principles (NPPs), based on the voluntary principles developed by the Privacy Commissioner during extensive consultations in 1997-98. The Act extends to the private sector the rights individuals have enjoyed in dealings with federal agencies since 1989 – to complain about breaches of the principles, and to access and correct data about themselves subject to exemptions.

A novel feature of the new private sector regime is its provision for Codes of Practice which can not only replace the NPPs (as long as the overall level of protection is not weakened) but can also introduce a sectoral Code Adjudicator as the first level of external dispute resolution. The government had intended this to be a complete substitute for the statutory complaint-handling regime, but an amendment forced by the Senate made the decisions of Code Adjudicators subject to appeal to the Privacy Commissioner.

Draft Guidelines on Codes, Principles and Health Sector

In 2001, the Federal Commissioner issued three sets of draft guidelines on the operation of the new regime, covering Code development and approval; interpretation of the NPPs, and application of the law to the

health sector. The first two have proved particularly controversial. The Code guidelines demonstrate starkly the high standards of both consultation and independence that will be required to gain approval of a Code that includes a Code Adjudicator. It is clear that establishing and maintaining such machinery will be costly, and as a result, several industry sectors expected to submit a Code for approval are now re-considering.

The NPP Guidelines have been even more controversial. The Commissioner's initial position in his draft Guidelines (May 2001) favoured individuals' interests over those of organizations much more than had been expected. Business groups were strongly critical of the Commissioner's interpretation on such matters as the meaning of consent (how informed? how free?); the need to specify a single primary purpose of collection, and the requirements for opt-in or opt-out for direct marketing. In some cases, even privacy advocates accepted that the Commissioner's interpretation did not appear to be well founded in law. Revised guidelines were issued in September 2001. These guidelines are considerably shorter and less detailed, thereby avoiding many of the more contentious issues.

Children's Privacy

The federal government has convened a consultative group to review existing Commonwealth privacy laws to consider whether there is a need for more specific protection of children's personal information. The group, which includes the Federal Privacy Commissioner, will review a discussion paper on children's privacy to ensure that all relevant issues have been fully considered before releasing it for public consultation.

Sectoral privacy issues

There have been several public sector initiatives during the year that raised significant privacy issues.

Forensic DNA data

A new system for collecting, storing and using DNA samples for law enforcement took effect. Complementary federal and state legislation dealing with forensic evidence has been passed and a new federal agency – CRIMTRAC – established. Samples are now being collected not only from suspects in new crimes, but also, compulsorily, from prisoners to match against crime scene evidence from unsolved crimes. The legislation also provides for samples to be taken from volunteers during major crime investigations. Some privacy safeguards have been put in place, but it remains to be seen if they are effective.

Detecting and prosecuting computer crime

Early in 2001, state and federal governments issued a report on a Model Criminal Code on Damage and Computer Offences. NSW has already enacted its version of the law without any opportunity for debate. A Senate Committee is at least considering the equivalent federal Cybercrime Bill 2001. The Bill has two main components; changes to the definitions of computer offences, and new investigatory powers for the federal police and other law enforcement agencies. Both parts have been strongly criticized – not only by privacy and civil liberties groups but also by the Information Technology Industry and professionals. Technologists say that the new computer offences are so broadly drawn that they will inadvertently criminalise many innocuous and even essential activities. And there are concerns about both the justification and the breadth of the investigatory powers.

National medication database

In May 2001, the federal health department put out a draft Bill to implement a Better Medication Management System (BMMS). The system would provide a centralized national database of prescription and dispensing of pharmaceuticals. Although the draft legislation was based on a voluntary opt-in model (both for patients and providers), it was widely criticized, not least on privacy grounds. The Health Department is understood to be re-considering it approach. In the meantime, all jurisdictions in Australia are discussing various proposals for electronic health records and privacy issues are at least recognized as highly significant.

Public Key Infrastructure

The federal government has been developing a framework for the use of public key infrastructure (PKI) for government use, and is reluctantly being forced to recognize the implications for its wider use in all sectors. This recognition led the National Office for the Information Economy (NOIE) to fund a project that resulted in the federal Privacy Commissioner drafting PKI privacy guidelines. The guidelines acknowledge the significance of such matters as individuals' ability to have more than one digital certificate, providing for attribute certificates which do not require identification, and access to certificate revocation lists as a form of transaction monitoring.

Nigel Waters,
Pacific Privacy Consulting,
Tel: +61 (0)2 4981 0828
Fax: +61 (0)2 4981 0995
E-mail: nigelwaters@iprimus.com.au

BELGIUM

The adoption of a new Royal Decree in February 2001 (Arrêté Royal portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel) determined the entry into force on September 1st 2001 of the Belgian data protection law implementing the EU Data Protection Directive.

The Decree tackles a number of issues left open by the law including:

- conditions for processing personal data for historical, statistical, or scientific use;

- conditions for processing special categories of data;

- exemptions to the individual's

right to be informed, and

• exemptions to the obligation to notify the Belgian Data Protection Commission about processing of personal data.

However, the decree has not dealt with such issues as the transfer of data outside the European Union, preferring to leave this issue open until a common position has been adopted between the Member States and the European Commission.

Sophie Louveaux, Namur, Belgium
Tel: +32 (0)81 403636
Fax: +32 (0)81 403635
E-mail: sophie.louveaux@fundp.ac.be

BRAZIL

The Brazilian Constitution provides a right of privacy as well as a Habeas Data legal action, which gives Brazilian citizens the right to find out what personal information the government maintains on them, and the right to correct it at no cost.

Although Brazil has no specific statute on personal data protection, several important laws deal with the issue, namely:

• the Consumer Code,

• the Criminal Code,

• the Intellectual Property Code and

• the Supplementary Law 105/2000 on the confidentiality of financial institutions' transactions.

Some bills before the Congress deal with the operation and protection of databases, mainly concerning transactions carried out over the Internet.

Another bill currently in the Congress, Bill no. 268 of 1999, is similar to the EU's Data Protection Directive. If approved, the Bill will apply to electronic or manual processing of records. However, it comprises only some of the features of the Directive, such as provisions on consent, sensitive data, and prohibiting its collection, except with the owner's express authorisation.

Cristiane Marrey Moncau
(cristiane@mattosfilho.com.br)

CANADA

Canada has acceded to the International Covenant on Civil and Political Rights and is bound by the privacy obligations set out in Article 17.

In 1984, Canada adhered to the OECD Guidelines for the Protection of Privacy and Transborder Flows of Personal Data. The Guidelines underlie the public and private sector data protection legislation that has been enacted in Canada to date.

The Canadian Charter of Rights and Freedoms, Canada's statement of constitutional rights, does not explicitly guarantee privacy rights. However, courts have interpreted sections 7 and 8 of the Charter as affording privacy rights when dealing with federal and provincial government institutions (although not private sector organizations), most often in criminal cases. Section 7 provides the right to "life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice." Section 8 provides the "right to be secure against unreasonable search or seizure." In R. v. Plant (1993), the Supreme Court of Canada held that this section 8 protection extends to a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.

Public Sector

Canada's Federal Privacy Act was passed in 1982. It came into force in 1983 and applies to the federal government and federal agencies. The Privacy Commissioner of Canada oversees the Act, and has powers, among others, to receive complaints, conduct investigations and attempt to resolve disputes. The Commissioner may also issue recommendations. Disputes about access by individuals to their personal information that are not resolved in this way can be taken to the Federal Court of Canada for judicial review.

Private Sector (federally-regulated)

In January 2001, the Personal Information Protection and Electronic Documents Act took effect, subjecting the federally-regulated private sector (banking, telecommunications and inter-provincial transport) to general data protection legislation. Although the law was enacted by Parliament in 2000, its provisions concerning personal health information entered into force on January 1, 2002.

The Act applies to the regulated organizations' collection, use and disclosure of personal information when undertaking their commercial activities. Unless the provinces bring in similar data protection provisions within three years of the Act's coming into force (only Quebec has done so to date), the law will extend to the entire Canadian private sector, not merely that regulated by the federal Parliament.

The backbone of the Act is Schedule 1, which contains the Model Code for the Protection of Personal Information. The Code is the product of a committee of representatives from consumer groups, business, government and labour. They spent three years under the auspices of the Canadian Standards Association (CSA) developing the Code, completing it in 1995. Also known as the CSA Code, it was approved as a national standard by the Standards Council of Canada and was published in 1996.

The Code sets out and elaborates 10 data protection principles. These are: accountability, the duty to identify the purposes of collection, the duty to obtain consent, limits on collection, limits on use, disclosure and retention, accuracy, security safeguards, openness, right of access and authority to challenge compliance with the principles. In essence, the drafters of the CSA Code took internationally accepted fair information principles and introduced them into the Canadian environment.

The Act requires every organiza-

tion subject to its jurisdiction to comply with Schedule 1(and, hence, the Code), with only minor exceptions. The Act, therefore, comes as close as one can realistically expect to reflecting a broad consensus on measures to protect personal information held by the private sector.

Under the Act, personal information is any information about an identifiable individual. Organizations include associations, partnerships, persons and trade unions. "Bricks and mortar" and e-commerce businesses are both covered. The term "commercial activity" includes the selling, bartering or leasing of donor, membership or other fund raising lists.

