January 2003

INVENTORY OF INSTRUMENTS AND MECHANISMS CONTRIBUTING TO THE IMPLEMENTATION AND ENFORCEMENT OF THE OECD PRIVACY GUIDELINES ON GLOBAL NETWORKS

This inventory was prepared to survey the available instruments and mechanisms (including law, self-regulation, contracts and technology) contributing to the implementation and enforcement of the OECD Privacy Guidelines on global networks. Such a study was intended to serve to identify a range of technological policy and legal tools which may be used as a resource for providing seamless, or at least effective, protection.

Chapter 6

INVENTORY OF INSTRUMENTS AND MECHANISMS CONTRIBUTING TO THE IMPLEMENTATION AND ENFORCEMENT OF THE OECD PRIVACY GUIDELINES ON GLOBAL NETWORKS[1]

Background

In order to contribute towards building a trustworthy environment for the development of electronic commerce and given its ongoing work in the area of the global information infrastructure and the global information society, its history in developing the OECD Privacy Guidelines and its continuing experience in issues related to privacy protection, the OECD decided in October 1997 to examine the various solutions which would facilitate the implementation of the privacy principles in the context of international networks.

The report "Implementing the OECD Privacy Guidelines in the Electronic Environment: Focus on the Internet" [DSTI/ICCP/REG(97)6/FINAL] proposed that OECD member governments:

- Reaffirm that the Privacy Guidelines are applicable with regard to any technology used for collecting and processing data.
- Encourage those businesses that choose to expand their activities to information and communication networks to adopt policies and technical solutions which will guarantee the protection of the privacy of individuals on these networks, and particularly on the Internet.
- Foster public education on issues related to protection of privacy and the use of technology; and
- Launch a dialogue involving governments, industry and businesses, individual users and data protection authorities, to discuss trends, issues and policies in the area of personal data protection.

In that context, a Workshop entitled "Privacy Protection in a Global Networked Society" was organised with the support of the Business and Industry Advisory Committee (BIAC) on 16-17 February 1998. The Workshop was intended to examine how the OECD Guidelines may be implemented in the context of global networks. The OECD sought to build on the various approaches adopted by its member countries and to help identify mechanisms and technological tools that could provide effective bridges between the different approaches to privacy protection developed by member countries. Furthermore an important focus was put on encouraging the private sector to provide meaningful protection for personal data on global networks by effective self-regulation.

With the goal of identifying appropriate practical solutions which could be implemented irrespective of the different cultural approaches, the Workshop sessions addressed the following issues:

- The identification and balancing of the needs of the private sector and of users and consumers and the formulation of efficient strategies for "educating for privacy".
- The development of "privacy enhancing technologies".
- The implementation of private sector-developed enforcement mechanisms for privacy codes of conduct and standards; and
- The adoption of model contractual solutions for transborder data flows.

At the end of the Workshop, participants recognised that increasing confidence in online privacy protection is an essential element for the growth of business-to-business electronic commerce, and that the OECD Guidelines continue to provide a common set of fundamental principles for guiding efforts in this area. They affirmed the commitment to protect individual privacy in the increasingly networked environment, both to uphold important rights and to prevent interruptions in transborder data flows.

The Chair noted widespread consensus that the protection of personal privacy requires: education and transparency; flexible and effective instruments; full exploitation of technologies; and enforceability and redress.

The Chair also highlighted the need to survey the available instruments (including law, self regulation, contracts, and technology) in order to describe their practical application in a networked environment and their ability to further the objectives of the OECD Guidelines (including effectiveness, enforceability, redress and coverage across jurisdictions). Such a study would serve to identify a range of technological policy and legal tools which may be used as a resource for providing seamless, or at least effective privacy protection.

At its May 1998 meeting, the Working Party on Information Security and Privacy agreed to undertake an inventory of instruments and mechanisms contributing to the implementation and enforcement of the OECD Privacy Guidelines on global networks.

Introduction

The development of digital computer and network technologies, and in particular the Internet, has brought with it a migration of social, commercial and political activities from the physical world into the electronic environment. The integration of global networks into everyday life raises concerns over the protection of personal privacy. In the world of digital technology and global networks, users often leave behind long-lasting "electronic footprints", that is, digital records of where they have been, what they spent time looking at, the thoughts they aired, the messages they sent, and the goods and services they purchased. Furthermore, these data tend to be detailed, individualised and computer-processable.

Simply "browsing" on the Web can make a considerable quantity of information available to the sites visited, even if much of this information is needed to enable Internet interaction and much of it is maintained in aggregate form. Whenever a Web page is accessed, certain "header information" is made available by the "client" (the user's computer) to the "server" (the computer that hosts the Web site being accessed) (Kang, 1998). This information can include:[2]

- The client's Internet Protocol (IP) address,[3] from which the domain name and the name and location of the organisation who registered this domain name can be determined through the Domain Name System.
- Basic information about the browser, operating system and hardware platform used by the client.
- The time and date of the visit.
- The Uniform Resource Locator (URL) of the Web page which was viewed immediately prior to accessing the current page.
- If a search engine was used to find the site, the entire query may be passed on to the server; and
- Depending on the browser, the user's e-mail address (if this has been set in the browser's preference configuration screen).

In addition, when a user browses through a Web site, he or she can generate "click-stream data" such as the pages visited, the time spent on each page and information sent and received.

Personal data is also often disclosed voluntarily. Many commercial sites ask users to complete and submit Web page forms in order to register; subscribe, join a discussion group, enter a contest, make suggestions or complete a transaction. The kind of data which are typically requested may include information such as the user's name; address, home or work telephone number and e-mail address. Data relating to age; sex, marital status, occupation, income and personal interests is also sometimes collected. In addition, purchasing forms will usually require credit card details, including the card type, number and expiration date. If a visitor is asked to send information to a Web site by e-mail, then the site (like any e-mail recipient) will be able to ascertain the visitor's e-mail address from the "e-mail header".

"Cookies"[4] are small data packets created by a Web site server and stored on the user's hard drive. Cookies were developed to assist in client/server interaction and data collection, and may be accessed by the server during current and subsequent visits to the Web site.[5] Cookies may be used to facilitate the collection, aggregation and re-use of header, click-stream and voluntarily disclosed data. This is typically accomplished by assigning a unique code to each visitor and storing this number in a cookie which is retrieved each time the site is visited. Information which is subsequently collected about the user can then be linked to this code number.

Thus, although the development of global networks and digital technology has brought many social and economic benefits, recent technology increases the risk that personal information may be automatically generated; collected, stored, interconnected and put to a variety of uses by online businesses or government bodies, without the data subject's knowledge or consent.

This Inventory focuses on the various overlapping and complementary instruments, practices, techniques and technologies which are used, or are being developed, to define, implement and enforce privacy principles in networked environments.

The Inventory is divided into two main Sections. Section I, describes the international, regional and national instruments, both legal and self-regulatory, which exist, or are being developed for the protection of personal data and privacy in OECD member countries. Special attention is paid to instruments which have been specifically developed for the online environment. Section II, discusses the mechanisms which exist, or are being developed, to implement and enforce privacy principles on global networks.

I. Legal and self-regulatory instruments

This Section of the Inventory discusses international, regional and national guidance instruments and related institutions, for the protection of personal data and privacy.

At the international and regional levels, a number of government and private sector multilateral organisations have produced, are producing, or intend to produce, texts and standards aimed at promoting privacy protection. These organisations are also fora for ongoing research, policy formulation and dialogue between governments, businesses, academics and public-interest groups. The instruments that have been developed through such organisations have greatly influenced many national laws and self-regulatory instruments on privacy protection.

At the national level, in most countries the protection of privacy and personal data involves a combination of legislative instruments, government agencies and industry-based self-regulation. All OECD member countries have laws of one sort or another that affect the processing of personal data. A number of countries have enacted "comprehensive" laws which apply personal data protection principles in a general

fashion to both the public and private sectors. Other data protection legislation is more sectoral, applying only to a specific sector (such as government agencies) or a particular type of data (such as health data).

Most OECD member countries have also created central oversight authorities, commonly known as Data Protection Officers or Privacy Commissioners. The roles and powers of these bodies vary from country to country, but generally include advice-giving, the investigation of complaints and enforcement actions.

Self-regulation is seen in some OECD member countries as a flexible and efficient solution to the protection of online privacy by allowing market forces and industry-led initiatives to provide innovative solutions. Self-regulatory instruments may broadly be defined as rules developed and enforced by the entities to whom they are intended to apply. Independent third parties may play a role in enforcement of self-regulation. However, public authorities may also be involved in the development, implementation and enforcement of industry codes and guidelines. Governments can work with the private sector to develop criteria for effective privacy protection which the private sector can implement through self-regulatory codes. In a number of jurisdictions self-regulatory codes are seen as a way of implementing privacy legislation in the context of a specific industry,[6] or as an aid to interpreting general privacy principles. In some OECD member countries such as Ireland and New Zealand, industry codes can, on receiving official approval, have the force of law.

A. International and regional instruments and organisations

1. Intergovernmental legal instruments

(a) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

Status

The *Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (the OECD Guidelines) (OECD, 1980) was adopted by the Council of the OECD on 23rd September 1980. Council Recommendations are not binding legal instruments but reflect a "political" commitment by member countries. The Council recommended that "member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines", that they "endeavour to remove, or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data", and that they "co-operate in the implementation of the Guidelines"(OECD, 1980).

The principles that comprise the OECD Guidelines have been applied in member countries and other countries through a variety of instruments.

Scope

The Guidelines are widely acknowledged as an internationally accepted and technologically neutral set of privacy principles that have stood the test of time. They apply to "any information relating to an identified or identifiable individual",[7] and their scope encompasses public and private sector data, all media for the computerised processing of data on individuals (from local computers to networks with global ramifications) and all types of data processing.[8]

Basic principles

The OECD Privacy Guidelines establish eight basic principles to govern the handling of personal information. These "Privacy Principles" are:

1. **Collection Limitation:** there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject;
2. **Data Quality:** personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date;
3. **Purpose Specification:** the purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose;
4. **Use Limitation:** personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the "purpose specification" except: (a) with the consent of the data subject; or (b) by the authority of law;
5. **Security Safeguards:** personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data;
6. **Openness:** there should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, the main purposes of their use, as well as the identity and usual residence of the data controller;
7. **Individual Participation:** an individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him: within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and, in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and, (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified completed or amended;
8. **Accountability:** a data controller should be accountable for complying with measures which give effect to the principles stated above.

Provisions on data flows

The OECD Guidelines tend to avoid the imposition of unnecessary impediments to transborder data flows.[9] Legitimate restrictions are, however, recognised. For example, a member country may impose transfer restrictions on "certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other member country provides no equivalent protection".

Provisions on further co-operation

The OECD Guidelines create a framework for future co-operation.[10] The areas of future co-operation include; ensuring that procedures for transborder flows of personal data and for the protection of privacy are simple and compatible with those of other member countries, establishing procedures to facilitate information exchange, and developing principles, domestic and international, to identify applicable laws of member countries in the case of transborder flows of personal data.

Provisions on implementation and enforcement

The Guidelines call upon member countries to implement these principles domestically by establishing legal, administrative or other procedures or institutions for the protection of privacy and personal data.[11] The means by which this can be accomplished include; adopting appropriate domestic legislation, encouraging and supporting self-regulation, providing reasonable means for individuals to exercise their rights, providing adequate sanctions and remedies in case of failures to comply with measures which implement the principles and ensuring that there is no unfair discrimination against data subjects.

Ongoing work

The OECD, through the ICCP Committee continues to work in the area of privacy and data protection and provides a forum for discussing new issues, such as the challenges presented by the emergence of global networks.[12]

(b) Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

Status

Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data of 18 September 1980 (Convention 108) (COE, 1980) was opened for signature by the Committee of Ministers of the Council of Europe on 28 January 1981. Since then, it has been signed by 33 countries and ratified by 29 (see Table 6.1).[13] Convention 108 which is open to the accession of any State, and not only to the members of the Council of Europe is a binding instrument in international law.

Scope

The terms of the Convention apply to automated personal data files and automatic processing of personal data in the public and private sectors.[14]

Basic principles

The Convention's basic principles are similar to those in the OECD Guidelines, but include a principle requiring appropriate safeguards for special categories of data (sensitive data) that reveal racial origin, political opinions or religious or other beliefs, that concern health or sexual life, or that relate to criminal convictions.[15]

Provisions on data flows

The principles of the Convention provide for the free flow of personal data between parties to the Convention who provide equivalent protection.[16]

Provisions on further co-operation

For the purposes of mutual assistance in the implementation of the Convention, each party to the Convention designates an authority to furnish information on its laws and administrative practices in the field of data protection.[17] In addition, Articles 18-20 establish the *Consultative Committee* which represents Member States and makes proposals as to the application of the Convention.

Provisions on implementation and enforcement

Each contracting State undertakes to take the necessary measures in its domestic law to give effect to the basic principles of data protection,[18] but the manner of implementation is left for each State to decide. Under Article 10, States undertake to establish "appropriate sanctions and remedies for violations of domestic law giving effect to the basic principles".

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows [ETS No. 181]

On 8 November 2001, an Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) regarding supervisory authorities and transborder data flows [ETS No. 181] (COE, 2001) was opened for signature. It has been signed by 21 member States and ratified by 2 States.

Ongoing work

Through the Consultative Committee, the Council of Europe continues its work in the area of privacy protection and has recently adopted a Guide to the preparation of contractual clauses governing data protection during the transfer of personal data to third parties not bound by an adequate level of data protection, which is intended to amplify and refine the clauses contained in the 1992 model contract, so that the two documents can be regarded as complementary. The Council of Europe's *Project Group on Data Protection* is also working on a draft report containing guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance.

Table 6.1. **National instruments**

	Ratification of Convention 108	Omnibus legislation dealing with privacy and data protection and applying to the:	
		Public sector legislation	Private sector legislation
Australia		✓	
Austria *	✓	✓	✓
Belgium *	✓	✓	✓
Canada		✓	Quebec
Czech Republic	✓	✓	✓
Denmark *	✓	✓	✓
Finland *	✓	✓	✓
France *	✓	✓	✓
Germany *	✓	✓	✓
Greece *	✓	✓	✓
Hungary	✓	✓	✓
Iceland	✓	✓	✓
Ireland *	✓	✓	✓
Italy *	✓	✓	✓
Japan		✓	
Korea		✓	
Luxembourg *	✓	✓	✓
Mexico		✓	
Netherlands *	✓	✓	✓
New Zealand		✓	✓
Norway	✓	✓	✓
Poland	✓	✓	✓
Portugal *	✓	✓	✓
Spain *	✓	✓	✓
Sweden *	✓	✓	✓
Switzerland	✓	✓	✓
Turkey			
United Kingdom *	✓	✓	✓
United States		✓	

* Denotes membership of the European Union.

(c) United Nations Guidelines for the Regulation of Computerised Personal Data Files

Status

The United Nations High Commissioner for Human Rights' Guidelines for the Regulation of Computerised Personal Data Files (Resolution 45/95 of 14 December 1990) (UN Guidelines) (UN, 1990) were adopted by the United Nations General Assembly pursuant to Article 10 of the UN Charter. This Article empowers the General Assembly to make recommendations to Members States. Members must take the Guidelines into account when implementing national regulation concerning computerised personal data files, but the procedures for implementing those regulations are left to the initiative of each State.

Scope

The UN Guidelines apply to computerised personal data files (both public and private) and may be (optionally) extended to manual files and to files on legal persons. Part A of the Guidelines are intended as the minimum privacy guarantees that should be provided in national legislation. Part B of the Guidelines are intended to apply to personal data kept by governmental international organisations.

Basic principles

The "Principles concerning the minimum guarantees that should be provided in National Legislation" broadly reflect the basic principles in the OECD Guidelines. In addition the UN Guidelines restrict the compilation of "sensitive data" within the "Principle of non-discrimination".[19]

Provisions on transborder data flows

Paragraph 9 of the UN Guidelines provides for free transborder data flows between countries with "comparable safeguards".

Provisions on implementation and enforcement

Regarding domestic legislation (Part A), Article 8 recommends that each country establish an independent authority to oversee application of the privacy principles set out in the Guidelines. In addition, violations of national implementing law should lead to "criminal or other penalties ... together with the appropriate individual remedies".

With respect to governmental international organisation (Part B), the creation of supervisory bodies is also recommended.

Ongoing work

A 1997 report (UN, 1997) of the UN Secretary-General looks at the implementation of the Guidelines within the United Nations system and at the national and regional levels.

(d) European Union Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data

Status

Directive 95/46/EC of the European Parliament and of the Council of the European Union of 24 October 1995 on the *Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data* (EU Directive) (EU, 1995) is a binding instrument that the 15 EU Member States were required to implement by 24 October 1998.

Scope

The Directive applies generally to the processing of personal data by a "controller" in an EU Member State.[20] It applies to data about natural persons, whether held by the public or private sector. Computerised data processing and most categories of manual processing are covered.[21]

Basic principles

The information privacy principles contained in Chapter II of the EU Directive are broader and more detailed than those in the OECD Guidelines. In addition to the OECD principles, the EU Directive contains, *inter alia*, special provisions for sensitive data,[22] detailed disclosure requirements,[23] registration provisions,[24] "opt-out" rights for data subjects to refuse commercial solicitations[25] and redress rights.[26]

Provisions on transborder data flows

The EU Directive transborder data flows within the EU on the basis of equivalent protection provided in all Member States and allows transfers to third countries which provide adequate protection. Member States are not permitted to inhibit the free movement of personal data within the EU simply for reasons of privacy protection,[27] because of the equivalent and high level of protection ensured by the Directive throughout the Community. A transfer of data outside the EU may take place to third countries which guarantee an "adequate" level of protection.[28] Adequacy is to be assessed "in the light of all the circumstances surrounding a data transfer operation [with] particular consideration ... given to the nature of the data, the purpose and duration of the proposed processing operation ... the country of origin and the country of final destination, the rules of law, both general and sectoral, in force in the third countries in question and the professional rules and security measures which are complied with in that country". Exceptions apply where, for example, the consent of the data subject has been obtained.[29]

Provisions on implementation and enforcement

The EU Directive defines the role of the supervisory authority or data protection body in each Member State as a key aspect of implementation and enforcement of the domestic law enacting the Directive. These authorities must act with complete independence and should have a wide range of powers that include investigative authority, intervention powers and the ability to engage in legal proceedings.[30]

With respect to enforcement, the EU Directive provides for judicial remedies, liabilities and sanctions.[31] It states that persons shall be entitled to judicial remedies and compensation from data controllers for damage suffered as a result of unlawful processing. Member States have to adopt suitable administrative, civil or criminal sanctions.

Provisions on further co-operation

Article 28 requires supervisory authorities to co-operate with one another as necessary, and in particular to exchange useful information.

The Directive establishes two bodies, one consultative (Article 29) and one "decision-making" (Article 31), to assist the European Commission with issues related to data processing.

Ongoing work

The *Article 29 Working Group* has already issued a number of reports and recommendations including "Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy" (EU, 1997a) and "Judging Self-Regulation" (EU, 1998).

Other developments

On 15 December 1997, Directive 97/66/EC (EU, 1997b) was adopted by the European Parliament and the Council. This Directive complements Directive 95/46/EC with respect to the processing of personal

data and the protection of privacy in the telecommunications sector. It provides for the harmonisation of the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the telecommunications sector and to ensure the free movement of such data and of telecommunications equipment and services in the Community.

(e) General Agreement on Trade in Services

The *General Agreement on Trade in Services* (GATS) is a multilateral agreement which aims to promote free trade in services. GATS is administered by the *World Trade Organization*[32] (WTO). Article XIV recognises that GATS does not prevent Member States from adopting measures necessary to secure "the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts."[33] However, Article XIV limits what a country can do with regard to privacy protection by subjecting it to the requirement or safeguard that any such measures must not be applied in a discriminatory manner and must not constitute a disguised restriction on trade in services.

2. International conferences and discussion forums concerning privacy protection

International conferences and discussion forums play an important role in contributing to information exchange, education and the development of instruments on privacy protection.

(a) Annual international conferences of data protection commissioners

From 1979 *International Data Protection Commissioners' Conferences* have been held annually. The Conferences have no particular legal status and do not vote on resolutions. Rather, they are a forum of information exchange. The 20th International Conference of Data Protection Authorities took place in Santiago de Compostela, Spain.[34]

(b) Conferences of the EU data protection commissioners

The annual Conferences of the EU Data Protection Commissioners provide an opportunity to develop common approaches to privacy protection and to address topical issues such as, telecommunications and police files.

(c) International Working Group on Data Protection in Telecommunications

The *International Working Group on Data Protection in Telecommunications*, led by the *Data Protection Commissioner of Berlin*, was initiated by the data protection commissioners from a number of countries to improve privacy and data protection in telecommunications and media. The "Budapest-Berlin Memorandum" on data protection on the Internet discusses the issues surrounding legal and technical protection of Internet user privacy (International Working Group on Data Protection in Telecommunications, 1996).[35]

(d) International Organization for Standardization

The International Organization for Standardization (ISO)[36] is a world-wide federation of national standards bodies from around 130 different countries. The ISO's work results in international agreements which are published as International Standards. In May 1996, the *Consumer Policy Advisory Committee* of ISO passed a unanimous resolution in favour of a proposal to develop an international standard on privacy based on the *Canadian Standard Association Model Code for the Protection of Personal Information.* An *Ad Hoc Advisory Group on Privacy* undertook a study on behalf of the ISO to examine whether there is a

need, under the pressure of the technological advances in the global information structures, for an international standard to address information privacy, measure privacy protection and ensure global harmonisation.[37] The Advisory Group concluded in June 1998 that it was premature to reach a determination on the desirability and practicality of ISO undertaking the development of international standards relevant to the protection of personal privacy.

(e) International Chamber of Commerce

The International Chamber of Commerce (ICC)[38] represents international businesses all over the world and has produced a number of documents and industry codes relating to the protection of personal privacy and information flows. These have included a range of marketing codes and guidelines, including guidelines for Internet advertising, with privacy provisions.[39] The ICC has also published a proposed model contract for transborder flows of personal data which builds on the 1992 ICC/Council of Europe/European Commission model contract.

(f) International Federation of Direct Marketing Associations

The *International Federation of Direct Marketing Associations* (IFDMA) is a collaboration of national and regional direct marketing associations. Its aims include fostering industry programmes of self-regulation and consumer education. The data protection "Online Principles" formulated by the IFDMA encourage direct marketers to post their privacy policies online in a manner that is easy to find, read and understand. The principles include special provisions with respect to children's online activities.

(g) Electronic Commerce Europe

Electronic Commerce Europe (ECE) is a group of European electronic commerce businesses and associations who are working on drafting a *Code of Conduct for Electronic Commerce*.

(h) Online initiatives for privacy information exchange

A number of privacy orientated non-governmental organisations have created Web sites to provide information on online privacy issues. These organisations include, *inter alia*:

- The *Electronic Privacy Information Center*[40] (EPIC), a public interest research centre established to focus public attention on emerging online civil liberties issues and to protect privacy.
- The *Center for Democracy and Technology*[41] (CDT), a public interest organisation working for public policies that advance civil liberties and democratic values in new computer and communications technologies.
- *Privacy International*,[42] a human rights group formed to act as a watchdog on surveillance by governments and corporations; and
- *PrivacyExchange.Org*,[43] a group intended to provide timely information on national data protection laws and practices, and distribute model policies, agreements and codes of conduct.

B. National instruments

AUSTRALIA

Laws

Commonwealth / federal laws

The federal *Privacy Act 1988* is the principal piece of legislation providing protection of personal information in the federal public sector and in the private sector.[44] The Privacy Act provides eleven Information Privacy Principles for the federal public sector and ten National Privacy Principles for private sector organisations based on the OECD privacy guidelines. These Privacy Principles deal with all stages of the processing of personal information, setting out standards for the collection, use, disclosure, quality and security of personal information. They also create requirements of access to, and correction of, such information by the individuals concerned.

The Privacy Act also establishes the Office of the Federal Privacy Commissioner which can receive complaints, conduct investigations and make determinations (including compensation orders) that are enforceable in the Federal Court of Australia.[45]

Other federal laws with privacy provisions

Other Commonwealth legislation provides privacy protection for specific types of information, such as "spent" criminal convictions (Part VIIC, *Crimes Act 1914* protects a person against the unauthorised use of certain criminal convictions after ten years) and taxation information (*Taxation Administration Act 1953*), and for specific procedures, such as the interception of telecommunications and the disclosure of personal information by telecommunications companies (*Telecommunications Act 1997*). The *Data-matching Program (Assistance and Tax) Act 1990* provides privacy protections in relation to the matching of personal information relating to tax and social welfare benefits by Commonwealth Government Departments.

State and territory laws

Several states and territories have legislated to establish privacy protections, either in relation to their respective public sectors or in relation to personal health information. Other states have established privacy regimes administratively that reflect the principles found in the federal Privacy Act.[46]

Self-regulatory instruments

The federal Privacy Act also provides for the development of privacy codes for private sector businesses and industries that can be approved by the Privacy Commissioner. Where there is an approved privacy code, the code operates in place of the legislative standards although codes must reflect those legislative standards as a minimum.[47]

AUSTRIA

Laws

Federal comprehensive laws

The *Federal Data Protection Act of* 1978 (*Datenschutzgesetz. BGBl. Nr. 565/1978*) regulates the use of computerised data in the public and private sectors, creates a central registration system and provides

civil remedies and criminal sanctions.[48] A new law is being prepared to implement the EU Data Protection Directive.

An independent Commission (the *Datenschutzkommission*), is responsible for enforcing the law, administering the registration system and authorising transborder data flows. The Commission acts on specific complaints against public data controllers, and can impose sanctions for certain actions, such as breaches of transborder data flow authorisations. A *Council for Data Protection* also exists and may be referred to by the Commission for advice on certain matters. Complaints against private data controllers must be brought before the courts.

The Chamber of Commerce and the Federal Chancellery run a court of arbitration, the *Schlichtungsstelle-Datenschutz*, which hears complaints against businesses who have not complied with a request by a data subject to access, correct or delete personal information.

Other federal laws with privacy provisions

There are many federal laws in Austria which relate to personal privacy. For example, the *Austrian Telecommunications Act* (1997)[49] imposes confidentiality and data protection obligations on suppliers of public telecommunication services. The use of personal information by direct marketing businesses is governed by Section 268 of the *Industrial Code* (1994).[50] Finally, the *Genetic Engineering Act 1994* contains data protection provisions relating to genetic data.

Implementation of the EU Directive

A first draft of the *Datenschutzgesetz* was submitted to Parliament.[51]

Laender (state) laws

The role which individual *Land* will play in data protection is presently being considered in the context of implementing the EU Directive.

Self-regulatory instruments

Whilst there are no codes of conduct in Austria which deal exclusively with privacy, members of the banking sector have codes in place containing general privacy clauses.

BELGIUM

Constitution

Privacy rights are contained in Articles 22 and 32 of the *Belgian Constitution*.

Laws

Comprehensive laws

The *Law on the Protection of Privacy Regarding the Processing of Personal Data* (1992) applies to both the public and private sectors in Belgium. The Law is supplemented by Royal Decrees with respect to, for example, sensitive data and information regarding criminal convictions. The law is supervised by an independent Commission within the *Ministry of Justice*, the *Commission Consultative de la Protection de la Vie Privée*.[52] The Commission handles data processing registrations and may also advise the government on privacy matters.

In terms of recourse for individuals, applications may be made to the *Tribunal de Première Instance* for rulings on the rights arising under the Law. The Law also includes criminal sanctions for breach of privacy obligations.[53]

Other laws with privacy provisions

The *Law of 30 June 1994* provides for privacy protection in the context of wire-tapping and the recording of private telecommunications.

Implementation of the EU Directive

A draft law designed to implement the Directive and based on the structure of the 1992 Law, is now before the Belgian Parliament.[54]

Self-regulatory instruments

The *Internet Service Providers Association* of Belgium has a Code of Conduct, approved by the Plenary Assembly, which encourages its members to comply with privacy protection law in their use of clients' personal data.[55]

CANADA

Laws

Federal laws

The *Privacy Act* (1983)[56] applies to virtually all federal public sector institutions in Canada. The Act regulates the confidentiality, collection, correction, disclosure, retention and use of personal information, and gives data subjects the right to examine information held about them and to request that errors be corrected. The Act reflects the principles of the OECD Guidelines.

The *Privacy Commissioner* is appointed by Parliament to investigate complaints and audit compliance with the Act by federal agencies. The Commissioner has the authority to conduct investigations, attempt to resolve disputes, and issue recommendations. Disputes about the right of access to personal information that are not resolved in this manner can be taken to the *Federal Court* for review.

Federal approach to privacy in the private sector

The Canadian federal government introduced privacy legislation to protect personal information in the private sector on October 1, 1998 Bill C-54. The *Personal Information Protection and Electronic Documents Act*, has received its second reading and is currently being studied by the Standing Committee on Industry, which will report back to Parliament in the spring of 1999. The legislation will initially extend privacy protection to the federally-regulated private sector as well as inter-provincial and international trade in personal information. Three years later the legislation will apply to the remaining private sector organisations which fall under provincial jurisdiction. If a province enacts substantially similar legislation, the commercial organisations operating under its jurisdiction will be subject to the provincial law. At this time, only the province of Quebec has such legislation. The obligations and rights set out in the bill are those of the Canadian Standard Association's *Model Code for the Protection of Personal Information* which is a recognised national privacy standard that is modelled on the OECD Guidelines. Individuals have access and redress rights and the federal *Privacy Commissioner* will exercise oversight by investigating and reporting on complaints. The Commissioner has ombudsman powers but complainants

may bring unresolved matters to the *Federal Court*, as may the Commissioner, and the Court has the power to issue binding orders and award damages.

Provincial laws

Most Canadian Provinces have passed privacy legislation governing the public sector and the majority of this legislation reflects the principles included in the OECD Guidelines.[57] Various sectoral statutes provide privacy protection in areas such as personal health information.[58]

Quebec is the only province where general legislation, the *Act Respecting the Protection of Personal Information in the Private Sector* (1993), regulates the handling of personal information by private sector organisations, including corporations, sole proprietorships, partnerships, organisations and associations. The Act governs the collection and use of personal information and provides individuals with a right of access and correction, disputes are resolved before the *Commission d'accès à l'information*, the agency which is responsible for oversight and redress for public sector information access and privacy rights in the province. It is noteworthy that the law has special provisions which apply to lists of names used for marketing purposes and to transfers of information about Quebec residents to third parties outside of the province.

Self-regulatory instruments

The CSA model code

Canada has a widely accepted model code of conduct with respect to privacy. The *Model Code for the Protection of Personal Information* was developed by the *Technical Committee on Privacy*[59] of the *Canadian Standards Association* (CSA) and was adopted as a National Standard by the *Standards Council of Canada* in 1996.[60] The Code reflects the OECD Guidelines, but also requires companies to identify an officer accountable for compliance to whom complaints may be addressed.

The CSA has prepared a workbook, "Making the CSA Privacy Code work for You",[61] to assist in the development of compliant codes (which may be certified by the *Quality Management Institute*, a division of the CSA). In terms of ensuring ongoing compliance with a code, the workbook highlights the importance of independent audits by duly certified auditors. Private sector codes may be certified as complying with the CSA standard by a quality registrar and a company may cite the standard in an ISO 9000 registration. There are a variety of ways in which a company may demonstrate compliance, *e.g.* the Canadian Bankers' Association *Privacy Model Code* was verified by Price Waterhouse.

Other initiatives

A number of companies and associations have or are in the process of developing CSA based privacy codes, including Stentor (the alliance of telecommunications providers), the Canadian Marketing Association, the Canadian Bankers Association, the Insurance Bureau of Canada, the Canadian Television Standards Association and the Canadian Medical Association.

Instruments relating to online privacy

The *Canadian Association of Internet Providers'* (CAIP's) voluntary *Code of Conduct*[62] requires CAIP members "to respect and protect the privacy of their users" and comply with all applicable laws. Enforcement is by a complaint-driven process to be established by each member.

CZECH REPUBLIC

Laws

Comprehensive laws

The *Protection of Personal Data in Information Systems Act* became effective on 1 June 1992.[63] The Act covers computerised data on natural persons and applies to both the public and private sectors.

This Act broadly conforms with the principles of the OECD Guidelines and sets down specific provisions for sensitive data. It contains civil remedies for breaches that are administered through the courts. There is no data protection commissioner in the Czech Republic at this time.

In anticipation of the Czech Republic joining the EU, the Government has appointed the *Office for the State Information System* (OSIS) to prepare the legislation that will be compatible with the EU Data Protection Directive.[64] The new legislation will establish the framework for an independent supervisory body. It is not expected that the legislation will receive Parliamentary approval before the middle of 1999.

Other laws with privacy provisions

A Bill is being prepared by the *Czech Telecommunication Office* in co-operation with OSIS which will implement the terms of EU Directive 97/66/EC on the protection of privacy in the telecommunications sector. A proposal for the Digital Signature Law is also being prepared by the Office for the State Information System (OSIS) which will implement the terms of the EU Directive on a common framework for electronic signatures.

DENMARK

Constitution

According to section 72 of the Constitution, regarding the sanctity of the home, it is forbidden, without a prior court order, to search an individual's house, open their letters or tap their telephone. It is generally accepted in Danish judicial theory that this section can be interpreted to also apply to data stored electronically and any form of telecommunication. The authorities may not, for example, open and examine one's e-mail without prior consent. They may intercept and open the message via the telecommunications networks only if they have a court order which allows them to. The main rule being that a search requires a prior court order, a search without a prior warrant may therefore only take place in exceptional cases where it is deemed absolutely necessary. A general permission is granted in accordance with the Law on Civil and Criminal Proceedings. Outside the scope of criminal proceedings, permission to perform administrative searches is granted under numerous laws, for example, to carry out an inspection by the Data Surveillance Authority of the locations of public filing systems.

Laws

The Law on Public Access ensures (§ 4 section 1) that any citizen may have access to documents which form part of public authority decisions. The wide access to documents is, however, limited by section 3 of § 4, which requires that the person seeking access is able to identify the case which he is applying for access to.

The following documents are exempt from access; records of criminal proceedings, application and procedures regarding the employment of civil servants and documents intended for internal use only. These

exemptions may be divided into two categories *1)* personal data concerning individual citizens in accordance with § 12; *2)* types of data to which access is denied for reasons of public policy, in accordance with §13. An example of the first category of data would be the political affiliation of a person. An example of a public policy interest that may outweigh access in the second category of data would be national security.

The Danish laws on public and private filing systems have been in effect since 1979. The laws provide privacy protection with respect to both governmental agencies and to filing systems kept by private entities.

The Law on Public Filing Systems is applicable to computerised filing systems held by public authorities containing personal information in accordance with § 1, section 1. The law applies only to the administration.

One of the purposes of the Law on Private Filing Systems is to ensure that economic and personal data about private citizens, institutions, societies, and companies are only recorded by private persons to the extent that they serve fair interests and that the recorded data are processed in a satisfactory way. The law contains a general ban on private parties systematically processing personal data, but does, however, contain certain exceptions to this rule. The law applies to any *systematic processing* (gathering, recording and passing on) of *personal and economic data*, carried out by private parties (persons or companies) *by electronic data processing* (EDP)) or, in some instances, *manual* processing.

The Danish Media law regulates the liability of the mass media (traditional news and IT related news). The media law is closely related to the Penal Code, because several of the punishable media offences relate to the rules on privacy in the Penal Code.

The Danish Penal Code, § 152, contains a prohibition for civil servants to illegally process or use confidential information, obtained through their work. The section contains the legal basis on which employees who abuse their duty of confidentiality may be fined. The Article states that the mere obtaining of information is permitted, but it is illegal to process or abuse that personal data. However, the obtaining of the information may be subject to ordinary disciplinary sanctions. § 152a-d states that the duty of confidentiality (and the sanctions affiliated to this) extends to include persons who are not civil servants, but who in some way perform duties for the public administration.