Private Sector (provincially-regulated)

Quebec is the only province to date that has enacted broad data protection legislation governing the private sector. In the rest of Canada, data protection in the private sector is sporadic and uneven. Some industries are not subject to any rules on collecting, using and disclosing personal information. A few are covered by what the Privacy Commissioner of Canada describes as a "patchwork" of laws, regulations and codes. The patchwork consists of various federal and provincial laws (for example hospital records, health-care and credit reporting legislation), resulting in protection that is incomplete and possibly inconsistent. This patchwork makes for uncertainty for business and gives consumers uneven protection.

The Uniform Law Conference of Canada (ULCC), an independent group promoting uniform legislation across the country, has been working since 1995 on a draft Uniform Data Protection Act. The provinces, territories and the federal government are each represented on the ULCC.

As well, four provinces have enacted statutory privacy torts, which give individuals a right of action against those, sometimes including governments, who violate their privacy without the right to do so. Quebec also has privacy provisions in its Civil Code. These provisions are broad enough to cover privacy violations relating to data. However, individuals rarely use the remedies provided by such legislation, perhaps because of the cost of taking legal action.

By January 2004, the Personal Information Protection and Electronic Documents Act will extend to any provinces that have not passed similar data protection provisions.

Eugene Oscapella:
eugene@privacylaws.com

PEOPLE'S REPUBLIC OF CHINA

The Provisional Measures Concerning Foreign-related Social Survey Activities (the Measures), which were promulgated by the National Statistics Bureau on 15th August 1999, may be the first data protection legislation in Chinese law.

Principles

The Regulations are built around two principles (Article 6):

Principle one: One must not use social survey activities to procure state secrets and to prejudice the state's interests and public interests.

Principle two: One must not use social survey activities to prejudice others' interests and (the collector) is under a duty of confidence.

The National Statistics Bureau and provincial statistics bureaus

The National Statistics Bureau and provincial statistics bureaus are the authorities supervising the foreign-related survey activities (Article 7). They more or less play the role of the Data Protection Commissioner.

Duly licensed institution

Article 8 of the Regulations stipulates that provincial statistics bureaus or the National Statistics Bureau shall duly license any institution engaging in foreign-related survey activities. Individuals are prohibited from taking part in social survey activities.

A duly licensed institution essentially functions as the "data controller" as in the UK Data Protection Act 1998. It is mandated to take strict organisational measures against disclosure of information (Article 8 (4)) obtained during survey activities. Disclosure of confidential information without data subjects' consent could lead to withdrawing the license.

Application for approval to conduct a specific social survey

To obtain approval for a social survey, a duly licensed institution must submit a proposal to provincial statistics bureaus (when the data subjects concerned are in one province) or to the National Statistics Bureau (when the subjects are in two or more provinces). The process appears stricter than "registration" under the UK Data Protection Act 1984 and "notification" under the UK Data Protection Act 1998.

The Regulations can be regarded as a landmark in Chinese data protection legislation, although they apply only to foreign-related social survey activities. Since China became a member state of the World Trade Organisation on December 11th 2001, it is expected that increasing cooperation between China and the EU will prompt establishment of data protection principle like "safe harbours" in China.

Chao Xi
LLB (Hons.) (Zhongshan Uni.)
LLM (UCL)
E-mail: c.xi@ucl.ac.uk

CZECH REPUBLIC

Data protection in the Czech Republic is based on Act No.101/2000 Coll. (Data Protection Act), and amends some related Acts. The existing legislation secures a level of personal data protection comparable with the EU standards, in particular Directive 95/46/EC.

The Act No. 101/2000 Coll. (Data Protection Act) was introduced on 4th April 2000 and took effect on 1st June 2000. The Act No.177/2001 Coll. was introduced on 16th May 2001 and became effective on 31st May 2001.

The above legislation applies to the protection of privacy of individuals when processing personal data either in an automatic or any other manner. The Data Protection Act defines such terms

as "personal data", "sensitive data", "anonymous data" as well as "data subject" or "personal data processing."

Some provisions of the Data Protection Act do not apply to certain special personal data processing carried out by the Intelligence Services, Police, Ministry of Finance, National Security Office and Ministry of Interior (for example, while investigating criminal offences, in activities against money laundering, and when processing classified information). Other exemptions are provided for using data for statistical and archival purposes.

The Act No.101/2000 Coll. empowers the independent supervisory authority – the Office for Personal Data Protection – to impose direct financial sanctions and to take other immediate measures, such as blocking data processing.

Data Protection clauses in other legislation or statutes

Credit Reporting: Act No. 21/1992 Coll., on Banks, amended by Act No.16/1998 Coll., includes some provisions applying to data protection. Act No.21/1992 Coll. was introduced on December 20th 1991 and became effective on February 1st 1992. The amending Act No.16/1998 Coll. was introduced on January 13th 1998 and entered into force on February 6th 1998.

Consumer Law: In this field, the Czech Republic has Act No.104/1995 Coll., amending and supplementing Act No.634/1992 Coll., on Consumer Protection, as amended by Act No.217/1993 Coll. and Act. No. 40/1995 Coll., and amending Act No.40/1964, the Civil Code, as amended. This Act (effective July 1st 1995) protects individuals and legal entities who purchase products or use services for purposes other than conducting business with these products or services.

Internet, e-mail and anti-hacking legislation

The only direct legislation is Act No.227/2000 Coll., on Electronic Signatures, containing no special data protection provisions. The general Act No.101/2000 Coll. is fully applicable in these fields. More than 80 special Acts mention personal data protection. Overall, the main aim is to define possibilities and limitations of access to personal data of a special nature and for special purposes.

Freedom of Information legislation (enacted and/or pending)

Legislation in this field is based on Act No.106/1999 Coll., on Free Access to Information. This act regulates access to information and stipulates fundamental conditions upon which the information can be disclosed.

The Act No.106/1999 Coll. was introduced on May 11th 1999 and entered into force on January 1st 2000.

The Act applies basically to central and regional state administrations, bodies and institutions running public financial services. Article 3 paragraph 3 is unclear as to the information which is included in access and retrieval, and many problems occur as a result of this unclear definition. Act 101, passed in 2000, clarifies the law by saying that if information contains personal data, then the data protection law will apply, but, in practice, this provision gives rise to complications, and gives excuses for civil servants not to disclose information. But, in general, the free access to information law has established some authorities with the duty to be more open to its citizens' requests.

The Act does not apply to providing personal data and information according to special legal regulations (e.g. Act No.101/2000 Coll./Data Protection Act/Act No.123/1998 Coll., on Right of Information on the Environment), or to providing classified information.

Constitutional Privacy Protection

The Constitution of the Czech Republic (1993) includes provisions relevant to the citizens' fundamental rights and duties, and human rights. Articles 3 and 10 of Part 1 are relevant:

Article 3: The Charter of Fundamental Rights and Freedoms is part of the constitutional order of the Czech Republic.

Article 10: Ratified and promulgated international agreements on human rights and fundamental freedoms bind the Czech Republic and have priority over the law.

Mr Karel Neuwirt,
Office for Personal Data Protection,
Prague, Czech Republic
Tel: +420 (0)2210-08288
Fax: +420 (0)2227-18943
E-mail: neuwirtk@uoou.cz

DENMARK

The Processing of Personal Data Act 2000 (lov om behandling af personoplysninger) establishes the level of data protection. The Act, which adopts EU Directive 95/46, was enacted in May 2000 and came into force two months later. The purpose of the Act is to ensure that personal data in both the public and private sector are used in such a way as to protect the personal integrity and privacy of citizens. The Act covers the private sector without exceptions, public administration and the courts. Parliament and institutions under Parliament, such as the ombudsman, are exempted and regulated directly by the Directive. The Act applies to data concerning individuals but not to legal persons (except for rules on credit reporting bureaus).

Violations of most of the rules can be dealt with using criminal sanctions. Violation of rules covering broad standards, such as fair processing, are not subject to criminal sanctions. However, non-adherence to the Data Protection Agency's decisions on the actual meaning of such a standard, can be a criminal offence and lead to criminal sanctions.

Other data protection measures

Section 6a of the Marketing Act (lov om markedsføring) regulates use of personal data in direct marketing. However, disclosure to other companies is covered by the Processing of Personal Data Act. Section 6a was enacted in 2000 and aims to provide strong protection for consumers. There are no exemptions and it is a criminal offence to violate this rule.

Section 12 of the Payments Act (lov om betalingsmidler), enacted in 2000,

prohibits using for marketing purposes personal data derived from such transactions as credit card purchases. Even the data subject's consent cannot make such usage legal. The purpose of this rule is to reduce the dangers that can result from the electronic trails left by credit card usage. It is a criminal offence to process data on what has been purchased. However, there is some latitude on processing data on *where* a credit card has been used.

Freedom of information legislation

FOI has been part of Danish law since 1970 and the current Act dates from 1985 (lov om offentlighed i forvaltningen). Its aim is to enable the general public to gain access to documents held by public authorities. Anyone can demand access and the demand need not be explained. The Act covers all documents that do not contain information specifically exempted – such as information that is strictly personal or concerns state security and defence. There are no sanctions other than administrative disciplinary action against civil servants who violate the act.

The Danish Constitution of 1953 contains no article directly aimed at protecting privacy.

Professor Dr. Peter Blume,
University of Copenhagen
E-mail: Peter.Blume@jur.ku.dk

ESTONIA

Two laws regulate data protection: the Personal Data Protection Act and the Databases Act. However, several other laws contain provisions regulating data processing and liability, including the Health Protection Act, Archives Act, State Secrets Act, Accountancy Act, Statistics Act, Criminal Code, Code of Administrative Offences, and the Public Information Act. (www.legaltext.ee/).