§ 263 of the Penal Code, subsection one, deals with the situation where someone opens another person’s mail, searches their private premises or listens in on their conversations. These rules can easily be interpreted to cover the situation in which someone gains unauthorised access to another person’s e-mail messages or intercepts their messages via telecommunications networks. Subsection 2 covers the situation in which someone gains unauthorised access to programmes or personal information destined to be used in a computer system. Intercepting data transmissions is also included in this subsection.

Under section § 264 d, it is a crime to pass on information or pictures concerning the personal affairs of other individuals. New network capabilities facilitate the circulation of such information to a much wider range of persons than was previously possible.

The Data Surveillance Authority monitors both public and private filing systems. It is organised under the competence of the Ministry of Justice, but complaints etc., about the authority cannot be brought before the Minister of Justice and he has no authority to instruct the Data Surveillance Authority, in other words the Authority is independent. This is known as functional independence, and is an important element of securing the integrity of the data subject.

Implementation of the EU Directive

A proposal to implement the EU Directive was introduced to the Danish Parliament (the *Folketinget)* on 30 April 1998.

Self-regulatory instruments

The Ombudsman for consumer issues is preparing a set of ethical rules aimed at use of the Internet, at this time there is no information on when the work will be completed.

Other self regulatory initiatives include:

- Fabel, an organisation to promote the responsible use of e-mail.
- FIB, an organisation for Internet users, with the purpose of trying to secure rights for Internet users; and
- FIL, an organisation consisting of Internet service providers. The organisation has worked to provide a set of rules protecting users.

FINLAND

Constitution

Section 10 of the *Finnish Constitution* provides that everyone's private life, honour and the sanctity of the home are guaranteed. More detailed provisions on the protection of personal data are laid down by the Act. Also the secrecy of correspondence, telephony and other confidential communications is inviolable.

Laws

Comprehensive laws

The *Personal Data Act* (523/1999),[65] as amended, represents a legal framework for all processing of personal data. It covers both automatically processed personal data and manual records of natural persons in both the public and private sectors. The Act regulates the collection, correction, disclosure, retention and use of personal data and gives data subjects the right to examine information held about them and to request that errors be corrected.

There are two overseeing bodies, the *Data Protection Ombudsman*[66] and the *Data Protection Board*. The Data Protection Ombudsman provides direction and guidance and supervises the processing of the personal data and decides matters concerning the right of access and rectification. The Data Protection Board deals with questions of principle relating to the Act, grants permissions for the processing of personal data or sensitive data and makes decisions in matters of data protection as provided in the Act.

The Personal Data Act includes civil remedies (for example, data controllers must compensate data subjects for unlawful data use) and criminal sanctions for violations.[67]

Other laws with privacy provisions

A number of statutes in Finland have implications for data protection and privacy, such as the *Statistics Act*, the *Act on the Medical Research Development Centre* and the *Act on the Status and Rights of Patients*. The *Act on Data Protection in Working Life* incorporates the main data protection issues relating

to working life by creating procedures for the needs of working life in particular. The *Act on the Protection of Privacy and Data Security in Telecommunications* promotes the data security of public telecommunications and the protection of the privacy and the legitimate interests of sub-scribers and users in telecommunications. The Ministry of Transport and Communications Finland is drafting the new Act on Privacy and Electronic Communications and it is scheduled to enter into force on October 2003. The purpose of the Act is to secure the confidentiality and privacy in electronic communications. The Act will implement the EU Directive on Privacy and Electronic Communications with several domestic amendments.

Implementation of the EU Directive

The Personal Data Act came into force on 1 June 1999. It was enacted to implement the EU Directive on data protection.

Self-regulatory instruments

The Personal Data Act contains provisions on sectoral codes of conduct drafted by the controllers or their representatives. The Data Protection Ombudsman may check if the code of conduct is in conformity with the legislation. The Finnish *Rules for Electronic Consumer Trade*[68] were prepared jointly by the *Finnish Central Chamber of Commerce*, the *Finnish Direct Marketing Association*, the *Federation of Finnish Commerce and Trade* and the *Finnish Federation for Communications and Teleinformatics*. Codes of conduct have also been drafted so far, inter alia, for direct marketing.

FRANCE

Laws

Comprehensive laws

Law No. 78/17 of 6 January 1978 on *Data Processing, Data Files and Individual Liberties* covers computerised and manual records on natural persons and applies to the public and private sectors. Law 78/17 was modified by Law No. 94-548 which introduced a special regime for the processing of personal health data for research purposes. Law 78/17 is supplemented by the *Penal Code*.[69]

Law 78/17 establishes a central registration system which is administered by an independent data protection authority, the *Commission Nationale de l'Informatique et des Libertés* (CNIL).[70] The data protection authority's role includes informing and advising the public on rights and obligations under the law, examining data processing proposals in the public sector prior to their implementation, and proposing changes in the law in line with technological developments. The authority acts on its own initiative or on complaints and queries, it carries out investigations and ensures that data subjects may exercise rights of access.

Unlawful processing or transfer of named data is punishable under Law 78/17 by fines and/or imprisonment.[71] A criminal prosecution for breach of the Act may be brought by an individual data subject or a prosecuting authority.

Other laws with privacy provisions

Sectoral laws with privacy provisions include, inter alia, the *Labour Code*[72] and the *Law on Video Surveillance* (1995).[73]

Implementation of the EU Directive

A report on implementing the EU Directive was issued on 3 March 1998, and a Bill is being prepared by the *Ministry of Justice*. The Bill will be discussed at ministerial level before submission to the *French Parliament*. The *National Commission for Human Rights* and the CNIL will be consulted on the draft law.

Self-regulatory instruments

Instruments relating to online privacy

The "*Charte de l'Internet"*[74] (Internet Charter) is a self-regulatory initiative established on the ground of national legislation. This Charter, aimed at Internet actors,[75] creates an independent supervisory body, the "*Conseil de l'Internet"* (Internet Council), with advisory and mediation powers. The Charter stipulates that users should have the right to use services anonymously, and imposes an obligation on Internet actors to inform users of the data being collected.

Other initiatives

Syndicat des Entreprises de Vente par Correspondance et à Distance (*SEVPCD),* a professional association for distance marketers, has developed a code of conduct designed to accord with the Law 78/17.[76] Only members who comply with these rules are entitled to display the Association's emblem, and violations may result in disciplinary proceedings before the Association's Supervisory Committee.

GERMANY

Laws

Federal comprehensive laws

Germany's *Federal Data Protection Act* (1990)[77] is applicable to computerised and manual records of natural persons. The Act distinguishes between public and private data controllers. Public sector name-linked files must be registered with the independent *Federal Data Protection Commissioner* who is elected by Parliament. The supervisory authorities for the private sector are designated by the laws of each German State (*Land*). Private organisations are required, under certain circumstances, to appoint data protection supervisors to see that the law is observed.

Anyone may lodge a complaint with the Federal Data Protection Commissioner if they believe that their rights have been infringed through the collection, processing or use of personal data by a Federal authority.[78] Complaints against private sector organisations may similarly be made to the Laender supervisory authorities. In terms of sanctions, the Act creates administrative penalties and criminal offences.[79]

Other federal laws with privacy provisions

The German Federal Government has enacted a significant number of specific issue laws and regulations[80] dealing with privacy, including legislation on; national registers and archives, federal statistics; population registers, the storage and transfer of personal data concerning foreigners in Germany (the *Central Register of Foreigners Act* (1994)), and telecommunications (the *Federal Telecommunications Act* (1996) and the *Telecommunications Carriers Data Protection Ordinance*).

Article 2 of the Federal *Information and Communication Services Act*[81] (1997) governs the processing of personal data in the networked environment. The Act refers to the anonymous use of teleservices, technical devices to minimise the amount of personal data collected and procedures for obtaining electronic consent. The *Tele Services Data Protection Act*[82] (2001) specifically governs the processing of personal data of users by providers of information society services. The Act refers to the anonymous use of teleservices, the minimisation of the amount of personal data collected by providers and the possibility and procedures for users to consent by electronic means into further processing of their data.

Laender (state) laws

Each *Land* has its own data protection law covering its public sector, as well as its own data protection authority.[83] The Data Protection Commissioners of the Federation and the Laender hold regular conferences.[84] The Laender have also laid down rules for specific information society services in their Media Services State Treaty which correspond to the rules of the federal *Tele Services Data Protection Act*.

Implementation of the EU Directive

The Federal Government and Laender are currently working on new legislation to implement the EU Directive.[85] Some of the Laender Commissioners have issued draft implementation proposals and have published Guidelines on transborder flows of data to countries without adequate protection provisions.

Self-regulatory instruments

The approach to privacy protection in Germany is currently based on laws rather than self-regulatory mechanisms.

GREECE

Constitution

The Greek Constitution contains rights to personal and family privacy (Article 9) and secrecy (Article 19).

Laws

Comprehensive laws

The Law No. 2472/97 regarding the *Protection of the Individual Against Processing of Personal Data* was approved on 26 March 1997 and implements the EU Directive.[86] The Law covers computerised and manual personal data on natural persons, and applies to the public and private sectors. The Law also establishes an independent *Data Protection Authority* to oversee the registration system, enforce the Law, promote the adoption of sectoral voluntary codes and impose sanctions for violations.[87]

The Law gives data subjects the right to be informed of, and have access to, their personal data and to apply to Court for the suspension of certain processing operations.[88] The Law provides civil damages for losses caused in contravention of the law,[89] administrative sanctions (such as fines and the cancellation of data processing licences)[90] and criminal sanctions.[91]

Other laws with privacy provisions

Law No. 2225/94 protects freedom of correspondence and communication.

Self-regulatory instruments

There are no specific privacy codes of conduct in Greece, however the Codes of Conduct of the *Journalists Association* and the *Greek Banks Association* both refer to the protection of privacy.

HUNGARY

Constitution

The Hungarian Constitution includes a right to the protection of personal data (Article 59).

Laws

Comprehensive laws

The law on the *Protection of Personal Data and Disclosure of Data of Public Interest*[92] (1992) covers both computerised and manual data regarding natural persons, applies to both the public and private sectors and includes a limited registration system. An independent *Parliamentary Commissioner for Data Protection and Freedom of Information* was elected pursuant to the Act in 1995. The Commissioner is responsible for observing the implementation of the Act, investigating complaints and maintaining the Data Protection Register.

The Act, which includes the basic principles in the OECD Guidelines, gives data subjects a number of rights over their personal data (including correction/deletion of data).[93] The Act also provides for remedies (including compensation) for breaches. Remedies may either be pursued through application to the Commissioner[94] or by initiating court proceedings.[95]

Other laws with privacy provisions

There are a number of specific-issue laws with provisions relating to data protection. These include Acts concerning the national registry; the handling of research and direct marketing information, the handling of medical data, education, archives, the police, banking and national security.

Self-regulatory instruments

Examples of self-regulatory initiatives can be found in the co-operation between direct marketing companies and in the rules adopted by, for example, Hungary's National Association of Journalists. The Office of the Data Protection Commissioner offers professional consultation to those in charge of drafting ethics regulations.

ICELAND

Laws

Comprehensive laws

Iceland's data protection legislation, *Act Nr. 121 Concerning the Registration and Handling of Personal Data* (28 December 1989), is applicable to both the public and private sectors. The legislation covers computerised and manual personal data of natural and legal persons. The legislation also establishes a central registration system which is overseen by the *Icelandic Data Protection Commission*. The Commission's other functions include handling violations of the Act,[96] and authorising the processing of data abroad.

Data subjects have rights of access to personal data, and can demand rectification or deletion.[97] Data subjects can also request that their names be deleted from direct mailing lists.[98] If there is a dispute over a data subject's rights, the matter can be referred to the Data Protection Commission. The Commission can make orders in cases where the data subject's rights have been infringed.[99]

The 1989 Law contains criminal sanctions for the infringement of certain provisions.[100]

IRELAND

Constitution

The Irish Constitution recognises a right to privacy.[101]

Laws

Comprehensive laws

The *Data Protection Act 1988* covers computerised personal data of natural persons and establishes a limited registration system applying to certain categories of data controllers including the public sector, holders of sensitive data, financial institutions, and organisations involved in direct marketing, debt collection and credit reference.

The Act establishes the government-appointed post of *Data Protection Commissioner*. The Commissioner enforces the law by investigating complaints, prosecuting offenders, supervising registrations and encouraging the development of sectoral codes of conduct. The Data Protection Commissioner's decisions may be challenged in the courts.

The Act establishes data protection principles which must be observed regardless of registration. The breach of one of these principles does not involve a criminal offence per se, however, if the Commissioner investigates a complaint and issues a Statutory notice, failure to comply without reasonable excuse becomes an offence. The Act provides for specified criminal offences such as unauthorised disclosure.[102] Civil litigation may be used by data subjects to seek compensation for violations of the Act.

Other laws with privacy provisions

Ireland also has specific statistical data laws, as well as regulations made pursuant to the Data Protection Act which relate to privacy and the protection of personal data.

Implementation of the EU Directive

A draft Bill to implement the EU Directive has been submitted to the Attorney-General's office and will go to Parliament before mid July 1999. This follows the "Consultation Paper on Transposition into Irish Law" produced by the *Department of Justice Equality and Law Reform* (November 1997).

Self-regulatory instruments

The *Irish Direct Marketing Association's* (IDMA's) Code of Conduct[103] provides guidance on the application of the Data Protection Act to direct marketing. In terms of enforcement, a company official should be appointed to ensure compliance and carry out reviews, complaints may be addressed to the IDMA Board whose powers include expulsion from the Association.

Sectoral codes of conduct may be validated by the Irish Parliament, thereby giving them force of law.

ITALY

Laws

Italy's Data Protection Act no. 675/1996 (which transposed EU Directive 95/46) covers both computerised and manual personal data of natural and legal persons in the public and private sectors. Processing of sensitive data was given stronger protection, and in particular specific provisions were adopted applying to the processing of sensitive data by public bodies (legislative decree no. 135 of 11.05.1999). The cases were specified in which the processing could be considered to serve a substantial public interest and was therefore automatically allowed with a view to achieving that purpose. As to private data controllers, lawfulness of the processing of sensitive data is based on a specific authorisation to be issued by the *Garante* – the data subject's written consent being necessary though not sufficient. Ever since 1997, this type of processing was authorised by the *Garante* via a "general authorisation" laying down the scope of said processing.

In a decree of 30.07.1999, no. 281, specific provisions were made in connection with the processing of personal data for historical, statistics and scientific research purposes. Special emphasis was put on the role played by codes of conduct and ethics. Decree no. 282/1999 was also enacted to regulate the processing of medical data by either public health care bodies or health care organisations or professionals discharging their functions on the basis of either an agreement with or the formal recognition of the national health service.

As to security measures, regulations were enacted in decree no. 318/1999 to set out the minimum security standards for the processing of personal data. Different measures were provided for depending on the use of electronic or automated means for the processing as well as on the types of the data (with particular regard to sensitive data).

In order to bring Italian legislation further into line with certain principles of the Directive, legislative decree no. 467/2001 was enacted. In particular, it simplifies and streamlines requirements of and prerequisites for the data processing and strengthens the safeguards applying to data subjects on the basis of the experience gathered in implementing the DPA. The main issues addressed by this Act are the balancing of interests principle, the prior checking issue, the simplification of the notification requirements and the applicable law. Special emphasis is put in the decree on the adoption of new codes of conduct and professional practice, which have proven quite effective to fully implement the principles set forth in the DPA as well as in Council of Europe recommendations concerning several sectors, which have all been expressly referred to in compliance with the adequate representation principle. Decree no. 467/2001 also

modified the punitive approach set out in Act no. 675/1996, by changing the nature of a few sanctions and providing, to some extent, for recognition of a controller's "repentance" as regards breaches of the regulations concerning minimum security measures. Additionally, serious instances of false statement and/or communication to the supervisory authority now carry criminal penalties. Some specific provisions supplemented decree no. 171/1998, which transposed EC Directive 97/66 into Italian domestic law. Such provisions concern, in particular, arrangements for making alternative payment methods actually available so as to ensure user anonymity, and the obligation for telecommunication service providers to adequately inform the public on calling line identification services as well as to ensure that presentation of calling line identification is prevented in connection with emergency calls.

The *Garante per la protezione dei dati personali* is the authority responsible, pursuant to Article 28 of EC directive 95/46, for monitoring the application of the provisions adopted to implement the directive. The *Garante* is also in charge of monitoring application of the Schengen, Europol, Eurodac and CIS conventions.

Among the most important tasks discharged by the *Garante*, reference can be made to verifying whether data processing operations are carried out in compliance with laws and regulations in force as well as with the relevant notification; receiving reports and complaints; encouraging, within the categories concerned and in conformity with the principle of representation, the drawing up of codes of ethics and conduct for specific sectors and contributing to the adoption of and compliance with such codes; informing the Government of the need for passing legislation as required by the developments in this sector. Furthermore, the Prime Minister and each Minister are required to consult the *Garante* when drawing up regulations and administrative measures which concern data protection.

The arrangements for lodging a complaint with the *Garante* – as per Section 29 in the DPA – were put into practice starting in 1999 (d.P.R. no. 501/1998). They represent an alternative approach to legal action in court and allow data subjects to obtain expeditious decisions. This type of complaint can only be lodged in case of partial or total failure to exercise the rights granted to data subjects by Section 13 of the DPA (rights of access, rectification, information, erasure, etc.).

Self-regulatory instruments

The Authority did take part in drawing up the following codes of conduct:

- The Code of conduct for the processing of personal data in the exercise of journalistic activities was drafted by the National Council of Press Association in co-operation with the Data Protection Authority. The above code allowed making detailed provisions in respect of the simplified arrangements – as also related to informing data subjects at the time of data collection – which were laid down for the processing of personal data in the exercise of journalistic activities. The Code of conduct applying to the processing of personal data for historical purposes was aimed at ensuring that personal data acquired in connection with historical research, exercise of the right to study and information, as well as the activity of archives would be used in compliance with data subjects' rights, fundamental freedoms and dignity, with particular regard to the right to privacy and personal identity.
- The Code of Conduct and Professional Practice Applying to the Processing of Personal Data for Statistical and Scientific Research Purposes within the Framework of the National Statistics System.
- The codes of conduct for defence counsel and private detectives are being finalised.

In the next future the following codes will have also to be adopted in pursuance of Section 20 of legislative decree no. 467/2001, as regards the processing of personal data:

a) That is performed by providers of communication and information services offered via electronic networks.
b) That are required for social security purposes or in connection with the employer-employee relationship.
c) That is performed for sending advertising material and/or for direct selling purposes.
d) That is performed for commercial information purposes.
e) That is performed within the framework of information systems owned by private entities.
f) That are included in archives, registers, lists, records or documents held by public bodies.
g) That is performed by means of automated image acquisition devices.

Compliance with the provisions set forth in the above codes will be a fundamental prerequisite for the processing to be lawful. The codes will be published in the *Official Journal* under the *Garante's* responsibility and will be annexed to the consolidated text of data protection provisions.

JAPAN

Laws

Public sector laws

The Act on Protection of Computer Processed Personal Data held by Administrative Organs(1988) covers computerized data on natural persons. The Act generally conforms to the OECD Guidelines. The Ministry of Public Management, Home Affairs, Posts and Telecommunications (MPHPT) oversees the Act. Under the Act, the government Agencies must publish notices listing their file systems and data subjects have the right to access to their own personal data.

The Cabinet proposes a new bill, covering both computerized and manual data , that will permit data subjects to exercise several rights on their own personal data (including data access, data correction, and suspension of use of data).

Approach to privacy regulation in the private sector

Basic Guidelines on the Promotion of an Advanced Information and Telecommunications Society (the Prime Minister's Office 1998) have been produced which include the following direction on the issue of privacy *(1)* the private sector should take the initiative to formulate guidelines, registration systems and mark granting systems specific to each area of industry and business; *(2)* on the other hand, governmental regulations concerning entities dealing with highly confidential information, such as personal credit data and medical data which could be damaging if leaked, should be taken into account. In short, the Government will be required to promote independent efforts in the private sector, as well as be expected to review the situation, taking into consideration legal regulations. The Government must also make the necessary efforts to encourage business to disclose to consumers the manner in which they protect personal data.

The report of "A Consultation Meeting for Protection and Utilisation of Personal Credit Data" (the Ministry of International Trade and Industry, the Ministry of Finance, 1998) indicated the need for legal regulation for protecting personal credit data. The report of the "Study Group on Privacy Protection in Telecommunications Services" (the Ministry of Posts and Telecommunications (MPT), 26 October 1998) also indicated the need for a legal background to make "Guidelines on the Protection of Personal Data in

Telecommunications Business" effective. The Japanese Government has also actively encouraged the adoption of codes of conduct by the private sector (see below).

In October 2000 the Legislative Committee for Personal Information Protection under the Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society published the "Outline of Fundamental Legislation for Personal Information Protection". In accordance with this outline Cabinet Secretariat proposes the Bill on the Protection of Personal Information. This bill covers the private sector comprehensively and gives data subjects several right on their own personal information (including data access, data correction, and suspension of use of data).

Local authority laws

There are a large number of Ordinances enacted by local authorities in Japan that provide privacy protection for manual and/or computerised data. While most Ordinances are only applicable to local government bodies, some extend to the private sector.[104]

Self-regulatory instruments

In March 1997, the *Ministry of International Trade and Industry* (MITI) published "Guidelines Concerning the Protection of Computer Processed Personal Data in the Private Sector".[105] The MITI Guidelines apply to electronically processed personal data and are intended to serve as a model for industry codes. They take into account both the OECD Guidelines and the EU Directive. According to the MITI Guidelines, a manager should be appointed in each organisation to implement the Guidelines.[106] A "System of Granting Privacy Marks" that certifies enterprises abiding by industry codes (based on the MITI Guidelines) which required the maintenance of appropriate levels of privacy protection was established by the Japan Information Processing Development Center in April 1998. This system also ensures that consumers can easily distinguish between the different levels of personal-data protection offered by enterprises.

The *Electronic Network Consortium*[107] (ENC) has produced "Guidelines for Protecting Personal Data" (December 1997) which reflect the OECD Guidelines. They apply to anyone handling personal data in electronic networks and are intended to encourage service providers to take a uniform approach to the management and protection of personal data.

Electronic commerce business associations have also produced privacy codes of conduct. The *Cyber Business Association*, in consultation with the MPT, has produced voluntary "Guidelines for Protecting Personal Information in Cyber Business" (December 1997). Guidelines have also been produced by the *Electronic Commerce Promotion Council* (ECOM).[108] The *ECOM Privacy Issues Working Group* has issued "Guidelines Concerning the Protection of Personal Data in Electronic Commerce in the Private Sector" (March 1998) which are based on the MITI Guidelines, and contain special provisions for children by requiring the consent of parents or guardians. They are intended as a model for individual companies.

In terms of self-regulation by Internet Service Providers (ISPs), the *Telecom Services Association* (TELESA) has also developed a model Code of Conduct which includes provisions on privacy and the protection of personal data.[109]

In April 1998, Japan's Data Communications Association launched a Mark Granting System to certify telecommunications carriers and service providers which provide appropriate privacy protection in their handling of personal information.

MPT established "Guidelines on the Protection of Personal Data in Telecommunications Business" in 1991 which were revised in 1998. The Guideline stipulates five basic principles which telecommunications

carriers and ISPs should observe; collection limitation, use and disclosure limitation, security safeguards and individual participation and accountability. Six extra clauses were included which focus on issues peculiar to the telecommunications sector; traffic data, itemised billing and calling line identification, etc. Also in 1998, the Telecommunications Business Law was amended and a Petition System was established. Users can file complaints and petitions with MPT about telecommunications services charges, other conditions and their manner of operations, including handling of users' personal data. This is expected to work as a proper mechanism for individuals to redress privacy infringement. MPT established some other Guidelines including; "Guidelines for the Protection of Personal Caller Information in the Use of Caller Identification Services" (1996) and "Guidelines on Protection of Subscriber's Personal Information in Broadcasting" (1996).

Other self-regulatory privacy initiatives include the *Centre for Financial Industry Information Systems* which produced "Guidelines on the Protection of Personal Data for Financial Institutions" based on the OECD Guidelines.

In March 1999, the Ministry of International Trade and Industry established a Japanese Industrial Standard (JIS) entitled "Requirement for Compliance Program on Personal Information Protection" to standardise the level of protection of personal data in enterprises.

KOREA

Constitution

The Constitution of Korea stipulates that every citizen shall not have their right to confidentiality and freedom of privacy (Article 17), and freedom of communication (Article 18) infringed.

Laws

Public sector laws

The *Protection of Personal Information by Public Organisations Act* governs the protection of personal information in the public sector. The Act reflects the principles in the OECD Guidelines and obliges public organisations to act carefully and promote confidentiality in dealing with personal data. Citizens are given the right to access their own personal data and the opportunity to have corrections made.

Other laws with privacy provisions

The *Use and Protection of Credit Information Act* focuses on the protection of personal data in financial transactions. For example, the Act prohibits a financial institution from revealing or sharing personal/financial data without the data subject's written consent. Korea also has an Act on the *Protection of Confidentiality in Communications.*

Approach to privacy in the private sector

The Telecommunications Network Use Proliferation Act was amended in January 1999 to institutionalise the protection of personal data in the private sector, reflecting the principles in the OECD Guidelines. The revised Act, which will be in effect as of January 2000, authorises the Government to place specified restrictions on information and telecommunications service providers in case they abuse or misuse an individual's personal data.

Self-regulatory instruments

There are no private sector self-regulatory initiatives in Korea at the present time, although discussions are expected.

LUXEMBOURG

Laws

Comprehensive laws

The *Nominal Data (Automatic Processing) Act*[110] (1979) covers computerised and manual personal data of physical and legal persons held in both the public and private sectors. *The Data Protection Consultative Commission* (the *Commission consultative à la protection des données*) works under the auspices of the Minister responsible for data banks, it performs an advisory function. The Minister is also assisted by an oversight authority, the *autorité de contrôle.*[111] Breaches of the privacy legislation can be referred to a prosecuting authority by the Minister.

The 1979 Act provides criminal sanctions (imprisonment or fines) for breaches of its provisions.[112]

Other laws with privacy provisions

A number of sectoral regulations have been passed pursuant to the Act. For example, regulations have been passed with respect to police and medical data files.[113]

Implementation of the EU Directive

A parliamentary Bill has been drafted to implement the EU Directive.[114] It was introduced to the Chamber of Deputies on 8 October 1997.

MEXICO

Constitution

Articles 6 and 7 of the *Mexican Constitution* provide for the right to information. Article 16 states that private communications are inviolable and the law will provide criminal sanctions for acts which violate the freedom and privacy of such communications.

Laws

Federal laws

The *Federal District Penal Code* provides sanctions for breaches of privacy rights by public servants with respect to personal information collected and maintained by public authorities.[115]

THE NETHERLANDS

Constitution

A constitutional right to privacy is contained in Article 10 of the *Constitution of The Netherlands*.

Laws

Comprehensive laws

The *Wet bescherming persoonsgegevens* (WBP, Dutch Data Protection Act[116]) applies to both the public and private sectors, and covers computerised and manual records. The independent supervisory authority is the *College bescherming persoonsgegevens* (CBP, Dutch Data Protection Authority). Its task include advising the government on draft bills or other regulations, approving codes of conduct, complaints handling and investigation, and keeping a public register of notifications.

Under the Act, data subjects have several rights, such as the right of access, rectification, erasure or blocking of data. Data subjects also have the right to object to the processing. If a request by the data subject is refused by a data controller, there are several options. If the data controller is a public body, the data subject should first lodge an objection to the public body, and can then appeal to the administrative court. In case the data controller is a private body, the data subject may apply to the District Court for review. Before turning to the court, the data subject can lodge a complaint at the Data Protection Authority. The Authority has powers of investigation, upon request and at its own initiative, and administrative powers of enforcement. The Dutch Data Protection Act also provides for criminal sanctions for certain violations.

Other laws with privacy provisions

Sectoral privacy legislation takes two different forms. On the one hand, there are sectoral acts that create a comprehensive privacy regime and exclude the applicability of the general act, the WBP. Examples of this legislation are the legislation regarding police files [*Wet Politieregisters*, Wpolr, Police Registration Act (1990)], the Municipal Database (Personal Records) Act [*Wet gemeentelijke basisadministratie persoonsgegevens*, Wgba, (1994)], and the Judicial Documentation Act [*Wet justitiële documentatie* (1955)].

On the other hand, there is sectoral legislation that specifies a number of rules regarding privacy, and the WBP remains applicable to those elements that are not covered by the sectoral legislation. Examples are legislation concerning medical data [*Wet geneeskundige behandelingsovereenkomst*, Wgbo, Medical Treatment Information Act (1995)], the General Social Security Act [*Algemene bijstandswet*, (1995)], and the Trade Register Act [*Handelsregisterwet* (1996)].

Implementation of the EU Directive

Directive 95/46/EC was transposed into national law by an Act of 6 July 2000. This Act (*Wet bescherming persoonsgegevens*, WBP*)* entered into force on 1 September 2001, replacing the old Data Protection Act (*Wet persoonsregistraties*, Wpr), which dated from 28 December 1988. On the same date, the name of the supervisory authority changed from *Registratiekamer* into *College bescherming persoonsgegevens* (CBP).

It differs in some ways from the preceding Data Protection Act, though in general there is a great degree of continuity from the old to the new act. It applies to the processing of personal data by automatic and manual means. The law contains regulations on the following issues; conditions for lawful processing of personal data, codes of conduct of organisations, supply of information to and rights for the data subjects, and publicity of data processing to controlling organisations and a broader public. The law also includes legal protection governing liability of the data controller, international data transfers and the relationships with other laws. The role of the Data Protection Authority has largely remained the same, although it has gained new powers of enforcement.

After 1 September 2001, all new processings had to comply with the new provisions. There was a one-year transition period for existing processings, ending on 1 September 2002.

Regarding the implementation of EU Directive 97/66/EC, the most relevant piece of legislation containing sectoral rules on this topic is the Telecommunications Act of 19 October 1998 *(Telecommunicatiewet,* Tw*).*[117] This Act partly implements Directive 97/66/EC into Dutch law. The remaining issues will be dealt with together with the implementation of Directive 2002/58/EC. The Dutch Data Protection Authority advised on the draft for a revised Telecommunications Act in December 2002.

Self-regulatory instruments

The Dutch Data Protection Authority is a strong supporter of self-regulation. It regards public authorities and private organisations as important stakeholders in data protection. Both the old and the new law in the Netherlands embody provisions for developing codes of conduct as a vehicle for implementing self-regulation with a possibility to seek the DPA's approval. Twelve codes of conduct were formally approved under the old Data Protection Act that covered major sectors like banking, insurance, direct marketing, health, credit reporting agencies, and pharmaceutical research. These codes still enjoy considerable respect. Most of the existing codes are being revised to bring them into line with the new Dutch Data Protection Act. Under the new act, codes of conduct for the pharmaceutical and the financial sector have been approved.

The Dutch Data Protection Act also provides for the possibility to appoint an in-company data protection officer, that supervises the processing of personal data. The data protection officer enjoys legal protection in order to ensure his independence. Since September 2001, approximately 100 organisations, ranging from ministries and municipalities to schools, hospitals and big and medium-sized companies, have appointed data protection officers.

NEW ZEALAND

Laws

Comprehensive laws

The Privacy Act 1993 applies to computerised and manual "personal information" held by almost all public and private sector organisations in New Zealand. The core of the Act is a set of 12 *Information Privacy Principles* (IPP's) which are based on the OECD Guidelines. The Act also includes rules on data matching between government agencies.[118]

The Act establishes the position of a *Privacy Commissioner*[119] (an independent officer of the Crown) who has the power to investigate and mediate complaints. The Commissioner may issue sectoral *Codes of Practice* which are enforceable in the same way as the IPP's.[120]

Neither the IPP's nor specific Codes of Practice create directly enforceable legal rights. Rather an alleged breach may form the basis of a complaint to the Commissioner who has broad powers of investigation and conciliation. Complaints which cannot be settled by consent are referred to a *Complaints Review Tribunal*[121] which has broad relief-granting powers.

Other laws with privacy provisions

Issue specific laws with privacy provisions include the Official Information Act 1982, the Local Government Official Information and Meetings Act 1987, the Electoral Act 1993 and the Domestic Violence Act 1995.

Self-regulatory instruments

In terms of the Internet industry, the *Internet Society of New Zealand* has developed an "Internet Service Provider Code of Practice".[122]

The *Privacy Act* also provides for the development of Codes of Practice which have the force of law. A Code may determine compliance and complaints procedures and may be more or less stringent than the IPP's but, once approved by the Privacy Commissioner, it replaces those principles for that specific agency, type of information, activity or industry group. Examples of Codes that have been developed pursuant to the Act are the *Health Information Privacy Code 1994*[123] and the *Justice Sector Unique Identifier Code 1998.*[124]

NORWAY

Laws

Comprehensive laws

Norway's legislation for the protection of personal data [Act of 14 April 2000 No. 31 relating to the processing of personal data (Personal Data Act)] covers both the public and private sectors and applies to manual and computerised records on natural and legal persons. Subsequent amendments to the Act cover direct postings, telemarketing and consumer credit information. This Act also covers camera surveillance, direct postings, telemarketing and consumer credit information. There are also two more legal acts specific covering aspects of protection of personal data: Act of 18 May 2001 No. 24 on Personal Health Data Filing Systems and the Processing of Personal Health Data (Personal Health Data Filing System Act) and act of 16 July 1999 No. 66 on the Schengen Information System (SIS).

The Act introduces a central registration system which is administered by the *Data Inspectorate* (the *Datatilsynet*).[125] The Data Inspectorate enforces the Act that includes inspections of practice in the companies. The Privacy Appeals Board shall decide appeals against the decisions of the Data Inspectorate, pursuant to Act of 14. April 2000 No. 31 relating to the processing of personal data (Personal Data Act) section 42, fourth paragraph. The Board is an independent administrative body subordinate to the King and the Ministry.

Under the Act, individuals have the right to inspect personal data, to request that corrections be made and to prevent their names from being used in the distribution of advertising. There is also special protection for sensitive data. Wilful or negligent violations of the conditions of a licence, or the terms of the Act, are punishable by fines or imprisonment. Persons suffering as a result of breach are entitled to compensation from the violator.

Other laws with privacy provisions

There are many provisions in Norwegian legislation which relate to protection of privacy. These include; the Telecommunication Act which concerns the protection of privacy in the telecommunication sector, and Rules of professional secrecy in the Public Administration Act and the National Register Act, which both limit government use of personal data.

Other instruments to protect personal data

The Basic Agreement between the Norwegian Confederation of Trade Unions (LO) and the Confederation of Norwegian Business and Industry (NHO) contains provisions of protection of personal data. The Agreement has special provisions regarding storing and use of personal data in private enterprises.

Implementation of the EU Directive

Norway has fully implemented the Directive 95/46 in national legislation. Self-regulatory instruments

The Personal Data Act, proposed that individual businesses and professional sectors should develop their own codes of conduct concerning personal data. In this regard the Committee made reference to Article 27 of the EU Directive on data protection, and the 1980 OECD Guidelines.

POLAND

Constitution

Article 51 of the *Polish Constitution* confers rights of protection for personal data.[126]

Laws

Comprehensive laws

The *Act on the Protection of Personal Data*[127] (1997) applies to manual and electronic data files and conforms with Convention 108 and the EU Directive. The data protection authority established under the Act is the *General Inspector for Personal Data Protection*. The Act contains a number of criminal sanctions (fines or imprisonment).[128]

Other laws with privacy provisions

An Order of the *Ministry of Health* in 1993 includes clauses protecting medical data.

PORTUGAL

Constitution

Article 35 of the *Portuguese Constitution* confers constitutional rights to privacy.

Laws

Comprehensive laws

The *Protection of Personal Data Act* (1991)[129] covers computerised data of natural persons, is applicable to both the public and private sectors and provides for a central registration system. The Act also creates a *National Commission for the Protection of Automated Personal Data* (the *Comissao Nacional de Proteccao de Dados Pessoais Informatizados*). The Commission is responsible for administering the registration system, hearing complaints[130] and enforcing privacy rights under the Act and the Constitution. The Commission also oversees the matching of computerised personal files and its authorisation is required for transborder flows.