An independent supervision authority, the Data Protection Inspectorate, began functioning in February 1999. The Inspectorate is subject to the control of the Legislation Committee of the Riigikogu (Estonian Parliament), as required by Article 17 of the Databases Act.

The Personal Data Protection Act establishes (in Article 28) that the head of the data protection supervision authority is, in the performance of his or her functions, independent and shall act pursuant to the Personal Data Protection Act, other Acts and legislation established on that basis.

The main task of the Data Protection Inspectorate is to provide independent supervision of personal data processing and storage to ensure its legality, as well as to organize data protection activities. The Inspectorate establishes principles for responsible and authorised personnel dealing with databases, as well as the administrative penalties for violating the personal data rules.

In addition to the rights provided for in the Personal Data Protection Act and the Databases Act, the data protection supervision authority has the right to inspect at any time the compliance of state and local government databases. This power allows the Inspectorate to issue, where provided by law, licenses for processing and cross-usage of data, and for integration, expansion and liquidation of databases. The Inspectorate can also resolve disputes arising from data processing and, impose the punishments the law provides for unlawful data processing or violating the procedure for maintenance of databases.

Since April 24th 2001, the Data Protection Inspectorate has a new statute and structure. The Inspectorate, headed by the Director General, now has three departments: Analysis and Development Department, Control Department and Administrative Department. Of its 23 positions, 15 are now filled.

The most significant actions of the Data Protection Inspectorate have been the following:

• Specifying security requirements and devising respective security categories and standard methods. This work enables the Inspectorate to set security requirements and apply pre-

cautionary measures in a more flexible and formalised way. The Inspectorate completed the actual work in 2000 and gave it to the working group established by the Ministry of Roads and Communication.

• Commenting on draft legislation that directly or indirectly influences either personal data or data security as a whole;

• Organizing many training and information days to inform civil servants, people involved with sensitive personal data, as well as the general public. The topics have included basic knowledge about how to register, security, practical suggestions on processing personal data, particularly sensitive personal data, and introduction of new knowledge and trends;

• Processing sensitive personal data in the Data Protection Inspectorate;

• Consulting chief and authorised processors on their databases and legalisation of their data interchange; and

• Consulting personal data processors on data security, which often leads to a course of supervision after the organization submits its registration request.

In December 2000, Estonia ratified the Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (adopted in Strasbourg in 1981) after having signed the Convention in Strasbourg in January 2000.

The Inspectorate will pay special attention to processing sensitive personal data concerning individuals' private lives, medical information and legal aid.

Although the Data Protection Inspectorate has begun its supervision, Estonia needs the type of separate data security-supporting agency that is common in many other countries. The Inspectorate's future plans are linked to its aspiration to evolve from a national supervision authority to include the functions of a supporting agency for information security co-ordination.

Gina Kilumets
Head of Administrative Department
Data Protection Inspectorate
Republic of Estonia
E-mail: gina.kilumets@dp.gov.ee
www.dp.gov.ee

FRANCE

On July 24th, 2001, the French government published a bill amending France's Data Protection Law, to implement the EU Data Protection Directive n° 95/46 EC of October 24th, 1995. This draft was communicated to the National Assembly and will probably be enacted and enter into force in 2002.

Provisions regarding territorial scope

Conforming to the provisions of the Directive, the bill specifies the territory in which the French law is to be applied. It states (similar to several data protection laws in force within the European Union) that France's Data Protection Law will be applied to data controllers located in France, or to the processing of data whose controller is located outside of the European Union but uses technical means on French territory, such as collection of data online, or hosting of a server.

However, France's Data Protection Law will not be applicable to data controllers located in another Member State of the European Union, even when they process personal data in France. In such cases, the law of that Member State will be applied. But France's Data Protection Authority (CNIL) will have power to investigate in such cases.

CNIL's new powers and sanctions extended

The provisions of the bill extend the CNIL's authority and sanctions. The CNIL may adopt financial sanctions against the controller. The bill specifies that the sanctions may be up to 300,000 euros (£186,000) or 5% of the organisation's turnover in the event of repeated offences.

The CNIL will have the authority to impose a temporary or definitive ban on processing or block certain processed data. The CNIL will be able to lodge complaints and sue for damages (whereas currently the CNIL has only the option of referring the matter to the Attorney General who decides whether or not to sue).

The CNIL will have the power to monitor processing within French territory, even if the controller is located in the territory of another Member State of the European Union. In this case, because the French law will not be applicable, it seems that the CNIL will enforce compliance with the law in force of the Member State where the controller is located.

The CNIL will be also be able to perform checks within French territory at the request of another EU Member State's Data Protection Supervisory Authority.

Registration with the CNIL

The principle of prior registration of processing remains an obligation, and the bill lays down a great variety of registration administrative rules.

There are many exceptions to this principle of prior notification. Some of these exceptions consist of a reduction or removal of the prior registration administrative rules. The option already exists under the current law, to file a simplified registration, but there is now the possibility of obtaining exemptions from registration. For example, when a controller handles several processing operations, all having the same purposes and procedures, it may be necessary to file only one registration for all these processing operations.

However, there are also many instances where prior registration rules are made more detailed, such as processing operations containing sensitive data or requiring the consultation or registration of a national identification number, or of a file which includes a large part of France's population.

In those cases, the controller shall, according to the case, file an authorisation request or a recommendation request with the CNIL, which exercises, therefore, greater power of control before processing is lawful.

Some processing operations shall also obtain prior authorisation, issued not by the CNIL but by a decree, having received prior approval from the Council of State, or by an order issued by another authority such as one or more ministers, préfet, or mayor.

Information about data subjects and international transfers

The bill integrates the provisions of the EU Data Protection Directive relative to transborder flows of data and information about data subjects. These provisions of the bill are identical to the provisions of the EU Data Protection Directive. In practice, it seems that the CNIL favors a transborder data flow agreement to consent.

Ariane Mole, Attorney at Law,
Head of Data Protection
and Privacy Dept,
Alain Bensoussan, Avocats-Paris,
29 rue du Colonel Pierre Avia,
Paris 75015, France
Tel: +33 (0)1 41 33 3500
Fax: +33 (0)1 41 33 3536
E-mail: ariane-mole
@alain-bensoussan.tm.fr

GERMANY

The general purpose of the Federal Data Protection Act (BDSG 1977) (FDPA) is "to protect the individual's right of privacy from being impaired through the handling of his personal data." The original FDPA was passed on 27th January 1977 and substantially revised in 1990 and 2001. The present Act came in effect on May 23rd 2001. The Act covers collection, processing and use of personal data in the private and Federal public sector. Additional State (Länder) Data Protection Acts apply to the State public sector. There is an exemption for processing for private and family use. Sanctions enable supervisory authorities to impose fines up to DM 500,000 (£160,000 or $230,000). In addition, there is a criminal sanction of up to two years imprisonment.

Sector Specific Laws and Regulations

Telecommunications Act (TKG 1996) and Telecommunications Data Protection Ordinance (TDSV 2000): The Telecommunications Act of July 25th 1996 regulates the telecommunications sector. The purpose of the Act is to promote competition, guarantee appropriate and adequate services throughout the country and regulate frequencies. Article 89 of the Act enables Germany's Legislature's Upper House (Bundesrat) to legislate provisions on data protection and personal data for telecommunications providers. One such provision is the Telecommunications Data Protection Ordinance (TDSV 2000).

The Telecommunications Data Protection Ordinance (December 18th 2000) regulates the collection, processing and use of the personal data of parties engaging in telecommunications by companies and persons providing telecommunications services on a commercial basis or contributing to such provision.

Teleservices Data Protection Act (TDDSG 1997): This Act (July 22nd 1997) deals with protection of personal data used in so-called teleservices. The Act applies mainly to Internet services. In addition, some German states (Länder) have passed legislation on media services.

Freedom of Information legislation

There are no constitutional rights to freedom of information but the Federal Data Protection Act includes a series of provisions entitling the data subject to be informed about the data being processed.

Some of the states (Länder) have adopted Freedom of Information Acts. The purpose of such Acts is to encourage democratic formation of opinion through open access to administrative files. However, the laws require that personal data be safeguarded.

Constitutional right of privacy

There is no explicit constitutional "data related" right to privacy in Germany but, according to a landmark 1983 Federal Constitutional Court decision--the so called census decision (Volkszählungsurteil – BverfGE 65,1), the "right of informal self-determination" derives directly from Articles 1 and 2 of the German Constitution which regulate human dignity and liberty. In addition, Article 10 of the German Constitution states that "the privacy of letters as well as the secrecy of post and telecommunication is inviolable." The Article can be restricted by a statute when it serves democracy or security purposes, the case with the "G 10-Act" which regulates wiretapping.

Pending Data Protection legislation

A draft bill to revise the Teleservices Data Protection Act has been proposed by the Federal Government as part of the implementation of the European e-commerce Directive.

Ulrich Wuermeling,
Wessing& Berenberg-Gossler,
Frankfurt, Germany
Tel: +49 (0)69 971 300
E-mail: u.wuermeling@wessing.de

GREECE

Greece was one of the last EU-Member States to adopt data protection legislation but it has succeeded in implementing the EU Data Protection Directive well ahead of schedule. The Law 2472/97 is a comprehensive framework, establishing principles and rules irrespective of the sector (public or private) or the form in which data is processed.

The Greek data protection law established a system of universal notification, for example, *a posteriori* notification and prior notification in case of processing of "sensitive data" or interconnection of files with sensitive data. However, two recent modifications (Art. 8 Law 2819/15.03.2000, modified recently by Art. 34 Law 2915/01) introduced some exemptions from the obligation to notify in cases when:

a) the processing relates directly to an employment relationship,

b) the data processed relates to members of unions, organizations or persons with regular contacts with them,

c) the processing pertains to customer data or

d) the data is processed by health pro-

fessionals or lawyers who are subject to legal obligations of secrecy.

The Greek law entitles every person to exercise the rights of access, rectification, erasure, blocking and the right to object to the processing of his/her data.

Transfers of personal data to non-EU countries are subject to the criteria of adequate protection, as well as the derogations provided explicitly by law, and require a licence be granted by the Data Protection Authority. The Data Protection Authority is an independent oversight body, empowered to investigate, intervene, and make decisions. It can impose administrative sanctions and fines. Infringements of the data protection legislation entail also civil and penal liability.

The data protection framework has been supplemented by the Law 2774/99, which mainly reflects the provisions of Directive 97/66/EC. It contains specific rules, legal and technical requirements pertaining to the processing of personal data in the telecommunications sector.

Greece's modified Constitution, which came into force on April 17th 2001, enacts a new constitutional right to data protection. The new Article 9A refers to everyone's right to the protection of his/her personal data with regard to the collection, processing and use of these data, especially by automatic means. The Constitution provides that an independent authority shall guarantee compliance with these rules.

Dr. Lilian Mitrou
Advisor to the Prime Minister
Tel: +30 (0)1 6717071
Fax: +30 (0)1 724 1776
E-mail: l.mitrou@primeminister.gr

GUERNSEY

Guernsey passed its Data Protection (Bailiwick of Guernsey) Law on May 26th 1986, which came into force on November 11th 1987. It covers physical persons and automated data in the public and private sectors. Until recently, Guernsey had no Data Protection Registrar. The Advisory and Finance Committee oversaw the law with the assistance of a Data Protection Officer who combined the work with other responsibilities. On July 26th 2000, the law was amended by the Data Protection (Office of the Commissioner) Ordinance 2000. This established the office of an independent Data Protection Commissioner. Mr W C Bull was appointed to this Office.

The States of Guernsey also agreed to replace the existing law with the new Data Protection (Bailiwick of Guernsey) Law 2001, which is similar to the UK Data Protection Act, 1998. The law passed the States of Deliberation (the Guernsey Parliament) on November 28th. When it has received approval from the Islands of Alderney and Sark, it is anticipated that the law will come into effect in the spring of 2002.

W C Bull
Data Protection Commissioner
Tel: +44 (0)1481 717000
E-mail: Dpcommission@gov.gg

ICELAND

The purpose of the Act on Protection of Individuals with regard to the Processing of Personal Data, No. 77/2000, is to ensure the processing of personal data in conformity with the fundamental principles of data protection and the right to privacy, to ensure reliability and quality of such data, and the free flow of personal data within the European Economic Area. (The European Economic Area consists of the 15 member states of the European Union and Iceland, Liechtenstein and Norway). The Act, implementing the European Union Directive 95/46/EU, came into force on January 1st 2001, substituting for the 1981 Act Respecting Systematic Recording of Personal Data. The current Act applies to any automated processing of personal data and to manual processing of such data if it is, or is intended to become, part of a file.

A Regulation on Credit Reporting, N. 246/2001, was issued March 13th 2001 by the Ministry of Justice and came into force immediately. It aims to ensure proper processing and confidentiality, integrity and availability of credit information. The Regulation applies solely to processing aimed at distributing credit information. It is based on provisions in the Act on Protection of Individuals with regard to the processing of Personal Data.

The Freedom of Information Act, N.50/1996, came into force on January 1st 1997. Its aim is to ensure appropriate public access to documents held by the government. Major exemptions from this right of access include sensitive documents concerning national security, internal workings of government which do not contain the relevant cases' final results, and applications for government jobs.

The right to privacy is specifically protected in Art. 71 of the Constitution.

Horour H Helagson
Legal Counsel,
Icelandic Data Protection Authority
Tel: + 354 (0)510 9601
E-mail: Hordur@personuvernd.is

ISLE OF MAN

The Data Protection Act 1986 is based upon the now repealed UK 1984 Act. The Act aims to regulate the use of automatically processed information concerning living identifiable individuals and provision of services in respect of such information.

To achieve its aim, the Act sets down eight data protection principles:

Personal Data shall be: fairly and lawfully obtained and processed; held only for specified purpose(s); used and disclosed only for the purpose(s) registered; adequate, relevant and not excessive; accurate and up to date; kept no longer than necessary; available for access, correction and erasure by Data Subjects; and protected by appropriate security measures.

Exemptions

Exemptions apply when personal data are held/used for: personal, family, household affairs or recreational purposes; payroll and accounting, including the distribution or recording the distribution of items or services; for distributing articles or information; distributing or recording the distribution of articles or information to members of unincorporated members' clubs; the interests of national security; the prepa-

ration of the text of documents, and; when personal data is required by law to be made available to the public.

Criminal Offences include: non-registration by data users and computer bureaux, knowingly or recklessly operating outside the descriptions contained in register entries; failure to notify a change of address; procuring the disclosure of personal data and/or selling such procured data.

Sanctions

Where there has been or may be a breach of principle(s) the Registrar may issue: an Enforcement Notice; a De Registration notice; a Transfer Prohibition Notice overseas.

Failure to comply with an Enforcement or Transfer Prohibition Notice is a criminal offence. The Data Protection Tribunal hears appeals against the issue of such notices.

Data Subjects' rights

Data Subjects are entitled to: subject to limited exemption, to be supplied by any data user with a copy of personal data held about him; seek compensation through the courts if damage has been caused by inaccurate data or by the loss, unauthorised destruction or unauthorised disclosure of the personal data. If damage is proved, the court may also order compensation for any associated distress; apply to the courts for correction or deletion of the data where the personal data held is inaccurate.

The future

As the Isle of Man is neither a Member nor Associate Member of the European Union, it is not required to implement directives. However, in November 2001, the Data Protection Bill 2002 was published. It aims to update the legislation ensuring that it is compatible with the Directive 95/46/EC; ease the burdens placed on voluntary bodies and small businesses by the existing Act.

After the consultation period which ended on January 11th 2002, the proposed timetable is for the Bill to be introduced into the House of Keys in February, Royal Assent to be received by the end of May and the appointed day for the new law to enter into force to be September 1st 2002.

Lynn Keig
Isle of Man Data Protection Registrar
Tel: +44 (0)1624 661030
Fax: +44 (0)1624 661088
E-mail: odpr@odpr.gov.im

ITALY

Italy substantially ratified the EU Data Protection Directive 95/46/CE with Act n. 675/96 on the Protection of Individuals and Other Subjects with regards to the Processing of Personal Data. The Act took effect on May 8th 1997. Unlike the EU Directive, it protects both the individual and the legal person, private or public, and all information whether or not found in databases. This Act aims at guaranteeing the rights, basic freedoms and dignity of individuals, with particular attention given to privacy and personal identity.

The following legislative decrees have been adopted: 51/99 establishing the Data Protection Authority; 135/99 authorising the processing of sensitive data in certain situations; 281/99 on processing historical, statistical and scientific data, and 318/99 on minimum security measures applying to the processing of personal data.

The Act provides for liability for damages resulting from the processing of personal data. Article 18 deems improper processing of personal data to be a 'dangerous activity', set out in art. 2050 of the Civil Code, which brings about a shifting of the burden of proof from the data subject to the processor of personal data. Moreover, this Act provides for various offences punishable by up to three years imprisonment. Those crimes stipulated by Act 675/96 are: failure to notify the Commissioner or incorrect notification (art. 34); unlawful processing of personal data (art. 35); failure to adopt measures required for data security (art. 36), and failure to comply with measures taken by the Commissioner (art. 37).

Data protection clauses in other legislation

Spamming is dealt with in art. 10 of the D.Legs. n. 11/98 (implementing the EU Directive 97/66/CE), which protects privacy in the telecommunications sector. The practice is subject to the express consent of the data subject. Internet users' privacy is protected by Act 675/96, ratifying the EU Directive 95/46/CE, and by the D.Legs. n. 171/98 ratifying the EU Directive 97/66/CE.

E-mail legislation is found in the criminal code and Act n.305/93 which modifies art. 616 of the code. The code extends the offence of breach, theft and suppression of mail to include electronic mail and mail via telecommunications. It also introduced art. 617-quarter, which punishes illegal interception, hindrance or interruption of electronic mail or telecommunications.

D.Legs n.518/92 (implementing the EU Directive 91/250/CE) includes software amongst the works protected by copyright. However, for the first time, Act 547/93 has introduced several computer crimes, such as illegal computer or telecommunications access (art. 615-ter c.p.), illegal possession and diffusion of access codes (art. 615-quarter c.p) and computer fraud (art. 640-ter c.p).

The principal legislative source on e-commerce is art.42 of Act n.428/90 that regulates contracts completed outside the commercial premises, articles 1, (d) and 9 of D.Legs. n.50/92 (implementing the EU Directive n.85/577/CEE) and D.Legs. n.185/99 (ratifying the EU Directive 97/7/CE).

In the Italian judicial system, it is necessary to distinguish between the right of access to administrative documents (art. 22, Act n.241/90) from the right of access to the Register of the Commissioner and data processed by the Controller (art. 13, Act n.675/96).