The Act creates a right of access for data subjects along with a right of correction/erasure.[131] Violations of the Act,[132] as well as the Constitution, are criminal offences.

Other laws with privacy provisions

There are a number of laws and regulations containing data protection provisions in Portugal. These include the Law on Computer Crime (1991),[133] regulations establishing institutions such as the Registry of Non-Donors of Human Organs[134] and the Identity Card Centre,[135] and regulations controlling the databases operated by the Gendarmerie,[136] the Border and Foreign Services[137] and the Criminal Police.[138]

Implementation of the EU Directive

In September 1997 a number of changes were proposed to Article 35 of the Constitution to conform with the principles of the EU Directive. In addition, a new data protection law has been approved by the Government and is currently before the Portuguese Parliament.

SLOVAK REPUBLIC

Laws

Comprehensive laws

The Convention 108 with annexes entered into force in the Slovak Republic on 1 January 2001. The Annexe protocol to the Convention No. 108, concerning body of guidance and Transborder Flows of Personal Data was ratified in July 2002. The new Act Nr. 428/2002 on Protection of Personal Data was adopted for provision of independent functions practise supervisory bodies for Protection of Personal Data. This Act entered into force on 1 September 2002. In connection with this act an autonomous, independent governmental body, The Office for Protection of Personal Data, was established.

In March 2002 the Act Nr. 215/2002 on Electronic signature was adopted by Parliament. It entered into force on 1 September 2002. The Act covers the relationships in connection with executing and using electronic signatures, rights and responsibilities of individuals and legal entities when using electronic signatures, plausibility and protection of electronic documents signed with electronic signatures.

SPAIN

Constitution

Article 18.4 of the *Spanish Constitution* states that "the law shall limit the use of data processing in order to guarantee the honour of personal and family privacy of citizens and the full exercise of their rights".

Laws

Comprehensive laws

The *Law on the Regulation of the Automated Processing of Personal Data*[139] (1992) covers computerised records in the public and private sectors. Its implementation is overseen by an independent public authority, the *Data Protection Agency*[140]. The Agency provides prior authorisations for the creation of databases, receives complaints and may make orders regarding public sector violations of the Law. It recently produced "Recommendations for Internet Users" which warn of the privacy risks associated with the Internet.

The Law provides that sanctions should be determined according to the nature and size of the violation.[141]

Other laws with privacy provisions

There is a Spanish Law on public statistics[142] which contains privacy provisions.

Implementation of the EU Directive

Work on revising the privacy legislation to meet the requirement of the EU Directive is underway.

Self-regulatory instruments

The *Spanish Association of Electronic Commerce* (which is part of the *Spanish Direct Marketing Association*) has a Code of Conduct on Internet privacy.[143] The Code advises its members of the privacy implications of operating on the Internet, specifying that users should be informed of their rights of access, rectification and deletion.

SWEDEN

Constitution

The Swedish Constitution (The Freedom of the Press Act[144]) guarantees the right of individuals to have access to documents and data held by public authorities. Furthermore, the Instrument of Government[145] provides 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.

Laws

Comprehensive laws

In April 1998, the Personal Data Act[146] was adopted by Parliament. The Act, which entered into force on 24 October 1998, implements the EU Data Protection Directive in Sweden. The Act represents a legal framework for all processing of personal data and is supplemented by regulations of the Government[147] and the Data Inspection Board. However, the provisions of the Act do not apply, *inter alia*, to the extent that they would contravene the provisions concerning the freedom of the press and freedom of expression contained in the Freedom of the Press Act and the Fundamental Law on Freedom of Expression.[148]

The Act confers on the Data Inspection Board a supervisory and advisory role.

The penalties for violating the Personal Data Act primarily comprise damages in favour of the data subject suffering loss.

Other laws with privacy provisions

Swedish laws containing privacy provisions include the *Credit Information Act*, the *Debt Recovery Act* and the *Official Statistics Act*.

Self-regulatory instruments

The Swedish Direct Marketing Association is engaged in self-regulatory activities.

SWITZERLAND

Laws

Federal laws

The *Federal Law on Data Protection* (1992) (FLDP)[149] covers both computerised and manual data concerning natural and legal persons in the federal public sector and the private sector. The *Federal Data Protection Commissioner*[150] (appointed by the *Federal Council*) oversees the application of the law by federal authorities, and acts as an ombudsman for the handling of personal data in the private sector. All federal data registers must be registered with the Commissioner, but private organisations are only required to register data collections in limited circumstances.[151] The Commissioner's duties include assisting Federal and Cantonal privacy bodies and examining the extent to which foreign data protection regimes provide comparable protection. The Commissioner can also conduct investigations (on its own initiative or at the request of a third party) and issue recommendations. The Commissioner has a mainly consultative function in the private sector. It may also act as an arbitration and appeal body.[152]

The FLDP reflects the basic principles of the OECD Guidelines. Sensitive data receives special protection. Transborder data transfers are prohibited under the FDLP unless adequate data protection can be assured, and the prior notification of transfers (to the Commissioner) is required in some circumstances.

Data subjects may seek the usual remedies of the Swiss Civil Code,[153] such as injunctions and compensation orders, for violations of the FLDP. Violations are also punishable by fine or detention.

Other federal laws with privacy provisions

A number of Swiss laws include privacy protection clauses, in particular: the *Telecommunications Law*; the law on *Employment Contract Provisions*; the law on *Federal Statistics*; and the *Swiss Criminal Code*. There is also a 1993 Ordinance regarding *Professional Secrecy in Medical Research*.

Cantonal (state) law

The activities of Cantonal authorities are governed by Cantonal law. Most of the Swiss Cantons have introduced data protection laws which apply to these agencies. The applicable rules are generally similar to those at the Federal level and include the establishment of data protection bodies.

Self-regulatory instruments

Instruments relating to online privacy

A working group of the *Office Fédéral de la Justice* has formulated recommendations for Internet access providers called the *Internet Charter*. The Charter includes recommendations on legal issues such as service provider liability and the disclosure of data to third parties.

Other initiatives

Industry codes of practice provide additional guidance in specific sectors, such as the medical profession, direct marketing and market research. There are well-known confidentiality obligations in the fields of banking, insurance and pensions privacy.

TURKEY

Laws

Turkey has a draft law on Data Protection which applies to both public and private sector data processing entities. It has yet to be approved by the Turkish Parliament. The draft law incorporates the basic principles of the OECD Guidelines and Convention 108, and establishes an autonomous *Authority for Data Protection*. The Authority is responsible for supervising the application of the law.

Under the draft law, individuals will have rights to receive information whenever their data are collected, to have access to data of which they are the subject, to correct inaccurate data and to object to certain types of data processing.

Work on electronic commerce was initiated in Turkey in February 1998, following a decision taken by the Science and Technology High Board (STHB). Three working groups under the Electronic Commerce Co-ordination Committee have handled the studies. An initial Report prepared by these groups was submitted to the STHB in June 1998. The Report covers the existing barriers to e-commerce in Turkey and makes recommendations, which include the development of authentication and certification processes to eliminate these obstacles properly. The next step will be the development of an action plan for submission to STHB. This Study will consider the issue of jobs, timing and entities to be assigned to improve the legal, technical and financial infrastructure which e-commerce needs to develop.

UNITED KINGDOM

Laws

Comprehensive laws

The United Kingdom's *Data Protection Act 1984*[154] applies to automatically processed personal data relating to living individuals in both the public and private sectors. The Act gives rights to individuals, about whom data are recorded, including a right of access to their personal data and a right to have any inaccurate data corrected or deleted. If an individual suffers damage caused by the loss, unauthorised destruction or unauthorised disclosure of information about themselves, or through that information being inaccurate, they can seek compensation through the courts.

The Act established an independent supervisory authority known as the *Data Protection Registrar.*[155] The Registrar's functions include establishing and maintaining a register of those who process personal information. Failure by a data user to register can give rise to criminal liability.

The Act sets out eight Principles of fair information practice. The Registrar considers complaints made about breaches of the Act and can serve notices on registered persons requiring them to take specified steps to comply with the Act. Failure to comply with such a notice is an offence.

The Registrar is also charged with promoting data protection compliance, including encouraging the development of industry-based codes of practice. These codes aid the interpretation of the law. The Registrar also issues guidance notes; including on the recently published "Data Protection and the Internet".

Other laws with privacy provisions

A number of statutes in the United Kingdom have implications for data protection; these include: the Financial Services Act 1986, the Human Fertilisation and Embryology Act 1990,[156] the Charities Act 1993[157] and the Criminal Justice and Public Order Act 1994.[158] The Government has proposed a Freedom of Information Bill which, if enacted, would extend rights of access to information, and also contain exemptions on privacy and other grounds.

The European Convention of Human Rights (ECHR)[159] has recently been embodied in national legislation in the form of the Human Rights Act 1998.[160] The Act received Royal Assent on 9 November 1998 but is not expected to come into force before 2000. The Act adopts Article 8 of the ECHR providing a "right to respect for private and family life".

Implementation of the EU Directive

The Data Protection Act 1998[161] which received Royal Assent on the 16 July 1998 was enacted to implement the EU Directive on data protection. Much of the detail of the new law will be contained in secondary legislation. The new law will be brought into force at the end of June 1999, or as soon thereafter as the Government finds it possible to do so.

The Act broadens the scope of current legislation by bringing personal data contained within structured manual filing systems within the scope of the Act. The definitions of "processing" and other terms have been amended to reflect the definitions found in the EU Directive. The 1998 Act also provides new rights for data subjects, in particular, to prevent their data being used for direct marketing and to object to important decisions concerning them being taken by automatic means but more generally to

provide a right to compensation for damages arising from any breach of the new law. When the Act comes into force the Data Protection Registrar will in future be known as the *Data Protection Commissioner*.

The *British Standards Institute* is working with the Data Protection Registrar to prepare a data protection compliance programme in preparation for the implementation of the EU Directive.

Self-regulatory instruments

Instruments relating to online privacy

The *Internet Service Providers Association (UK)*[162] has developed a Code of Conduct, which is voluntary for the first 12 months, and thereafter becomes obligatory for all members. The Code provides guidance on registering with the Data Protection Registrar. It also encourages members to notify users as to the purposes for which personal information are collected and to give the user an opportunity to prevent such usage.

Other initiatives

A number of other industry associations have produced codes of conduct that include data protection provisions.[163]

UNITED STATES

Constitution

The US Constitution does not explicitly mention a right of privacy. However, case law has recognised that the Constitution confers such a right with respect to government restrictions on certain activities or invasions of physical privacy.

Laws

Federal sectoral laws

The United States does not have federal comprehensive legislation or mandatory "baseline" privacy requirements. Instead, the United States relies on a combination of self-regulation, sector-specific legislation, educational outreach and enforcement authority. For example, the Federal Trade Commission (FTC) enforces its authority to prevent unfair and/or deceptive trade practices in commerce and other federal agencies enforce privacy provisions applicable to the sectors that they regulate, such as health care, transportation, and financial services.

Congress has adopted legislation to protect certain highly sensitive personal information, such as children's information, financial records, and medical records. Below are some of the most recently enacted laws:

- **Children's information.** The Children's Online Privacy Protection Act of 1998 (COPPA) requires sites aimed at children under the age of 13 to obtain verifiable parental consent before they gather and use personal information received from the children. The FTC issued rules to implement this Act in April 2000 to require that sites get parental permission via mail, fax, credit card, or digital signature before disclosing a child's personal information to a third party.

- **Financial information.** The Financial Services Modernization Act of 1999 (commonly known as Gramm-Leach-Bliley Act or GLBA) requires banks and other financial institutions that share or sell confidential customer information to provide clearly stated privacy policies and provide consumers the right to opt-out of third-party information sharing.

- **Medical records.** The Department of Health and Human Services (HHS) issued new medical privacy regulations on December 20, 2000, pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). These rules include standards to protect the privacy of individually identifiable health information communicated electronically, on paper, or orally. In July 2001 HHS issued its first guidance to clarify certain provisions of the rule, such as whether relatives can pick up a prescription for a patient.

In addition to these Acts, Congress previously enacted sector-specific legislation regarding: financial privacy [Right to Financial Privacy Act (1978); Fair Credit Reporting Act (1970, last amended 1996)]; privacy of communications [Telephone Consumer Protection Act (1934, amended in 1991, last amended 1994); Telecommunications Act of 1996; Electronic Communications Privacy Act (1986)]; and other miscellaneous privacy provisions [Driver's Privacy Protection Act of 1994 (amended in 1996); Video Privacy Protection Act of 1998; Cable Communications Privacy Act of 1984 (last amended 1992); Privacy Protection Act of 1980; Family Education Rights and Privacy Act (1974, amended in 2000)].

The use of personal information held by federal government agencies is regulated by the *Privacy Act* (1974)[164] which establishes *fair information principles* for handling personal data. The *Office of Management and Budget* is responsible for overseeing the Act. The Privacy Act provides data subjects with a civil right of action which may result in monetary damages and/or injunctive relief. The Act also provides criminal penalties for knowing violations of the Act.

State laws

A number of state constitutions include a right to privacy. States generally follow the federal sectoral model and enact privacy enhancing statutes on a sectoral (industry by industry) basis. However, a few states, namely Minnesota and California, have recently enacted, or are considering, more comprehensive privacy laws. The level of protection varies from one state to another.

Approach to privacy regulation in the private sector

The US government believes that private sector-developed and enforced codes of conduct are an effective way to protect privacy online without creating a bureaucracy which could stifle the growth of electronic commerce. The US government encourages the development of industry codes of conduct to protect online privacy. While various government agencies, including the Department of Commerce and the FTC, have worked with industry associations on their development of comprehensive and enforceable codes of conduct, the US government does not officially endorse any particular code of conduct. Reports by government bodies and statements by officials include:

- "Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information" (June 1995) by the *Information Infrastructure Task Force* (IITF) [165] which outlined a set of *Privacy Principles* based upon the OECD Guidelines.

- "Privacy and the National Information Infrastructure: Safeguarding Telecommunications-Related Personal Information" (October 1995)[166] by the *National Telecommunications and Information Administration* (NTIA) (part of the *Department of Commerce*) which recommended that telecommunications and information service providers put into practice privacy policies that

notify users of their information practices and obtain user consent for the use of personal information.

- "Options for Promoting Privacy on the National Information Infrastructure" (April 1997) by the *Information Policy Committee* of the IITF which sets out options for the implementation of online privacy protection including the creation of a federal privacy entity.
- "Individual Reference Services: A Report to Congress" (December 1997) by the FTC which discussed the benefits and risks of look-up service databases used to locate, identify, or verify the identity of individuals. The report also discussed the self-regulatory principles adopted by industry members.
- "Elements of Effective Self-Regulation for Protection of Privacy" (January 1998)[167] by NTIA (US Department of Commerce) which outlines actions which the private sector can take in order to meet an acceptable level of privacy protection.
- "Privacy Online: a report to Congress" (June 1998)[168] by the FTC which emphasises the importance of notice, choice, security and access to privacy protection, suggests that incentives are needed to spur self-regulation and ensure widespread implementation of basic privacy principles, and recommends the enactment of legislation to protect children's online privacy. In testimony before the *Subcommittee on Telecommunications, Trade and Consumer Protection* in July 1998, the Chairman of the FTC recommended that unless effective and broad-based self-regulation is in place by the end of 1998, legislation establishing statutory standards should be enacted authorising enforcement by a government agency.[169]
- "US Government Working Group on Electronic Commerce: First Annual Report" (1998) which describes progress made toward the establishment of self-regulation for privacy, and suggests an appropriate government role in protecting privacy."
- *Protection Consumers' Privacy: 2002 and Beyond*, Remarks of FTC Chairman Timothy J. Muris, at the Privacy 2001 Conference, Cleveland, OH, 4 October 2001, www.ftc.gov/speeches/muris/privisp1002.htm.

Self-regulatory instruments

Instruments relating to online privacy

A number of self-regulatory initiatives have been developed in the United States, including private sector codes of conduct and the establishment of "seal programs." Various industry-led associations have formed to develop private sector codes of conduct to protect online privacy. These include:

- The *Privacy Leadership Initiative (PLI)*, composed of more than 20 companies and associations, is also developing an "etiquette" model practices for the exchange of personal information between businesses and consumers.
- The *Network Advertising Initiative*, an example of a sector-specific code of conduct, was created by the leading online advertisers engaged in "online profiling." This initiative sets forth self-regulatory principles for online advertisers to protect consumers' privacy while engaging in online advertising.
- The *Information Technology Industry Council*[170] which has adopted principles for the protection of personal data in electronic commerce which serve as a foundation upon which member companies can build their own privacy policies.[171]

- The *Interactive Services Association* which has published voluntary "Principles on Notice and Choice Procedures for Online Information Collection and Distribution by Online Operators" (June 1997) based on a regime of notice and opt-out.
- The *Online Privacy Alliance*[172] (formed in June 1998 by 50 US Internet-related companies and associations) which has produced Guidelines for Online Privacy (which urge Alliance members to adhere to the OECD Guidelines and use third party privacy seal programmes such as *TRUSTe* and *BBBOnLine*), and a set of guidelines for safeguarding children's privacy; and
- The *American Electronics Association* which has announced (June 1998) self-regulatory action plans including the adoption of a set of privacy protection elements for implementation by member companies.

Seal programs

"Seal programs," such as those operated by BBBOnline, TRUSTe and the Direct Marketing Association (DMA), are also becoming more widely used by a wide variety of online companies. These seal programs are designed to ensure that a company's practices comply with fair information practices and that the online companies will engage in a dispute resolution mechanism. TRUSTe, BBBOnline and the DMA now have several thousand client-companies between them.

Other initiatives

Other self-regulatory initiatives include:

- The establishment by the *Direct Marketing Association*[173] of voluntary guidelines and the development of *Online Guidelines* based on the principles of disclosure and opting-out.
- The publication by the *Children's Advertising Review Unit* of the *Council of Better Business Bureau* of "Self-Regulatory Guidelines for Advertising to Children".[174] The Guidelines require "reasonable efforts" be made to provide notice and choice to parents when information is collected from children online.
- The development by the Coalition for Advertising Supported Information and Entertainment of a statement of Goals for Privacy for Marketing in Interactive Media.
- The agreement between the *Individual Reference Services Group* (IRSG) and the FTC in December 1997 to abide by a set of *IRSG Principles* which address the availability of information obtained through computerised database services which may be used to locate, identify or verify the identity of individuals. Firms must submit to an annual third party audit with the results made public.

II. Mechanisms to implement and enforce privacy principles on global networks

There are various practices, techniques and technologies which are used, or are being developed, to implement and enforce privacy principles in networked environments. These different mechanisms are highly interrelated, many are based on recent technological developments, and some blur the traditional distinctions between setting, implementing and enforcing privacy guidelines. Some allow users to take charge of their own personal data protection and privacy (for example, by blocking the transfer and collection of header information and click-stream data), others are implemented by data controllers (for example, by digitally labelling a Web site's privacy practices), and others may be facilitated by governments and/or private sector organisations (for example, by creating model clauses for transborder data flow contracts).

This part of the Inventory categorises the various mechanisms for the protection of privacy on global networks according to whether their purpose is:

- Minimising the disclosure and collection of personal data.
- Informing users about online privacy policies.
- Providing users with options for personal data disclosure and use.
- Providing access to personal data.
- Protecting privacy through transborder data flow contracts.
- Enforcing privacy principles; or
- Educating users and the private sector.

A. Minimising the disclosure and collection of personal data

Users of global networks can act with relative anonymity by minimising the amount of personal data they disclose and/or allow to be collected[175]. This is an important means of protecting privacy. To help preserve online anonymity, mechanisms are available which: *(i)* empower users to restrict the automatic disclosure and collection of Web-browsing data; and *(ii)* reduce the need for personal data to be disclosed voluntarily.

1. Restricting or eliminating the automatic disclosure and collection of personal data

As discussed in the general introduction, header information and click-stream data may be disclosed whenever a Web site is visited and cookies are often used to facilitate the collection of such data. In general, a user's level of anonymity may be increased by restricting the creation of cookies, or by blocking the transfer, and collection, of automatically generated data (header information, e-mail headers and click-stream data) from the user's computer. Both these techniques empower users to take control over their own privacy.

(a) Management of cookies

Since cookies can be used to associate a unique code with a particular user, one approach to preserving anonymity while using the Web is to allow individuals to limit or prevent the creation of cookies. Methods which may be used include the following:

- The most recent versions of *Microsoft Explorer* and *Netscape Communicator* allow users to set their preferences to be warned when a server tries to set a cookie and be given the opportunity to refuse its creation; and
- Software applications have been developed to automatically delete unauthorised cookies (some of these applications can also control the header information which is transferred from the client to the Web site). Examples include the *Internet Junkbuster Proxy*[176] and the *Cookie Crusher*.[177]

These technologies require a considerable degree of user sophistication and they generally do not prevent the server from retrieving basic header information from the user's browser. However, further development of the technologies may make their use more streamlined and effective.

(b) Blocking the transfer and collection of automatically generated data

Mechanisms are available to block the transfer and/or collection of automatically generated data, such as e-mail headers, header information and click-stream data.

"Anonymous re-mailers" allow e-mail messages to be sent without revealing the identity of the sender. Some, such as *Hotmail*[178] and the *Freedom Remailer*, run by the *Global Internet Liberty*

Campaign,[179] operate through Web pages where an e-mail is created and sent without any information identifying the sender. Other re-mailers are designed to receive an e-mail message from one party, re-address it and send it to a second party. In the process, header information that would identify the sender is removed. Examples include the re-mailers at *Replay* and *Nymserver*. Such re-mailers offer varying degrees of protection to prevent the identity of the sender of an anonymous e-mail being determined by eavesdropping on the messages being received and sent via the re-mailer and making matches based on, for example, their length and timing information (Goldberg *et al.*, 1997). Many anonymous re-mailers have been forced to close down because of abuses, such as offensive messages and mass mailings.

An "anonymising intermediary" may be used to prevent a Web site automatically collecting header information about the user,[180] associating click-stream data with a particular user or setting cookies on the user's computer. The intermediary is a Web server which operates between the user and the rest of the Web. When the user wishes to view a Web page he or she requests the page from the intermediary. The intermediary retrieves the page and passes it back to the user. Since the user is never directly connected to the site being browsed, no header information about the user is passed on, nor is the Web site able to set a cookie on the user's computer. An example of such a service is the *Anonymizer*.[181]

Issues which have been raised about the use of anonymising intermediaries include the need for the intermediaries to follow good data practices, and the risk of abuses of anonymity.[182]

2. Reducing or avoiding the need for personal data disclosure

One of the reasons that personal data are requested on global networks is to prove that a user is eligible for a certain transaction or that payment details are genuine. Mechanisms are being developed which, if adopted by users and online businesses, will allow for the verification of such details without requiring the disclosure of personal information.

(a) Anonymous payment systems

Some payment mechanisms cause more data to be revealed than others. In the off-line world the most anonymous means of payment is cash. Since the value of cash is inherent and irrefutable, recipients do not require additional assurances of authenticity. In contrast, other payment mechanisms, such as credit cards, often require the disclosure of personal data (such as the name and billing address of the payor) as a means of authenticating the payment. The facility to engage in cash-like transactions in the online world increases user anonymity, and limits the ability for header information and click-stream data to be linked to a real world identity.

A number of companies are developing cash-like payment mechanisms for use on global networks.[183] An example is *Mondex*.[184] Here funds are stored in a "smart card"[185] and transactions are carried out directly between the parties without the transaction being reported to a central computer. For security and practical reasons, rolling audit trails are held on each individual card and with retailers. These trails can be revealed to resolve disputes, to correct failed transaction or if required by legal authorities. In normal transactions, however, an individual's privacy is protected because the retailer does not have access to the bank information which links an individual's name to their Mondex card reference number.

As with payment systems in the off-line world, electronic payment mechanisms do have limitations. First, they are subject to network externalities and will only be practicable when they are accepted by a critical mass of merchants. Second, personal identity information may still be revealed if, for example, a name and address are supplied so a product can be shipped to the purchaser or if the merchant is able to automatically collect identity revealing information such as the user's e-mail address. Finally, some commentators fear that anonymous payment mechanisms may be used to facilitate money laundering,

fraud and tax evasion. However, these payment systems constitute an important tool for protecting privacy, especially when used in conjunction with other technologies and privacy policies.

(b) Digital certificates

Another potential means of facilitating "faceless" anonymous transactions across global networks is the use of "digital certificates" based on public key cryptography techniques to establish personal attributes without revealing the party's true name or other identification information (Froomkin, 1996).

Digital certificates issued by a trusted source, such as a "certification authority", can provide independent verification of information such as identity and transaction details. In the context of minimising the disclosure of personal data and preserving anonymity on global networks, digital certificates can be issued to establish personal attributes such as age, residence, citizenship, registration to use a service or membership in an organisation without revealing the transacting party's identity. Such certificates may reduce, or avoid, the need for personal data to be disclosed where the important issue is not who a party is, but whether he or she possesses a certain characteristic. For example, a merchant selling age-sensitive products in the electronic environment may be satisfied by a digital certificate which states that a particular consumer is not underage without needing to know the consumer's actual identity.

The use of digital certificates for establishing personal attributes raises a number of issues which may require further consideration, such as the problem of attributes which change over time, fraud, and the importance of certification authorities, which may hold large amounts of personal data, following good privacy practices.

(c) Anonymous profiles

One of the reasons why Web sites collect data about users and their browsing habits is to develop profiles which can be used to facilitate the targeting of advertising, editorial and commercial content to individual visitors. However, this may be accomplished by using "anonymous profiles" which reveal the desired information about browsing habits, but do not contain any personally identifying information. For example, *Engage Technologies*[186] has created a database of 16 million Web-user profiles by using cookies to assign a unique numerical identifier to each visitor of an "Engage-Enabled" Web site. Other companies which run similar systems include *DoubleClick*[187] and *Clickstream.*[188]

A number of privacy concerns have been voiced about such systems on the basis that, although the profiles are in a sense anonymous, a large quantity of data is nonetheless collected which can be sold on a commercial basis, affect future browsing sessions and, potentially, be linked to the user's real identity[189] at a later date.

B. Informing users about online privacy policies

There is a balance between benefit from anonymity and the disclosure of personal information in order to participate fully in the wide range of interactions, relationships, and communications available on international networks. Also, many users will not have the knowledge, or be prepared to make the effort to keep their personal data private.

The percentage of Web sites which currently include statements about their privacy and personal data practices is still growing.[190] Various privacy bodies (such as, *TRUSTe* [191] and *BBBOnLine*[192]) and trade associations (such as, the *Online Privacy Alliance*[193] and the *American Electronics Association*[194]) promote appropriate disclosure practices and common standards for privacy protection. For example, in the TRUSTe licensing programme participating sites must, at a minimum, declare their policies with respect to what information is gathered, what is done with that information, with whom is it shared, and the site's

"opt-out" policy.[195] One important factor in determining whether or not users trust Web sites to follow their announced privacy policies is the mechanisms available for ensuring compliance with these policies and providing redress if they are breached. These mechanism are discussed below.

The ways in which a Web site can inform its visitors about what (if any) personal data is being collected and how it will be used include: *(i)* posted privacy policies; *(ii)* the terms and conditions of online agreements; and *(iii)* digital labelling.

1. Posted privacy policies

The simplest way for an organisation engaged in online activities to declare its privacy policy is via a specific page on their Web site. The information contained in Web site privacy policies should reflect the OECD Guidelines and could include:[196] who the organisation collecting the data is and how they may be contacted; what information is being collected and how; how the collected data will be used; what choices the user has regarding the collection, use and distribution of the data; what security safeguards are used; how data subjects can access their information and have corrections made; what redress is available for violations of the policy; whether there any applicable privacy laws or codes of conduct; whether any auditing or certification procedures are in place; and whether any technologies are used to enhance privacy protection. Privacy policies are also sometimes found within the Frequently Asked Questions (the FAQs) or "Help" sections of a Web site.

To supplement the information provided in such a statement some Web sites offer hypertext links to direct visitors to information about privacy issues, privacy organisations and technical issues such as cookies. Access to a privacy policy may also be facilitated by providing hypertext links from convenient locations, such as the site's homepage and any pages from which personal data are requested, and by including "privacy" in the keyword index if the site has an internal search engine. The development of well-recognised "privacy icons", with hypertext links to Web site privacy policies, can also improve the accessibility of these policies. Such icons may serve additional functions, such as signalling that a site's privacy policy and information practices meet the requirements of a third party certifier.

2. Terms and conditions

A Web site may include its privacy policy as a part of the terms and conditions which apply between the site and its visitors. For example, where a Web site requires the user to accept some form of registration agreement to gain access to non-public portions of the site, a privacy clause is often included.[197] Like the other means of notification, privacy clauses in online terms and conditions vary widely as to their scope and the amount of privacy protection afforded to the user.

3. Digital labels

"Digital labelling" of privacy practices can provide an alternative or complementary means of notification. The basic idea is that a uniform "vocabulary" for Web site information practices, developed by a particular online community or organisation, would be used to describe the practices of individual sites. The description would take the form of a label included in the header of a Web page and readable by the user's browser software.

The *Platform for Privacy Preferences* project (P3P)[198] takes this approach. P3P is being developed by the World Wide Web Consortium (W3C) and is based on their *Platform for Internet Content Selection* (PICS) framework for labelling Web sites[199]. The goal of P3P is to allow Web sites to simply express their privacy practices over the collection and use of personal data and to enable users to specify their own preferences.[200] The privacy vocabulary being developed currently includes a list of data categories and data practices relating to, for example, the purposes for which data are used and disclosed, the ability of an

individual to access and correct stored data and the identity of the person to whom problems should be addressed[201]

The interaction between the privacy preferences of the site and the user is mediated by P3P. Sites with practices which fall within a user's preference set will be accessed "seamlessly". Otherwise, users will be notified of a site's practices and have the opportunity to agree to those terms, to be offered new terms, or to discontinue browsing that site.

C. Providing users with options for personal data disclosure and use

The interactive nature of global networks may be used to provide users with options regarding what information they are prepared to disclose and how it will be used.

1. Optional data fields and click-box choices

Some Web sites offer choice by collecting data through online forms which distinguish between obligatory and optional data fields, and which display "click boxes" giving visitors options as to how information supplied may be used. For example, obligatory data might include identification and payment information required for a transaction between the parties, while optional data might correspond to the user's age, sex, occupation and various personal preferences. In terms of use options, visitors may be given boxes to click on which will determine whether their data may be used for marketing purposes and/or passed to third parties.

A similar approach to allowing individual control over personal data disclosures has been developed by companies in the business of providing personal profiles to other Web sites. *Firefly* is an example of such a system. A Firefly user creates a "passport" which contains the information that he or she is willing to divulge on the Web. The passport, which is in effect a personal profile of likes and dislikes, is then instantaneously made available to participating sites that the user visits. *MatchLogic*[202] operate a similar system. A unique random number is assigned, using a cookie, to each user visiting one of its sites.[203] This number is used to track click-stream data relating to, for example, the kinds of advertisements viewed.

2. Online negotiation of privacy standards through digital labels

Digital labelling and automated filtering, which were discussed above, may also be used to give a user new options when a Web site's standard privacy practices are not consistent with the privacy preferences that are set on his or her browser software. This would constitute a simple form of online negotiation.

3. "Opting-out"

Controlling the use of personal data after collection

To allow users to express a change of mind over how their data may be used, some Web sites allow a control decision to be conveyed by e-mail, regular mail or telephone.

Preventing the receipt of unsolicited e-mail advertising

Various technologies and practices are also available to prevent the receipt of unsolicited e-mail advertising. One mechanism is for user's to adopt filtering tools to block e-mail messages originating from known bulk e-mail distributors. Another practice is to allow the recipient of an unsolicited bulk e-mail to reply to the sender and request that no more e-mails are sent to that address. A broader proposal is to develop an "E-mail Preference Service" (an e-MPS) or "E-mail Robinson List".[204] An e-MPS would allow consumers who do not wish to receive marketing e-mails to add their address to a common register which

participating marketers would use to remove people from their own lists.[205] The US *Direct Marketing Association* is developing such a programme and intend to make its use a condition of membership from July 1999 (DMA, 1998).[206] Another proposal, which comes from the UK Data Protection Registrar, is to use a universally agreed upon character in e-mail addresses to indicate that the user does not want to receive any marketing solicitations.

Opting-out of anonymous profiling

Different approaches currently exist with respect to data which has been automatically collected from header information and click-streams. In the anonymous profile systems operated by Engage Technologies and MatchLogic, click-stream data which are collected automatically are not treated as "personal data" over which the user is entitled to exercise control. For example, the DoubleClick system, which also uses cookies to assign unique identification numbers and collect click-stream data, offers users an "opt-out" option. If selected, the unique identification number is erased and click-stream data are no longer recorded.[207]

D. Providing access to personal data

Access to one's data can be provided using either traditional off-line mechanisms (such as mail or telephone) or interactive online procedures where the request and the response are executed in real time during a connection between the Web site and the data subject.

E. Protecting privacy through transborder data flow contracts

Transborder data flow contracts are an important means of implementing Privacy Principles in the context of a transfer of personal data between a data controller in one country and a data controller in another. Such contracts provide a mechanism for safeguarding personal data transferred between jurisdictions which may have different legal regimes, with respect to privacy protection.

Many international documents require special treatment for transborder data flows. For example, Part Three of the OECD Guidelines state that member countries may restrict flows of certain categories of personal data specifically controlled by domestic legislation to member countries which have no "equivalent" protection. A similar provision is contained in Article 12 of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (COE, 1980). This issue is particularly topical because of Article 25(1) of the European Union Data Protection Directive provides that data transfers from a member country to a third country can only take place where that country ensures an "adequate level of protection". Transborder data flow contracts may provide a bridge between different systems of privacy protection where the data importer is not otherwise regarded as providing adequate protection.[208]

The Council of Europe Model Contract, 1992 and the Guide to the preparation of contractual clauses governing data protection during the transfer of personal data to third parties not bound by an adequate level of data protection, 2002

The *Council of Europe Model Contract to Ensure Equivalent Data Protection in the Context of Transborder Data Flows* (Model Contract) was the result of a joint study by the Council of Europe, the Commission of the European Communities and the International Chamber of Commerce (ICC). The contract is a collection of model clauses designed to ensure "equivalent protection" in the context of transborder data flows based on the guarantees in Convention 108. As well as being applicable to the equivalent protection clause in the OECD Guidelines, the Council of Europe Model Contract provides a useful reference in determining what may amount to "adequate protection" under the EU Directive.

Under the Model Contract the party sending the data warrants that data have been obtained and handled in accordance with the domestic privacy laws of the country in which it operates. In particular reference is made to fair and lawful data collection, the purpose for which the data has been stored, the adequacy and relevance of the data, the accuracy of the data and the period for which data storage has been authorised.

The party receiving the data undertakes to abide by the same principles that apply to the data sender in its home country. To supplement this undertaking, the data receiver also agrees to use the data only for the purposes set out in the contract, to protect sensitive data in the manner required by the domestic law of the data sender, not to communicate the data to a third party unless specifically authorised in the contract and to rectify, delete and update the data as required by the data sender.

The remaining clauses deal with liability for the misuse of the data by the data receiver, rights of data subjects[209], dispute settlement and termination of the contract. The applicable law is left open as a matter for the parties to determine.

In 2002, the Council of Europe adopted a Guide to the preparation of contractual clauses governing data protection during the transfer of personal data to third parties not bound by an adequate level of data protection. The purpose of this Guide, which supplements and refines the 1992 Model Contract, is to assist parties in the drawing up of contractual clauses conforming to the protection requirements deriving from Convention 108 and inform data controllers and data subjects concerned by transborder flows of what they need to look out for as well as to provide assistance for data subjects seeking to assert their rights in the data protection field. Therefore, this Guide does not replace the contractual clauses contained in the 1992 Model Contract; rather, the two documents should be read together.