Constitutional protection

The right of privacy is not expressly set out in the Constitution but is referred to in art.2. However, Act 675/96, speaks for the first time expressly of the right to privacy. This right is protected by criminal sanctions in certain provisions, such as art. 615 bis c.p, which establishes the offence

of illegal interference in privacy, and art. 614 c.p punishes trespassing.

Riccardo Imperiali
Gruppo Imperiali,
Naples, Italy
Tel: +39 02 58430905
Fax: +39 02 58430778
E-mail: riccardo.imperiali @imperiali.com

JAPAN

Data Protection law

Japan has privacy legislation in the public sector. The Act on Protection of Computer Processed Personal Data held by Administrative Organs was enacted on December 16th 1988 and came into force in stages from October 1st 1989 to October 1st 1990. The Act covers automated data in national government departments. It is based on several data protection principles, but contains a number of exceptions.

In March 1997 the Ministry of International Trade and Industry (MITI) issued guidelines for data processing in the private sector. The guidelines are based on the OECD Guidelines and the Council of Europe Convention number 108. A supervisory authority was established in February 1998 under MITI to monitor the adoption of the guidelines and the system of privacy protection marks.

Bilateral talks have started with the EU with regard to transborder flows and adequacy.

In July 1999, after some years of discussion, a working party was set up to consider how best to draft a comprehensive law. This led to a Bill in March 2001, but discussion of it was delayed. At late-January 2002, it is expected that the Bill will be debated and passed in the session of the National Diet (legislature) which started on 21st January 2002.

The Bill was drafted to apply mostly to the private sector, though it lays down general principles applicable to all areas. There are some provisions relating to personal data held by local authorities; only about half of them have their own ordinances on data protection. There is also provision for legal and other measures affecting administrative agencies, whether state-owned or not. Transborder exchanges are not covered.

The Bill complements rather than replaces the 1988 Act affecting national government, and is intended to form a basis for sectoral legislation in sensitive areas. It does not apply to news media, academic and research organisations, or religious or political organisations holding personal data for certain purposes. These organisations are expected to put in place their own systems of self-regulation. The Bill also requires the Prime Minister to consult with the Social Policy Council and put to the Cabinet a basic policy for the comprehensive and integrated promotion of measures.

The idea of a national supervisory authority was rejected. Instead, infringements and complaints are to be dealt with by whichever government minister is deemed to be responsible for the sector in question. The minister may issue instructions or legally enforceable orders, punishable by imprisonment or a fine in cases of non-compliance. Certified bodies may be set up to handle complaints for a group of data-handling organisations, but ministers will have the power to revoke certification in the event of a dispute.

Freedom of Information law

Japan adopted a Freedom of Information Act on 7th May 1999. It entered into force in April 2001.

Dr. Michael Spencer,
based on a report by
Professor Masao Horibe, Tokyo
E-mail: mhoribe@tamacc.chuo-u.ac.jp, mikespen@gn.apc.org

LATVIA

On October 31st 2000, Latvia acceded to the Council of Europe Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data. The provisions entered into force in Latvia on September 1st 2001. As well, in 1992, Latvia acceded to the International Covenant on Civil and Political Rights. It also signed (1995) and ratified (1997) the Convention for the Protection of Human Rights and Fundamental Freedoms.

On January 1st 2001, Latvia's Law on the Registration and Protection of Personal Data Processing Systems entered into force.

The new Law generally applies to the processing of all types of personal data, and to any natural and legal person involved in personal data processing. However, it does not extend to information systems made by natural persons for personal or household and family purposes and the personal data are not disclosed to other persons.

The Law also does not apply to the processing of personal data carried out by public institutions in the fields of national security and criminal law. Instead, the protection of personal data declared to be official secret matters falls under the Law on Official Secrets. Personal data processed for journalistic, artistic or literary purposes are covered by the Law, but certain of the general principles for personal data processing set out in Chapter II of the Law do not apply.

The State Data Inspection Authority is responsible for the protection of personal data. This body is subject to the supervision of the Ministry of Justice. The Authority's Director is appointed and can be dismissed from the position by the Cabinet on the recommendation of the Minister for Justice.

The State Data Inspection Authority is charged with making decisions and reviewing complaints regarding protection of personal data. It has the power to inspect personal data processing systems before their registration, order that data be blocked, or that incorrect or unlawfully obtained data be erased or destroyed, or order a permanent or temporary prohibition of data processing. The State Data Protection Authority may bring an action in court for violations of the Law. Decisions of the Authority may also be appealed to the courts. Access to the courts provides another independent mechanism for ensuring compliance with the Law.

The Law provides the State Data Inspection Authority with specific investigative powers, such as the authority to enter non-residential premises, and to require explanations and the production of documents. The Law also gives persons the right to receive com-

mensurate compensation if they suffered harm or losses from a violation of the Personal Data Protection Law.

The European Commission is now analysing the Latvian legislation to see if it meets the "adequacy" requirements of Article 25 of the EU Data Protection Directive.

Eugene Oscapella
E-mail: eugene@privacylaws.com

LITHUANIA

Privacy and Data Protection

Article 22 of the Constitution of the Republic of Lithuania confers a right to privacy:

"The private life of an individual shall be inviolable. Personal correspondence, telephone conversations, telegraph messages, and other intercommunications shall be inviolable. Information concerning the private life of an individual may be collected only upon a justified court order and in accordance with the law. The law and the court shall protect individuals from arbitrary or unlawful interference in their private or family life, and from encroachment upon their honour and dignity."

Lithuania adopted a law on the Legal Protection of Personal Data in 1996 and amended it in 1998. Following the EU Data Protection Directive 95/46/EC, the new version of the Law on Legal Protection of Personal Data was adopted in 2000.

On February 20th 2001, the Seimas (legislature) ratified the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS 108). In the third quarter of 2001, the Government nominated an institution to implement the provisions of Convention ETS 108. The State Data Protection Inspectorate (SDPI) provides extended powers to assist data subjects resident abroad, as well as provide information on administrative practice.

Aligning the Law on Legal Protection of Personal Data with Directive 95/46/EC effected the exceptions allowed by part 2 of Article 3 of the Directive. Therefore, the Law provides that it shall not apply for the purposes of state security, defence and operational activities, nor when co-operating with the EU Member States in fields of justice and home affairs. Ratification of Convention ETS 108 is expected to extend the scope of application of the Law on Legal Protection of Personal Data.

The Administrative Code was supplemented with regulations on unlawful processing of personal data in 1998. The law also defines monetary penalties; for example:

• illegal processing of personal data will incur a penalty of from 500 to 2000 Litas (approximately $125 to $500 or 142 Euros to 568 Euros)

• preventing a person from accessing his/her personal data in an information system or from obtaining information about sources of this data, will incur a penalty of from 100 to 200 Litas ($25 to $50 or 28 Euros to 57 Euros).

The law granted the State Data Protection Inspectorate the right to issue protocols for violations of the Administrative Code and impose penalties from 100 to 200 Litas for failure to execute Inspectorate instructions or for preventing the Inspectorate from checking data processing.

The new Civil Code, which came in force on July 1st 2001, has been supplemented with regulations on a right to privacy and secrecy of private life. The Penal Code was supplemented with subsequent regulations on illegal collection, disclosure or use of information.

Freedom of Information

Regulations on co-ordination of personal data processing with rights to public information are provided for in the Law on Legal Protection of Personal Data. However, the main legal acts on Freedom of Information are the Law on Provision of Information to the Public, and the Law on the Right to receive the Information from State and Municipal Institutions.

Andrew Visockis
Chief Reviewer, State Data Protection Inspectorate
Lithuania
Tel: +370 (0)2 22 75 32
Fax: +370 (0)2 61 9494

THE NETHERLANDS

The new Dutch Data Protection Act of July 6th 2000 entered into force on September 1st 2001. This law implements the European Union Data Protection Directive 95/46/EC into Dutch law.

This new law replaces the Act of December 27th 1988 but there is considerable continuity from one Act to the other. A number of differences deserve highlighting.

The scope of application is now defined in the same terms as the European Directive. While the previous law applied to the so-called "registration of persons", with an emphasis on keeping files concerning several persons, the new Act refers to "processing", defined as in article 2 of the Directive.

The new law makes no difference between public sector and private sector processing operations in general terms.

Transparency becomes the cornerstone of the law. In particular, the Act emphasises the need to provide adequate and timely information to data subjects so that they can make informed decisions concerning their own personal data.

A new right to oppose processing is defined in the same terms as in the Directive.

The new Act contains a whole chapter dealing with the issue of transborder data flows to countries outside the European Union. In principle, data may be sent only to countries with an adequate level of protection, or when one of the exceptions enumerated in the Act applies. The Minister of Justice may, on the advice of the Data Protection Authority, grant a permit for a specific transfer or set of transfers if the controller adduces sufficient guarantees. This can be done, in particular, through contractual clauses.

The new Act renames the Dutch Data Protection Authority the College Bescherming Persoonsgegevens (formerly Registratiekamer) and provides it with new authority. In particular, and in addition to the penal provisions contained in the Act, the DPA gains new powers concerning sanctions and may impose fines or administrative measures of constraint in some cases. The Dutch DPA has no jurisdiction concerning freedom of information issues.

Constitutional data protection

Article 10 of the Dutch Constitution of 1989 grants all citizens an explicit right to privacy and states that rules concerning the protection of this right will be laid down by an Act of Parliament. Article 13 of the Constitution deals with the right of the privacy of correspondence, telephone and telegraph.

Data protection clauses in other laws

The most relevant piece of legislation containing sectoral rules on this issue is the Telecommunications Act of October 19, 1998 . This law partly implements Directive 97/66/EC into Dutch law but a number of issues remain to be dealt with in secondary legislation.

Other relevant pieces of legislation are the law on police files of 1990, the law on the stimulation of employment of minorities of 1994, the law on medical examinations of 1997, the Medical Treatment Act of 1997 and the law on the social security system of 1997.

Diana Alonso Blas, LL.M.
Senior International Officer
Dutch Data Protection Authority

NEW ZEALAND

New Zealand's Privacy Act 1993 entered into force on July 1st 1993. The Act repealed and consolidated the Privacy Commissioner Act 1991 and included comprehensive new provisions.

The Act applies to both public and private sector agencies and all personal information, in whatever form it is held. In December 1998 the Privacy Commissioner completed a review of the 1993 Act, required by the Act every five years. Some of the Commissioner's 150 recommendations address issues raised by the EU Data Protection Directive. Two resulting amendments were introduced to Parliament in December 2000 to help secure a finding of "adequacy".

The European Commission has not yet decided whether it regards the New Zealand law as providing adequate protection for personal data in transborder data flows.

Blair Stewart
Assistant Commissioner,
Office of the Privacy Commissioner,
New Zealand
Tel: +64 (0)9 302 8654
Fax: +64 (0)9 302 2305
E-mail: Blair.Stewart@privacy.org.nz
BlairStewart@compuserve.com (laptop)
www.privacy.org.nz

NORWAY

Norway's principal piece of data protection legislation is the Personal Data Act 1999 (lov om behandling av personopplysninger av 14 april 1999 nr 31), in force as of January 1st 2001. This replaces the Personal Data Registers Act 1978 (lov om personregistre mm av 9 juni 1978 nr 48).

The Personal Data Act follows closely the provisions of the 1995 EC Data Protection Directive, which has been incorporated into the 1992 Agreement on the European Economic Area (to which Norway is a party).

The formal aim of the Act is to safeguard the privacy and integrity of data subjects and to ensure adequate 'quality' of personal data.

Unlike the previous legislation, the Act dispenses completely with express protection for data on corporations and other legal/juristic persons. However, provision is made for protection of such data to be introduced in the future with respect to credit-reporting activities.

Most data-processing operations must be reported to the Data Inspectorate. Non-automated data registers are exempted from this requirement, unless they contain especially sensitive data.

The Act also requires licensing prior to the processing of especially sensitive data, unless:

- the data subject voluntarily supplies the data; or
- the processing is carried out by a government agency pursuant to statutory authorisation; or
- the processing consists of television surveillance for the purposes of crime control.

The Data Inspectorate is empowered to determine, on a case-by-case basis, whether other data-processing operations require licensing when they obviously infringe weighty data protection interests.

The Act goes further than the Directive in three significant respects. First, data subjects must always express not imply consent (also for processing non-sensitive data). Secondly, data subjects must automatically be informed of certain profiling practices. Thirdly, the Act includes rules dealing specifically with closed circuit television surveillance.

A variety of sanctions and remedies are stipulated for breach of the Act. In a departure from the 1978 legislation, the Data Inspectorate may impose ongoing enforcement damages during the period when a data controller fails to comply with the Inspectorate's orders. Also new is the power to award compensation for purely non-economic injury. Strict objective liability for damages is stipulated for harm caused by credit-reporting agencies.

Data protection clauses in other legislation

Clauses concerning data protection are scattered across the Norwegian statute books. Many significant examples are to be found in the Criminal Code 1902 (almindelig borgerlig straffelov 22 mai 1902 nr 10); for example, see section 390 which punishes violation of 'privacy' caused by 'public disclosure of information relating to personal or domestic affairs'.

Independently of statute law, Norwegian courts have developed a general protection of personality on a case-by-case basis. A major dimension of this case law has involved privacy/data protection (such as in relation to covert video surveillance).

Freedom of Information legislation
The principal piece of such legislation is the Freedom of Information Act 1970 (lov om offentlighet i forvaltningen av 19 juni 1970 nr 69) which provides citizens with a general right of access to government-held information.

Constitutional protection
The Norwegian Constitution (Grunnlov) of 1814 lacks a provision dealing specifically with the protection of privacy or personal data. The closest to such a provision is section 102, which prohibits searches of private homes, except in cases of criminal investigation.

Dr. Lee A. Bygrave,
Norwegian Research Centre
for Computers and Law,
PO Box 6706,
St Olave Plass,
Oslo N 01300, Norway
E-mail l.a.bygrave@jus.uio.no

PERU

Peru enacted a sectoral data protection law in June 2001 which came into effect in August 2001 (Law No. 27489). It regulates credit reporting databases.

Privacy is also covered in Article 2 of the Constitution and Peru has a law (no. 26301) which implements this provision. Recently there has been a data protection bill (no. 5,233) entitled Sobre la Privacidad

Law 27489 has 23 articles and includes the following features:

• it regulates the incorporation of credit bureaus and qualifications to be a shareholder of one of these companies,

• it defines what sources of information they can use (public sources or from creditors) without the consent of the individual,

• it establishes what information must be provided where the data has not been obtained from the data subject (similar to art. 11 of EU Directive); and

• it sets out a set of data protection principles.

The Law protects both individuals and companies whose information is recorded in databases.

In addition, the Law prohibits credit bureaus from collecting:

• sensitive information,

• data violating the confidentiality of bank or tax records,

• inaccurate or outdated information,

• bankruptcy records older than five years,

• other debtor records five years after the debt was paid.

Credit bureaus must adopt security measures.

Individuals' rights include:

• access to information,

• the right to modify or cancel their personal data.

The law also creates strict liability for damages. The Government Agency for Consumer Protection is in charge of applying fines for violation of the law and issuing injunctions to correct errors.

Pablo Palazzi
E-mail: Palazzi@fordham.edu

SPAIN PART 1

The protection of personal data is regulated by Organic Law 15/1999, December 13, on the Protection of Personal Data (hereinafter, the Law) which implements the EU Directive 95/46/EC.

1 Principles

1.1 Scope of the Law
The Law affects all kinds of personal data regardless of how it is stored. It includes in its scope the processing and subsequent use of personal data registered in a physical form and whether or not treated by automatic means.

In Spain, privacy is a constitutional right. The Spanish Constitution rules that law shall limit the use of information to guarantee personal privacy and honour of individuals, and the full exercise of their rights.

1.2 Data Quality
The Law provides that personal data must be accurate, up to date and not kept for a period longer than necessary for the purposes for which it was collected.

1.3 Information rights
The Data Controller must inform the individuals, to whom the data relates, of the purposes for which the data is intended to be processed as well as any other relevant details, such as information as to whether individuals will be contacted for marketing purposes, and the potential recipients of the data.

1.4 Consent
The processing of personal data requires the unequivocal consent of the data subject. There are certain exceptions to this general principle, for example, where it is provided by law.

1.5 Sensitive Data
Spain's Constitution declares that no-one can be forced to provide information on his ideology, religion or beliefs. Therefore, the processing of sensitive data in databases is subject to strict rules.

1.6 Rights of access, rectification and cancellation
A number of rights allow individuals to exercise a certain degree of control over the way their data is used and, therefore, the users of the data must be prepared to honour those rights. Data subjects may not be charged for exercising such rights.

2. Registration
The controller or his representative must provide prior notification of any processing of data to the Spanish Data Protection Agency.

3. Security
Spanish Data Protection Law requires the data controller to adopt appropriate security measures. The Royal Decree on Security Measures for Databases establishes different levels of security (basic, medium and high), which have to be observed depending on the type of information processed.

Those technical and organisational measures must protect the personal data against any unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular, when the processing of the data involves its transmission over a network.

The Law also establishes a requirement for data controllers to ensure that where a third party processes data on behalf of the data controller, a written contract is set in place between the parties whereby the data processor agrees to act only on the instructions of the data controller and to adopt appropriate security measures.

4. International data transfers
Personal data must not be transferred to countries or territories outside the EEA that do not provide an adequate level of data protection. However, this prohibition can be overridden by obtaining individuals' consent or under other specific circumstances.

5. Sanctions
The controllers of the files and the persons in charge of the processing are subject to the system of sanctions established by this law. Infringements of the Data Protection legislation may be punished with fines up to EUR. 601,000 (£372,620) plus deletion of the infringing database.

Gabriel Nadal / J.M. Pérez
Protección de Datos –
Jausas Nadal & Vidal
E-mail: Gnadal@safenetsolutions.com

SPAIN PART 2

Another correspondent, Genoveva Goetsch, provides the following additional information.

The aim of this Law, in force since December 14th 1999, is to protect and guarantee the public freedoms and fundamental rights of individuals, especially their right to dignity and privacy in the field of data processing.

The Statute applies to both public and private processing containing personal data. Moreover, it applies to personal data stored in both manual records and in computer files.

Territorial scope
Regarding territorial scope, the Law governs the following activities:

1. data processing activities where the data controller has its business established in Spanish territory.

2. data processing activities where the data controller is not established in Spanish territory but according to international law, Spanish law applies.

3. data processing activities where the data controller is not established in the EU but uses means which are located in Spanish territory, unless they are used with a transitory purpose.