The revised ICC model contract

The 1992 model contract clauses have been revised by the International Chamber of Commerce in light of the EU Directive's requirement of "adequate protection" in data exchanges to third countries.[210] The revision takes into account comments of the European Commission's Working Party set up pursuant to Article 29 of the EU Directive.[211]

An illustrative agreement: German railways (Deutsche Bahn AG) and Citibank

In 1994, German Railways (Deutsche Bahn AG) arranged with the German subsidiary of Citibank for the production of Railway Cards (offering discounts for frequent travellers) which also functioned as VISA cards (Dix, 1996). Because the cards were produced by a Citibank subsidiary in the United States, the agreement gave rise to substantial transborder data flows. In response to German data protection concerns, an Agreement on Inter-territorial Data Protection was entered into to give German citizens the same level of privacy protection which they would have had if the cards had been produced in Germany. In particular, the contract provided for the application of German law, limited the transfer of the data to third parties, allowed for on-site audits by the German data protection authorities at Citibank's subsidiaries in the United States, and held German Railways and the German Citibank subsidiary liable to German data subjects for any violations of the agreement by their American counterparts.

F. Enforcing privacy principles

The mechanisms used to enforce privacy guidelines vary from country to country. In particular, different balances have been struck between relying on laws and self-regulation. Additionally, the privacy concerns created by global networks have led to the development of novel technological, institutional and contractual solutions which are in the process of gaining acceptance in different parts of the world. For

example, trusted third parties who certify that a Web site complies with its posted privacy policies are emerging as a new private sector mechanism for enforcing privacy principles.

Irrespective of the regime in question, effective enforcement has two aspects. The first side to enforcement is comprised of those mechanisms designed to ensure *ex ante* that privacy guidelines are followed in practice. The second aspect of enforcement is concerned with what happens if privacy guidelines are breached. In particular, who can a data subject complain to, what remedies are available to injured parties and how can infringing data controllers be forced to comply with the applicable privacy guidelines? This distinction between proactive "compliance" and *ex post* "complaint resolution" procedures is adopted in the following discussion of the mechanisms which are available to enforce privacy guidelines[212].

1. Ensuring compliance with privacy standards

There are many *ex ante* means of monitoring compliance with privacy guidelines regardless of whether those principles originate from legislation, codes of conduct or agreements between businesses and consumers. The following section distinguishes between four main means of ensuring compliance; appointment of an internal data protection officer, third party certification as to compliance, membership of industry bodies which impose privacy standards and investigations by central oversight authorities.

(a) Internal data protection officers

Privacy laws and self-regulatory codes may require the appointment of an internal data protection officer by data controllers[213] or designating a particular person within an organisation who is responsible for ensuring that the organisation complies with the applicable privacy practices. As well as being answerable within the company for its compliance record, appropriate laws may make the internal data protection officer externally accountable to, for example, central oversight authorities.

(b) Third party compliance reviews and Web site certification

Compliance reviews undertaken by third parties help ensure that Web sites follow their privacy statements. Ongoing compliance reviews typically involve periodic information practice "audits" and "seeding" (personal information is submitted to the site and its use is compared with the site's stated policy). Sites which continue to satisfy these reviews display a certification mark, such as a digital label[214] or a well-recognised icon,[215] as a public confirmation that they comply with their privacy statements.

There are different reasons why a Web site may seek third party compliance reviews and certification. Sites may voluntarily submit to compliance reviews. For example, a Web site may want to demonstrate its commitment to privacy and ease consumer fears that their personal information could be misused. The risk of having its certification withdrawn, and the publicity which would accompany it, may provide a sufficient incentive for Web sites to comply with their privacy statements. In addition, privacy laws, self-regulatory codes of conduct and/or industry organisations,[216] may require an online business to seek third party certification.

The following are examples of businesses and professional organisations that offer certification schemes with respect to privacy practices and others, such as BBB Online, are being developed.

TRUSTe

TRUSTe is an independent, non-profit making organisation that certifies Web sites which meet the requirements of the TRUSTe programme.[217] In particular, a Web site must: disclose its information management practices in an online privacy statement; adhere to these stated practices and co-operate with

all reviews conducted by TRUSTe. The substance of the site's privacy policy is determined by the site itself, but, at a minimum, its privacy statement must disclose:

- What type of information the site gathers.
- How the information will be used; and
- Who the information will be shared with (if anyone).

TRUSTe also announced in June 1998 that its licensees will be required to provide consumers with the opportunity to exercise control over how their personal information may be used, including transfers to third parties.

Once a company has agreed to the terms of the TRUSTe programme and satisfied an initial review by TRUSTe, it is permitted to use the TRUSTe "trustmark". To ensure that the Web site continues to adhere to its published privacy statement the TRUSTe programme is backed by an on-going "assurance" process. In particular, TRUSTe monitors a Web site's compliance with its stated privacy practices by:

- Conducting periodic reviews of participating sites.
- Regularly "seeding" sites by submitting personal user information and checking that it is not used in a way that violates the site's stated privacy policies; and
- Organising onsite conformance "audits" conducted by outside accounting firms.

Standards authorities

Standards authorities are another type of organisation which may act as third party certifiers by developing privacy standards and offering formal certification to compliant Web sites. An example is the *Canadian Standards Association* (CSA) which has developed a *Model Code for the Protection of Personal Information*. The CSA emphasises the importance of conducting independent audits by auditors certified in privacy auditing to verify ongoing compliance.

Accounting firms

Privacy audits are one of the services now being carried out by large accounting firms.[218] Such audits may be part of a compliance programme run through an organisation such as TRUSTe or the CSA, or it may be organised directly by an accounting firm. The *WebTrust* programme provides a framework for individual accounting firms to provide certification services.[219] Developed by the *American Institute of Certified Public Accountants* and the *Canadian Institute of Chartered Accountants*, the WebTrust Seal is designed to assure online consumers that a participating Web site complies with the WebTrust principles which include information protection. To monitor and ensure ongoing compliance with the WebTrust principles, assurance examinations are conducted by specially licensed accountants on a regular basis. The US *Individual Services Reference Group* principles provide for annual audits by a third party accounting firm.

(c) Membership-based industry bodies

Industry bodies which specify certain privacy practices as a pre-requisite for membership can play a role in ensuring that privacy practices are complied with on global networks. Examples include: the *Online Alliance* which was formed in June 1998 in response to the call for the creation of third party verification mechanisms, it is a cross-industry coalition designed to address online privacy issues whose members have agreed to adopt, implement and disclose privacy policies);[220] the Australian *Internet Industry Association* (which has proposed an Industry Code of Practice utilising a code compliance icon); and the US *Direct Marketing Association* (an industry based-association, whose members engage in database marketing, which encourages its members to post privacy policies on their Web sites).[221] Also *BBBOnLINE*, a membership-based certification programme for online businesses, is considering adopting a privacy

standard amongst its qualifying criteria, possibly by means of a separate privacy charter represented by its own seal or icon.[222]

How satisfactory an industry body is likely to be in ensuring compliance with privacy standards depends on a number of factors. These include: how the applicable privacy code is publicised to members; how the organisation checks that the code is being followed and how often; how does the organisation deal with consumer complaints, and, when a member is shown to have breached the code, how it is sanctioned.

(d) Central oversight authorities

Most jurisdictions with laws for the protection of personal privacy also establish a central oversight authority such as a data protection office or a privacy commissioner that may be empowered to perform proactive audits on their own initiative.

The "supervisory authorities" referred to in the EU Directive,[223] for example, are intended to play this role. In particular, these authorities are endowed with investigative powers (such as the right to access data) and powers of intervention (such as the right to ban a particular method of data processing. In the EU, for example, these powers are subject to a right of judicial appeal.

Other legal requirements may be imposed to facilitate the compliance monitoring role of central oversight authorities. For example, a system of compulsory registration increases the information available to such authorities[224] and initial audits can be required to ensure adherence to the law before data processing commences.

2. Complaint resolution procedures for breaches of privacy standards

When a data subject believes that the privacy guidelines which apply to his or her relationship with a particular data controller have been breached, he or she should have access to redress or remedy. The privacy complaint resolution procedures which can be found in different OECD member countries vary in many ways.

There are different ways in which privacy complaints may be addressed according to whether (1) the complaint is resolved directly between the data subject and the data controller; (2) the complaint is brought to the notice of a third party certification agency or industry body; or (3) administrative, civil or criminal proceedings are pursued.

The kinds of questions which can be asked in comparing each of these categories are:

- What kinds of *redress* are available to the data subject? The redress being sought may vary from securing compliance with the applicable privacy principles (for example, by allowing access to, or correcting, the personal data in question or by entering the user on a "opt-out" list so that the personal data will not be used by advertisers in the future), to obtaining orders for compensation.
- What are the *ultimate sanctions* available to force compliance by the data controller? Ultimate sanctions may include orders by central oversight authorities, civil court remedies, criminal sanctions (which may be pursued by the data subject, a central oversight authority or some other prosecuting body), removal of a certification seal or expulsion from an industry body.
- How formal and complicated is the procedure? The resolution of a privacy complaint may involve different levels of formality, from direct and informal communications between the data subject and controller, to mediation by a central oversight authority, to formal judicial proceedings.

(a) Complaint resolution between the data subject and the data controller

A data subject's initial complaint is likely to be made to the alleged infringer. Companies that collect and use personally identifiable information may be able to resolve many privacy disputes by providing mechanisms to receive and address consumer complaints. Obtaining redress directly from the data controller is likely to be the quickest, cheapest and least complicated means of complaint resolution.

Good reasons exist for online businesses to attempt to amicably resolve the privacy complaints of their customers. These incentives include protecting their reputations, fostering good customer relations and avoiding the threat of more formal complaint procedures being initiated.

Some online businesses offer clearly defined complaint procedures to facilitate the amicable resolution of privacy complaints. These provisions may address issues such as the method by which an organisation may be contacted, the remedies available (for example, liquidated damages, that is, a set amount of money to be paid for breaches of privacy) and procedures for bringing a claim to arbitration.

Some Legislation and self-regulatory codes require data controllers to appoint internal data protection officers to facilitate the resolution of complaints by providing a clear point of contact with an individual who has well defined responsibilities.

(b) Enforcement through private sector certification schemes and industry bodies

Certification schemes and industry bodies may offer avenues of redress for data subjects alleging privacy breaches by a member Web site. Such organisations are useful in two ways. First, the privacy criteria set by the certification scheme or industry body provide a benchmark against which the data controller's practices may be judged. Second, the third party certifier or industry body has a reputational interest in ensuring that members comply with its privacy rules and is also likely to have a large degree of bargaining power relative to its members. These factors give the third party certifier or industry body both the incentive and capability to assist the data subject in resolving his or her complaint.

Third party certifiers and industry bodies may take a variety of roles in the resolution of a privacy dispute, ranging from investigation to mediation to adjudication. The redress available might include compliance with applicable privacy principles and compensation for any losses.

Sanctions that may be assessed may include:

- The publication of the business' name on a "bad actor" list.
- The revocation of the Web site's compliance certification icon.[225]
- Removal from an industry body;[226] and/or
- Administrative or judicial proceedings against the Web site (for example, for breach of contract or misuse of trademarks).

The following are examples of certification businesses and industry bodies who may play a role in resolving user complaints over a Web sites privacy practices.

TRUSTe

When TRUSTe receives a complaint it first sends a formal notice and gives the alleged infringer a chance to respond. If this proves unsatisfactory, TRUSTe conducts an escalating investigation. Depending on the severity of the breach, the investigation could result in penalties, an on-site conformance review or revocation of the participant's trustmark. Serious cases may be referred to the FTC for enforcement action

under the *Federal Trade Commission Act* or TRUSTe may conduct breach of contract or trademark infringement litigation against the site.

The Australian Internet Industry Association

In February 1998, the Australian *Internet Industry Association* released a draft *Industry Code of Practice.*[227] In the first instance, it is intended that complaints will be dealt with between the user and the Code Subscriber within a time frame specified by the Code. If this is not successful, however, the Code sets out other procedures including the appointment of a mediator, or the making of orders by the Code's *Administrative Council* directing the subscriber to comply with the Code or to provide corrective advertising and/or the payment of compensation. The Council may also withdraw permission for a site to use its *Code Compliance Symbol*.

(c) Enforcement through administrative, civil and criminal proceedings

State organs may provide redress either in the form of an administrative remedy through a central oversight authority or a judicial remedy through the court system. Judicial remedies may be either civil (where compensation and/or orders for compliance are typically provided for the breaches of privacy principles) or criminal (where sanctions are typically imposed on offending data controllers).

Administrative proceedings

Central oversight agencies

Privacy regimes often create central oversight agencies, such as a Data Protection Authority or a Privacy Commissioner. Such agencies will typically provide an administrative mechanism for resolving privacy complaints.

One reason for involving a central oversight authority is because individual data subjects may not have the expertise or investigative powers to determine exactly when or by whom his or her privacy was violated. A Data Protection Authority or Privacy Commissioner will also bring its experience and institutional authority to bear in attempting to resolve a privacy complaint.

The grounds upon which a complaint may be brought to a central oversight agency will depend on the terms of its empowering legislation, but typical reasons include breaches of privacy laws and, possible, self-regulatory codes of conduct or privacy statements.

The powers of a specific central oversight agency, and the kinds of redress available to the data subject, will also depend on its empowering legislation, but typically such bodies are empowered to:

- Investigate complaints.
- Conduct or demand audits.
- Attempt conciliation between the parties.
- Examine witnesses.
- Issue recommendations.
- Act as specialist tribunals and impose quasi-judicial orders involving, for example, compensation and sanctions; and/or
- Either refer complaints to, or prosecute complaints in, a judicial forum.

Decisions of central oversight agencies are often subject to review in the court system or through a specialist tribunal (such as the Data Protection Tribunal in the United Kingdom with respect to enforcement notices).

Other administrative agencies

Other administrative agencies may become involved in resolving privacy complaints. Where the conduct complained of involves not only a breach of privacy principles but also fair trading standards by, for example, violating the terms of a privacy statement, then administrative bodies charged with enforcing these practices may be complained to. For example, in the US the Federal Trade Commission (FTC), in its role as an independent law enforcement authority, has broad powers to investigate and adjudicate complaints of businesses engaging in unfair and deceptive conduct.[228] The FTC has recently conducted an investigation against a company (it may not be appropriate to single out a company) for misleading its customers as to how their personal information were being used which has resulted in a consent order being issued.

Civil proceedings

Breaches of privacy legislation

Privacy legislation may provide data subjects with the right to a judicial remedy for breach of privacy principles established by the legislation[229]. Procedurally, such complaints are usually brought to court by the injured data subject. In addition, in some common law countries, actions may also be brought based on a tort of invasion of privacy.

A court may be given a wide variety of powers to provide suitable redress in a given case. The range of remedies which may be provided for include the power to:

- Order payment for compensation or restitution.
- Impose a monetary fine.
- Make corrective orders (for example, by allowing access to, or correcting, the personal data in question).
- Mandate or prohibit certain data processing practices; and
- Require periodic reviews to ensure compliance.

Violations of privacy statements, online agreements and transborder data flow contracts

The range of civil remedies available to a data subject is not limited to those found in privacy legislation. The general laws relating to breach of contract, fraud and fair trading may also apply where the data controller has violated the terms of a privacy statement, online agreement (such as the terms and conditions associated with a registration form) or a transborder data flow contract.

The breach of a privacy statement or online agreement may give rise to a number of possible civil remedies. Essentially, by providing notification of its privacy practices a Web site offers a commitment that it will follow these practices. Depending of the nature of the breach, most jurisdictions provide remedies for wrongful misrepresentations and/or fraudulent conduct if that commitment is broken.

A contractual remedy may also be available to Web site visitors. A contract is most likely to exist between the parties where they have entered an online agreement by, for example, explicitly agreeing to terms and conditions referred to in a registration form. However, the distinction between a posted privacy policy and an online registration agreement is often one of degree. For example, the Web site may include a “Terms and Conditions” section which is expressed like a contract but which, unlike a registration form, does not require the user to explicitly acknowledge their consent.[230] In general, however, the more a privacy policy looks like a term of an agreement between the parties, the more likely it is to be given contractual effect and be capable of giving rise to a legal remedy for breach of contract. The contractual effect of a privacy clause will depend on the other terms of the contract (relating to, for example, jurisdiction and arbitration of disputes) and the laws of the jurisdiction in which it is being considered.

The breach of a transborder data flow contract by a data controller may also provide the basis for a judicial remedy for an effected data subject. Since the data subject will not usually be a party to this agreement, enforcement difficulties will exist in jurisdictions which do not permit claims by third party beneficiaries to a contract. The solution adopted in the German Railways - Citibank contract was to hold the German Railway and the German Citibank subsidiary liable to German data subjects for any violations of the agreement by their American counterparts. Similarly, the Council of Europe Model Contract provides that damage caused to data subjects, through the use of the transferred data or upon termination of the contract, should be repaired by the party sending the data under domestic law or international private law.

Alternative dispute resolution

Civil remedies need not be pursued exclusively through a court system. Alternative dispute resolution procedures may be followed by the parties where, for example, a contract provides for arbitration hearings. Both the *Council of Europe Model Contract to Ensure Equivalent Data Protection in the Context of Transborder Data Flows* and the *Revised ICC Model Contract* (May 1998 Draft) contain clauses which provide for the arbitration of disputes between the sending and receiving data controllers.

Criminal proceedings

Proceedings under privacy legislation

Privacy legislation may provide for criminal sanctions to be imposed in cases where there have been serious breaches of the legislation.[231] One reason for such sanctions is to provide companies with a greater incentive to follow good privacy practices than would be provided merely by forcing the payment of compensatory damages when breaches have been proved. The range of entities who can bring criminal proceedings (for example, individual data subjects, data protection authorities and public prosecutors) and the range of available sanctions (for example, fines and prison sentences) will depend on the implementing legislation.[232]

Other criminal proceedings

In addition to criminal prosecutions based on privacy legislation, where a data controller falsely asserts that it is following a particular privacy policy prosecutions may be possible under fair trading legislation.