Exceptions
The exceptions to the law are: files kept by individuals for their exclusive personal or domestic use; files under the scope of classified materials regulations (the electoral regime regulated by the statutory instruments LO 5/85 and LO13/94; data used for statistical purposes according to the public statistical function law L12/89 or further local legislation; data relating to the armed forces, personnel regimes, central registry of criminal convicts, data on images and sounds recorded by video cameras belonging to the forces and security bodies according to their specific legislation) and; files created to investigate terrorist related activities and other organised criminal behaviour. Nevertheless, in these cases, the data controller must previously communicate the existence of the file, aim and main features to the Data Protection Agency (APD).

Other privacy-related laws
1. Organic Law 17/82 granting protection of the fundamental rights to dignity and privacy.

2. The Criminal Code, Article 197.1, establishes that any interception of personal communications (including e-mail) with a view to violating an individual's privacy is considered a criminal offence.

3. Database Law 5/88, in line with the provisions under EU Directive 9/96 on databases.

Constitutional Right to Privacy
A fundamental right to privacy is provided under Title I of the Spanish Constitution (CE) in Article 18. According to Article 18.4, the law will limit the use of computers so that the citizens' dignity, privacy, and full exercise of their rights are guaranteed. This protection applies only to Spanish citizens. Protection of foreigners is given by virtue of international or bilateral treaties.

The constitutional relevance is reinforced in article 20.4 CE. This article provides that the rights of freedom of expression and information are limited under the provisions established under Title I, especially the right to dignity, and the right to privacy.

Genoveva Goetsch
E-mail: uctlggo@ucl.ac.uk

SWEDEN

Data Protection law
The Personal Data Act (1998:204) entered into force on October 24th 1998. The Act replaced the Swedish Data Act of 1973 and implements the EU Data Protection Directive 95/46.

Section 1 of the Personal Data Act defines the purpose as protecting people against the violation of their personal integrity caused by processing of personal data. Further provisions are given in the Personal Data Ordinance (1998:1191) which came into force at the same time as the Act. Since October 1st, 2001, the new law has applied to all data processing.

The Personal Data Act applies to processing of personal data that is wholly or partly automated. It also applies to other processing of personal data if the data is included in, or intended to form part of a structured collection of personal data available for

searching according to specific criteria.

Processing of personal data during purely private activities is exempted from the Act. Provisions in other statutes or enactments that deviate from the Act shall apply instead. Furthermore, the Act does not apply if it would contravene the constitutional provisions concerning the freedom of the press and freedom of expression. Nor does the Act apply to processing of personal data carried out exclusively for journalistic purposes or artistic or literary expression—except for the security provisions. Finally, the Act does not apply when it would limit an authority's obligation to provide personal data under the principle of public access to official documents in Chapter 2 of the Freedom of Press Act.

Violation of certain provisions in the Personal Data Act is punishable with a fine or imprisonment of at most six months (or two years if the offence is grave).

Other data protection provisions

There are several Swedish Acts and Ordinances containing specific provisions for certain sectors, for example, the Act on Medical Data Records (1998:543), the Act on Health Care Records (1998:544) and the Police Data Act (1998:622).

Freedom of Information legislation

The Instrument of Government (chapter 2, article 1, adopted 1974) states that all citizens shall be guaranteed freedom of information, that is, the freedom to obtain and receive information and otherwise acquaint oneself with the statements of others in their relations with the public administration. This freedom may be restricted in law in circumstances when it can affect the integrity of the individual and the sanctity of private life.

Constitutional right to privacy

The Instrument of Government (chapter 2, article 3, para. 2) states that citizens shall be protected to the extent determined in detail by law against any infringement of their personal integrity resulting from the registration of information about them by means of electronic data processing.

Elisabeth Wallin
International Secretary,
The Data Inspection Board,
Sweden
E-mail: elisabeth.wallin@datainspektionen.se

SWITZERLAND

Federal Data Protection Law

The principal goals of the Law are the protection of privacy and fundamental rights of persons about whom data is processed. This law has been in force since July 1st 1993, and is accompanied by the Ordinance on the Federal Law on Data Protection. The Law applies to the processing of personal data by both the public and private sectors, covering both automated and manually processed data. The Law protects not only personal information on individuals, but extends the protection to legal persons as well.

The Law does not apply to personal data that is processed by a natural person exclusively for personal use and is not disclosed to third parties. Also exempt are the deliberations of the Federal Parliament and Parliamentary Committees as well as pending civil suits, criminal proceedings, international judicial assistance proceedings, as well as constitutional and administrative proceedings (with the exception of administrative proceedings of the first instance). Public registers based upon private law are also excluded (but covered by separate regulations), as is personal data processed by the International Committee of the Red Cross.

The Law provides individuals with a right of access to their data. Should private bodies breach certain duties regarding individuals' right of access, they shall (upon request) be imprisoned or fined. Furthermore, private bodies shall be sanctioned when infringing their duties concerning registration of data files with the Federal Data Protection Commissioner. They must also be sanctioned if they provide false information or refuse to cooperate with the Data Protection Commissioner in his/her legally prescribed investigations. Whoever breaches the duty of professional secrecy will also be punished.

Revision of Federal Law on Data Protection:

One of the main objectives of this "small" revision is to increase transparency during data collection, particularly when sensitive data and personality profiles are being collected. The revision also allows administrative bodies to test access to databases during the trial phase of a project, in particular when dealing with on-line access. The revision also aims to provide adequate level of protection for federal data while being processed by cantonal or communal authorities. The schedule for enacting the revisions has not yet been determined.

Data protection provisions in other laws

Among other legislation, data protection clauses can be found in labour law, the Federal Law on International Private Law, the Federal Law on Radio and Television, the Federal Law on Aviation, the Federal Ordinance on Recruitment Agency Services, and the Federal Law on Money Laundering.

Federal Act on Freedom of Information

With some exceptions, actions of administrative authorities are generally secret in Switzerland. The draft Freedom of Information Bill (Bundesgesetz über die Öffentlichkeit der Verwaltung) reverses the principle of secrecy by granting the right to access to official documents to everyone. This right shall be granted without the need to demonstrate any special interest in the claimed information. The administration is currently preparing the legislation, after which it will be reviewed by parliament. The implementation schedule is still open.

The legislation will apply both to the federal administration and to organizations and persons of private and public law that do not belong to the federal administration but execute public duties. The draft bill treats as a public document any information that is recorded, on any information carrier

and in any format, and is held by an official body that has either produced the information or received it during the execution of public duties. However, the right to access official documents will be restricted, postponed, or denied if preponderant public or private interests are opposed.

Constitutional right

The Swiss Constitution provides for a right to privacy in Article 13, which reads: "All persons have the right to receive respect for their privacy and family life, home, and secrecy of their mail and telecommunications. All persons have the right to be protected against the abuse of personal data."

The Commission of the European Communities decided on July 26th 2000 that the Swiss data protection legislation is adequate under the EU law. On the other hand, Switzerland has not recognized that the EU has an adequate standard of data protection.

Urs Maurer
Maurer Law Offices,
Zollikerstrasse 20,
CH-8032 Zurich,
Telephone: +41 (0)1 385 99 11
Fax: +41 (0)1 385 99 22
www.swisslawfirm.com
www.neweconomylawfirm.com

TAIWAN

Currently, there is no general legislation to protect personal data in Taiwan although Article 12 of the Taiwanese Constitution reads "that the people shall have freedom of privacy of correspondence" and the newly revised Civil Law Code protects the right of privacy explicitly.

To meet the privacy protection challenges of the computer age, the Computer-Processed Personal Data Protection Law was enacted in August 1995. This legislation regulates the collection and use of personally identifiable information by government agencies and various sectors of private business. First, the law requires that "The collection or utilization of personal data shall respect the rights and interests of the principal and such personal data shall be handled in accordance with the principles of honesty and credibility so as not to exceed the scope of the specific purpose."

To ensure informed consent and data quality, this legislation also provides individuals with rights of access and correction, and the ability to ask to stop computerized processing and use, and to have data deleted. Damages can be assessed for violations of the law. Finally, the legislation specifically identifies eight categories of organizations and businesses as regulated industries; credit information organizations, hospitals, schools, the mass media and the telecommunications, financial, securities and insurance industries. Both the Ministry of Justice and the central government authorities in charge of regulating industry may designate other enterprises, organizations, or individuals.

However, the law permits retrieval and access to electronic personal data without the individual's consent when there are broad "public interest" and "national security" concerns. As more and more incidents about the privacy of online transactions have dominated the front pages of local papers, the Ministry of Justice is now working on a revised version of the Computer-Processed Personal Data Protection Law and will send the draft to the Legislative Yuan for consideration after its completion.

The Legislative Yuan of Taiwan passed the Communication Protection and Surveillance Act in June 1999. The legislation replaces the martial law-era Telecommunications Surveillance Act. This legislation aims at imposing stricter regulation on the use of wiretaps although they can still be approved for broad reasons such as "national security" and "social order." It is particularly noticeable that the law requires telecommunications providers to assist law enforcement bodies and sets technical requirements for interception. In May 2000, the Ministry of Justice proposed that all banks link their customer databases to a central database at the Ministry of Finance. The proposal was opposed by the Ministry of Finance and has never been adopted.

Freedom of Information law

Finally, the Legislative Yuan passed the Administrative Procedure Act in February 1999. This Act contains a section for provisions that protect freedom of information. Before more general legislation protecting freedom of information is introduced, these provisions are the only ones that regulate when and how information held by executive agencies can be requested.

Ching-Yi Liu
Assistant Professor of Law,
National Central University, Taiwan
E-mail: Tgcn143@attglobal.net

THAILAND

The new Thai Prime Minister, Mr. Thaksin Shinnawatra, leading the cabinet from March 2001, appointed Mr Krasae Chanawong, Minister to the Prime Minister's Office, as a new chairperson of the Official Information Commission.

The Official Information Act 1997 is the only Act that guarantees freedom of information and privacy protection. According to the 2000 report approved by the Official Information Commission (OIC), there were 164 complaints that year, compared with 122 in 1999, an increase of 34%. The majority of the cases are complaints about public authorities not providing requested information. These can be categorised into complaints against: Local government (municipality, provincial authorities etc.) – 34 cases ; Ministry of Education – 21; Ministry of Finance – 16; Ministry of Agriculture and Cooperatives – 13; Prime Minister's Office – 12; Ministry of Communication – 11; Ministry of Interior – 11, and; Ministry of University Affairs – 10.

Requesters are mainly public servants and civil service employees (45.12%), private citizens (25%), business persons (20.12%), mass media and reporters (4.88%) and NGOs (2.44%).

There were 83 appeal cases in 2000, 74 of which were resolved.

The complaints cited civil servant discipline process - abuse of power, misconduct, unethical conduct (10%), public procurement (construction pro-

curement) (10%), bad debt and non-performing loan restructuring procedures of banking and financial institutions (10%). Organisations complained against can be categorised into Ministry of Agriculture (13%), Ministry of Finance (12%), Prime Minister's Office (10 %) and Ministry of Education (8%). The appellants include public servants (44.58%), business persons (28.92%), private citizens (15.66%), mass media (3.61%0 and NGOs (2.41%).

Data protection provisions in other laws

Besides the Official Information Act 1997, there are privacy protection provisions in the administrative law and the penal code. The data protection law proposed by the Ministry of Science, Technology and Environment, is still being drafted by an ad hoc committee and waiting to be submitted to cabinet for consideration. The Electronic Transactions Bill and Electronic Signatures Bill are mixed in with the Electronic Transactions Bill proposed by the Ministry of Science. All are awaiting Upper House consideration as is the Fair Credit Reporting Bill, proposed by the Ministry of Finance. A computer crime law, electronic fund transfers law and national information infrastructure law are in the drafting stages.

Niti Wirudchawong
Senior Legal Official,
Legal Affair Section,
The Office of the Official Information Commission,
Thailand
E-mail: niti@oic.thaigov.go.th

UKRAINE

When independence was proclaimed ten years ago, Ukrainians had no legal tradition of protecting private life from state interference and no notion of "privacy" in their domestic legal vocabulary.

The first information law of the Ukrainian Parliament was that of October 2nd 1992. This law laid the groundwork for further developments in information law. The law contains several articles on personal data protection. Among them, the law guarantees access at no cost to personal data held by public bodies. It also gives the right to challenge the unlawful refusal of access or the unlawful hiding, collection, use or dissemination of personal data.

The 1992 law classifies information as publicly available or restricted. Restricted information is divided into two categories: confidential and secret. Confidential information is that owned by physical and legal persons and disseminated by them at their discretion. State secrets and other secrets protected by law are treated as "secret data."

Several other pieces of legislation protect data in specific situations. The April 23rd 1991 law on freedom of conscience and religious organizations guarantees "secrecy of confession."

A law dated December 19th 1992 protects legal confidences, meaning issues raised by a citizen or legal person with an advocate, the contents of the consultation and other data received by the advocate when acting in a professional capacity.

Health protection legislation dated November 19th 1992 governs medical confidentiality. Medical personnel and others who in their work obtain data concerning disease, medical examinations and results, as well as the intimate family life of a citizen, have no right to disseminate the data unless the law states otherwise.

Article 32 of the Ukrainian Constitution, adopted on June 28th 1996, states: "The collection, storage, use and dissemination of confidential information about a person without his or her consent shall not be permitted, except in cases determined by law, and only in the interests of national security, economic welfare and human rights. Every citizen has the right to examine information about himself or herself, that is not a state secret or other secret protected by law, at the bodies of state power, bodies of local self-government, institutions and organizations..."

To enhance the protection of personal data and to bring domestic law into accord with the Council of Europe Convention 108 and the EU Data Protection Directive, draft legislation on personal data was introduced in the Ukrainian Parliament in May 2001. The draft is based on the prevailing approach of European countries to the protection of personal data adopted.

Adapted by Eugene Oscapella from a report, "From Secrecy to Privacy: The Task of Changing the Legal Framework of Personal Data Privacy in Ukraine," by Andriy Pazyuk, NGO Privacy Ukraine. E-mail: privacy@ukrnet.net.

UNITED KINGDOM

Freedom of Information

In November 2000, the UK's first Freedom of Information Act was passed, and on 30th January 2001 the Data Protection Commissioner assumed responsibility for implementing both measures under her new title of Information Commissioner. The Act gives a general rights of access to all types of "recorded" information held by some 50,000 public authorities and places a number of obligations on them. There are 23 exemptions comprising class exemptions (such as investigations and proceedings by public authorities), exemptions subject to a test of prejudice to the activity or interest concerned, and cases such as law enforcement or those affecting the interests of the UK abroad. Requests for personal data relating to the applicant will continue to be treated under the rules of the Data Protection Act 1998.

The Act has to be fully in force by the end of November 2005. It was originally expected to be applied to public authorities in stages, starting with Government departments in 2002 and adding other categories in subsequent years. However, in November 2001 the Government announced that the right to request information under the Act from any authority would be delayed until January 2005. Meanwhile, public authorities would undertake a staged introduction of approved "publication schemes" which set out classes of information published by an authority, the manner of its publication, and details of any charges.

Data Protection

The Data Protection Act 1998 covers

both manual and automated data, but there were two transitional periods for its retrospective application to existing manual records. The first of these expired on 23 October 2001, and subject access rights now apply to all the categories of manual data covered by the Act. A second transitional period will exempt a few classes of data from certain other aspects of the Act until 23 October 2007. The Information Commissioner has issued a new legal guidance manual which deals with this complex subject.

Telecommunications are subject to separate Regulations. On 1st March 2000 the revised Telecommunications (Data Protection and Privacy) Regulations 1999 came into force. These regulations implement the EU's directive 97/66/EC on the protection of privacy in telecommunications. They guarantee users the ability to withhold calling or called line identification without charge, subject to limited exemptions; give a right to be excluded from public directories, or to have the entry limited in content; provide for protection against unsolicited direct marketing calls and faxes; and strictly restrict the retention of traffic data. This last provision has, however, been undermined by more recent legislation (see below).

In October 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 entered into force. These regulations authorise businesses to monitor or record communications on their telecommunication systems without consent for limited purposes relating to business transactions, compliance with regulatory or self-regulatory practices, quality control and staff training, crime prevention or detection, unauthorised use of systems, and monitoring effective technical operation of the system.

The Lawful Business Practice Regulations were made under the Regulation of Investigatory Powers Act 2000, a wide-ranging measure which (when fully in force) will introduce or extend law-enforcement powers to cover the acquisition of "communications data" (traffic data and anything else except the contents), covert surveillance, the monitoring of internet traffic through service providers, and the power to demand encryption keys.

The powers regarding traffic data are, however, overtaken by provisions in the Anti-Terrorism, Crime and Security Act 2001 which received Royal Assent in December 2001. Part 11 of the Act provides that communications data may have to be retained for an extended period (possibly 12 months) in case it is needed for any purpose connected with national security or crime. The details will be clarified in a Retention of Communications Code of Practice which had not yet been issued by mid-January 2002. The Act also removes statutory restrictions on disclosure affecting numerous public authorities, wherever the information is needed for such purposes.

In a period of recurrent controversy over new powers for law-enforcement authorities, the Criminal Justice and Police Act 2001 was also passed to give additional powers of seizure that would cover computers suspected of containing illegal material. This wide-ranging Act also authorised the retention, in specified circumstances, of fingerprints, beyond those allowed by the Data Protection Act. This again was augmented by the Anti-Terrorism, Crime and Security Act 2001 mentioned above, which removes any restriction on retaining fingerprints taken under immigration and asylum legislation.

Dr. Michael Spencer
E-mail: mikespen@gn.apc.org

The Privacy Laws & Business editorial team wishes to express its appreciation to all the contributors to this feature. We acknowledge the co-operation of James Michael, Director, Centre for Communications & Information Law, Faculty of Laws, University College, London, and a group of his LL.M. students. All correspondents have been listed individually and we publish their contact details in different forms to reflect their individual wishes.

Reference to further information about each country is available in the index published annually by Privacy Laws & Business and in the newsletter section of the Privacy Laws & Business website: www.privacylaws.com where, in both cases, references are given by country, subject and by company.

News continued from page 2

Ontario Commissioner Investigates Vulnerability of Online Medical Records

Toronto's *Globe and Mail* newspaper reported, on December 10th 2001, that a computerised medical records system set up by the Ontario government just one month earlier may have already permitted serious breaches of physician-patient confidentiality. The Ontario Health Ministry set up the computer system as part of its five-year programme to streamline the practice of family medicine.

The newspaper report states that the "Physician Project" had received approval from Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, just before the first team of doctors began using the system, but that Dr. Cavoukian had not been given full details about how the information is handled. She has launched an investigation into the allegations of confidentiality breaches. Among the issues that she may investigate:

• the possibility that the system can be hacked into over the Internet

• the alleged failure to inform patients fully about what happens to their data

• allegations that a computer technician took unencrypted backup tapes containing thousands of medical records to his home for several nights and then lost three of the tapes

• the possibility that three private companies have been granted access to raw data files, including patient names and medical histories.