G. Educating users and the private sector

The nature of the global information network makes educating users and commercial entities about privacy issues an important step for the protection of personal privacy. Education supplements all of the other guidance instruments and mechanisms referred to in this Inventory.

Global networks turn businesses into data controllers. The ease with which data are collected and transferred electronically means that online merchants find themselves dealing with far more personal data, far more often, than if they had remained off-line. More and more entities find themselves acting as data controllers and subject to data protection laws, codes of conduct and self-regulatory industry codes. The better educated these ISPs, online merchants, content providers, browser designers and bulletin board operators are in privacy matters, the more likely it is that practices will be effectively implemented in practice.

Global networks also raise new privacy issues for users. The emerging trend for privacy rights to be protected through technological tools and by exercising choice as to privacy options means that users will only be fully protected if they are knowledgeable enough to look after themselves. Unlike the off-line world where individuals rarely have to consciously consider the privacy implications of their actions, the

online public must be educated as to the consequences of where they go, what they say and what they do when on the Internet. For example, users should be aware of the information they reveal simply by browsing the Web; sending an email or posting a message to a newsgroup. They should also be alert to the consequences of agreeing to particular privacy practices, how to use privacy enhancing technologies and how to set appropriate browser settings for their desired level of privacy.

In addition to traditional methods of public education in schools, the workplace and the media,[233] various Web sites offer online advice on personal privacy protection on global networks. These sites are run by *(1)* international organisations, such as the Council of Europe[234]; *(2)* government bodies, such as the FTC in the United States[235] and many central oversight authorities in other parts of the world;[236] and *(3)* private sector organisations, such as *Project OPEN* (the Online Public Education Network), the US *Direct Marketing Association*[237], the *Center For Democracy and Technology,*[238] the *Electronic Privacy Information Center,*[239] "Call for Action" and TRUSTe.[240]. Hyper-text links can be used to provide access to these sources of privacy information from Web sites which collect personal information.

NOTES

1. Sections I and II of this inventory have been updated to reflect (some, but not all) member country changes, as of January 2003.

   In addition, in April 1999, the following specific changes came to the attention of the secretariat:

   - On 21 April 1999, Poland signed the Council of Europe (COE) Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108).
   - On 26 April 1999 50 Internet service providers signed up to use Freedom Network, an international collection of independent server operators providing technology to support privacy for Web users. The 50 participating providers and networks are located in Australia, Austria, Canada, Japan, Netherlands, United Kingdom and the United States (see www.zeroknowledge.com/partners).

2. This information, and in particular the user's e-mail address, may potentially be sufficient to trace the individual's real name and address through an e-mail directory (see, for example, the Four11 directory at www.bfm.org/misc/four11_com.html).

3. Each computer on the Internet has a unique IP address usually, expressed in the form #.#.#.# (where each # is a number from 0-255).

4. For a discussion of cookies, see www.cookiecentral.com/.

5. Cookies are useful because they allow a user and a Web site to interact over time. For example, if a user places an order for a particular music CD on one page, this information can be accessed when the user arrives at the payment page. Cookies are also used to allow sites to recognise a particular user on any subsequent visits to the site. Each time the user returns, the site can call up specific information about the user which might include a preferred language, password information, or the user's interests and preferences as indicated by items or documents which the user has accessed in prior visits.

6. Article 27 of the EU Directive notes that Member States should establish mechanisms for putting in place codes of conduct "to contribute to the proper implementation" of national data protection provisions.

7. This is the definition of Personal data in Paragraph 1, Annex to the Recommendation of the Council.

8. Paragraphs 2-3, Annex to the Recommendation of the Council.

9. Paragraph 15-18, Annex to the Recommendation of the Council.

10. Paragraphs 20-22, Annex to the Recommendation of the Council.

11. Paragraph 19, Annex to the Recommendation of the Council.

12. Other work by the ICCP Committee (in addition to this Inventory) includes a report on "Implementing the OECD Privacy Guidelines in the Electronic Environment: Focus on the Internet" (October 1997); an OECD Workshop on "Privacy Protection in a Global Networked Society" (February 1998) and the resulting report (July 1998); a consultant report analysing the results of an OECD Web survey; and a "Ministerial Declaration on the Protection of Privacy on Global Networks" (from the Ministerial Conference, *A Borderless World: Realising the Potential of Global Electronic Commerce* (Ottawa, 7-9 October 1998).

13. Figures as at December 1997. Table 6.1 of National Instruments shows those OECD member countries which have ratified Convention 108.

14. Signature of the Convention represents a political, rather than legal, commitment. The scope of application of Convention 108 can be extended or restricted by means of a declaration by the party addressed to the Secretary-General of the Council of Europe at the time of signature or ratification.

15. Article 6, Convention 108.

16. Article 12.3(a), Convention 108.

17. Article 13.2, Convention 108.

18. Article 4, Convention 108.

19. Part A, Paragraph 5, Guidelines for the Regulation of Computerized Personal Data Files.

20. This includes controllers established in a place where a Member State's law applies by virtue of international public law, or making use of equipment situated in the Member State (unless only for the purposes of transit).

21. Articles 3 and 4, EU Directive.

22. Article 8 of the EU Directive prohibits the processing of sensitive data subject to certain exceptions such as the explicit consent of the data subject.

23. Articles 10, 11 and 12 EU Directive.

24. Article 18-21, EU Directive.

25. Articles 14, EU Directive.

26. Articles 22-24, EU Directive.

27. Article 1(2), EU Directive.

28. Article 25(1), EU Directive.

29. Article 26, EU Directive.

30. Article 28, EU Directive.

31. Article 22-24, EU Directive.

32. See www.wto.org/.

33. Article XIV(c)(ii), Part II, GATS.

34. Further information can be found at http://europa.eu.int/comm/dg15/en/media/dataprot/news/santen.htm.

35. The paper was referred to by the European Union Article 29 Working Party in a recommendation in December 1997.

36. ISO was established in 1947. See www.iso.ch/.

37. Other ongoing work on privacy within ISO is being conducted by: JTC1 (a Joint Technical Committee); SC27 (a Subcommittee considering security of data); TAG12 (a Technical Advisory Group); and ISO's Committee on Medical Informatics.

38. See www.iccwbo.org.

39. See www.iccwbo.org/home/menu_advert_marketing.asp for more information.

40. See www.epic.org.

41. See www.cdt.org.

42. See www.privacy.org.

43. See www.privacyexchange.org.

44. A copy of the Privacy Act 1998 can be found at http://scaleplus.law.gov.au/html/pasteact/0/157/top.htm.

45. The Privacy Commissioner's Web site is www.privacy.gov.au.

46. Links to the various state and territory regimes can be found at www.privacy.gov.au/links/index.html#2.

47. A Register of Approved Codes is maintained at www.privacy.gov.au/business/codes.

48. Provisions on international transfers came into force on 1 July 1987.

49. Federal Law Gazette I Nr.100/1997.

50. Austrian Federal Law Gazette Nr. 194/1994.

51. This can be downloaded in German from the Parliament Web site at www.parlinkom.gv.at. This link leads directly to the page www.parlinkom.gv.at/pd/pm/XX/I/his/016/I01613_.html. The official German and an unofficial English text of the Federal Data Protection Act, as well as English translations of other texts are available from the *Datenschutzkommission* by e-mail free of charge (contact georg.lechner@bka.gv.at). The whole body of Austrian law is available on the net in German at www.ris.bka.gv.at.

52. See www.privacy.fgov.be.

53. Articles 37-43.

54. Document available at www.lachambre.be.

55. Document available at www.ispa.be/fr/c040201.html.

56. Document available at http://laws.justice.gc.ca/en/p-21/93445.html.

57. In Alberta see the Freedom of Information and Protection of Privacy Act (1995); in British Columbia see the Freedom Of Information and Protection of Privacy Act (1993); in Manitoba see the Freedom of Information and Protection of Privacy Act (1998); in New Brunswick see the Protection of Personal Information Act (1998); in Newfoundland see the Freedom of Information Act (1982); in the Northwest Territories see the Access to Information and Protection of Privacy Act (1997); in Nova Scotia see the Freedom of Information and Protection of Privacy Act (1993); in Ontario see the Freedom of Information and Protection of Privacy Act (1988) and the Municipal Freedom of Information and Protection of Privacy Act (1991); in Quebec see the Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information (1982); in Saskatchewan see the Freedom of Information and Protection of Privacy Act (1991) and the Local Freedom of Information and Protection of Privacy Act (1993); and in Yukon see the Access to Information and Protection of Privacy Act (1996). Information on all of Canada's privacy laws is available at http://infoweb.magi.com/~privcan/other.html.

58. See, for example, Manitoba's *Personal Health Information Act (1997).*

59. The committee was comprised of representatives of industry and the Canadian government.

60. CAN/CSA-Q830-96. The CSA Standard can be viewed/ordered at www.csa-intl.org/onlinestore/welcome.asp?Language=EN.

61. Publication PLUS 8300 (December 1996). This document can be ordered from the CSA Web site: www.csa-intl.org/onlinestore/welcome.asp?Language=EN.

62. Document available at www.caip.ca. Information technology codes have also been developed by associations such as the Information Technology Association and the Canadian Information Processing Society.

63. Act No.256/1992.

64. The *Ministry of the Interior* and the *Czech Telecommunication Office* are co-operating with OSIS in the preparation of the bill.

65. See www.finlex.fi/pdf/saadkaan/E9990523.PDF.

66. See www.tietosuoja.fi.

67. Sections 47-48, Personal Data Act.

68 . See www.ssml-fdma.fi.

69. Articles 226-16 to 226-24.

70. See www.cnil.fr.

71. Criminal sanctions under Articles 41-44 of Law 78/17 and Article 226-21 of the French Penal Code.

72. Law No. 92-1446 of 31 December 1992.

73. Law No. 95-73 of 21 October 1995.

74. Document available at http://users.info.unicaen.fr/~herve/publications/1997/charte/charte.final.html.

75. Internet actors who commit themselves to the charter are mainly users and ISPs, based in French territory.

76. *Code de Déontologie sur la protection des données à caractère personnel*.

77. Law of 20/12/1990 on data protection. The act is available in English on the Berlin Data Protection Commissioner's site: www.datenschutz-berlin.de/gesetze/bdsg/bdsgeng.htm

78. Section 21(1).

79. Sections 43 and 44.

80. Federal regulations (in German) available at www.datenschutz-berlin.de/recht/de/rv/index.htm.

81. Otherwise known at the IuKDG (01.8.1997), an outline of which is available at www.iukdg.de.

82. See www.iid.de/iukdg/aktuelles/fassung_tddsg_eng.pdf. More information is available at www.iukdg.de.

83. Addresses of the Laender data protection authorities are available at www.datenschutz-berlin.de/sonstige/behoerde/aufsicht.htm

84. The conference of 29 April 1996 sets out key points for regulation in matters of data protection of online services. See www.datenschutz-berlin.de/sonstige/konferen/sonstige/old-res2.htm.

85. Latest draft of the new Federal Act (in German) is available at www.datenschutz-berlin.de/themen/ds-allg/bdsg_neu.htm.

86. English Translation, Official Gazette of the Hellenic Republic, Volume One, Issue No. 50 of 10 April 1997.

87. The Greek Data Protection Authority's duties are specified under Article 19 of the Law.

88. Articles 11-14.

89. Article 23.

90. Article 21.

91. Article 22.

92. Act No. LXIII of 1992. The Act was modified by Acts No LXV and LXXVI of 1995.

93. Articles 11-15.

94. Article 27. The Data Protection Commissioner has enforcement powers under Articles 25 and 26.

95. Articles 17 and 18.

96. Article 33.

97. Article 14(1).

98. Article 22.

99. Article 33.

100. Articles 37-39.

101. The right to privacy has been interpreted as one of the unspecified personal rights under Art. 40(3) of the Constitution.

102. Sections 21-23.

103. IDMA Code of Practice on Data Protection (3 May 1995).

104. See, for example, Kanagawa Prefecture, Ordinance passed on 26 March 1990.

105. The Guidelines were originally issued in April 1989.

106. Articles 22 and 23 of the Guidelines.

107. The ENC is a trade organisation run by the New Media Development Association, an auxiliary organisation of MITI. See www.nmda.or.jp/enc/index-english.html.

108. See www.ecom.or.jp.

109. Document available at www.telesa.or.jp/e_guide/e_guid01.html.

110. 31 March 1979.

111. Established by a Law of 9 August 1993, the oversight authority is composed of the public prosecutor and the Secretary General and two members of the Consultative Commission.

112. Articles 32-39.

113. See Laws No. 65 of 20 August 1993 and No. 74 of 2 October 1992.

114. Bill No. 4357.

115. Article 214, Federal District Penal Code.

116. Wet van 6 July 2000, Stb. 302, *houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens).* An unofficial translation of the act is available at the Web site of the Dutch Data Protection Authority, www.cbpweb.nl.

117. Wet van 19 October 1998, Stb. 610, *houdende regels inzake de telecommunicatie (Telecommunicatiewet).*

118. Sections 97-109, Privacy Act.

119. See www.privacy.org.nz/top.html. The functions of the Commissioner are set out in Section 13, Privacy Act.

120. Sections 46-53, Privacy Act.

121. Section 85, Privacy Act.

122. Document available at www.internetnz.net.nz/icop/icop99the-code.html.

123. Document available at www.privacy.org.nz/top.html.

124. Document available at www.privacy.org.nz/comply/justice.html.

125. See www.datatilsynet.no.

126. Article 51 states:

(1) No one may be obliged, except on the basis of statute, to disclose information concerning his person.

(2) Public authorities shall not acquire, collect nor make accessible information on citizens other than that which is necessary in a democratic state ruled by law.

(3) Everyone shall have a right of access to official documents and data collections concerning himself. Limitations upon such rights may be established by statute.

(4) Everyone shall have the right to demand the correction or deletion of untrue or incomplete information, or information acquired by means contrary to statute.

(5) Principles and procedures for collection of and access to information shall be specified by statute.

127. 29 August 1997, Dz.U. nr 133, poz. 833. The Act came into force on 30 April 1998.

128. Articles 50-54.

129. Law No. 10/91, as amended in 1994 by Law No. 28/94 to reinforce protection of sensitive data and data in transborder flows between parties to Convention 108.

130. Article 8(h).

131. Articles 27, 29 and 30.

132. Articles 34-41.

133. Law 109/91 of 17 August 1991.

134. Decree-law 296/94 of 24 December 1994.

135. Decree-law 1/95 of 12 January 1995. There is also a decree-law 48/97 on identity cards of the Healthcare National System.

136. Regulative Decree 2/95 of 25 January 1995.

137. Regulative Decrees 4/95 and 5/95 of 31 January 1995.

138. Regulative Decree 27/95 of 31 October 1995.

139. Law 5/92 of 29 October 1992. The document is available on line at www.ag-protecciondatos.es/datmen.htm.
In 1993, a Royal Decree was adopted which supplemented (*inter alia*) the provisions on transborder data flows, registration procedures and data subjects rights.

140. See www.ag-proteccionadatos.es.

141. Articles 43 and 44 of the Law.

142. Law No. 28/94.

143. Code available (in Spanish) at www.aece.org/default.asp.

144. *Tryckfrihetsförordningen* (Act No. 1949:105). – This Act and other Swedish Acts, Government Bills, etc. are accessible via the Internet at: www.riksdagen.se/rixlex/index_en.htm.

145. *Regeringsformen* (Act No. 1974:152).

146. Act No. 1998:204.

147. The Personal Data Ordinance (Act No. 1998:1191).

148. *Yttrandefrihetsgrundlagen* (Act No. 1991:1469).

149. 19 June 1992.

150. See www.edsb.ch.

151. Article 11 of the FLDP.

152. Article 23 of the FLDP.

153. Articles 28 and 28f, Civil code (SR 210).

154. As supplemented by Orders in 1987, 1990 and 1997. The Data Protection Act is available at www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm.

155. See www.lcd.gov.uk/foi/datprot.htm.

156 . For a summary of the Act see www.hmso.gov.uk/acts/acts1990/Ukpga_19900037_en_1.htm#end.

157 . For a summary of the Act see www.hmso.gov.uk/acts/acts1993/Ukpga_19930010_en_1.htm#end.

158 . For a summary of the Act see www.hmso.gov.uk/acts/acts1994/Ukpga_19940033_en_1.htm.

159 . For more information see http://conventions.coe.int/Treaty/EN/cadreprincipal.htm.

160 . For the full text of the Act see www.hmso.gov.uk/acts/acts1998/19980042.htm.

161. For the full text of the Act see www.hmso.gov.uk/acts/acts1998/19980029.htm.

162. See www.ispa.org.uk.

163. Examples include the Advertising Association; the Code of the Banking Practice Review Committee; and the Code for Computer Bureau Services by the Computing Services Association.

164. 5 U.S.C. § 552a (1994).

165. See www.ibiblio.org/nii/NII-Task-Force.html.

166. Document available at www.ntia.doc.gov/ntiahome/privwhitepaper.html#B11.

167. Document available at www.ntia.doc.gov/reports/privacydraft/198dftprin.htm.

168. Document available at www.ftc.gov/reports/privacy3/index.htm.

169. Congressional testimony of Robert Pitofsky, Chairman of the FTC, 21 July 1998. Document available at www.ftc.gov/os/1998/07/privac98.htm.

170. See www.itic.org.

171. The ITI principles broadly reflect the OECD Guidelines, with special provisions on "Educating the Marketplace" and "Adapting Privacy Practices to Electronic and Online Technologies."

172. See www.privacyalliance.org. Members include Microsoft, AOL Time Warner, Sun Microsystems, Dell, Ernst & Young, and Yahoo!.

173. See www.the-dma.org

174. See www.bbb.org/alerts/carupr.asp for more information.

175. In the off-line world anonymity is an important (although often taken for granted) means of protecting personal privacy. For example, cash purchases can be used to prevent the creation of a transaction trail, controversial opinions may be expressed under a pseudonym and guarantees of anonymity are often given to encourage people, such as police informants, news sources and "whistle blowers" to reveal information.

176. See http://internet.junkbuster.com.

177. See www.thelimitsoft.com/cookie.html.

178. See www.hotmail.com.

179. See www.gilc.org/speech/anonymous/remailer.html.

180. This would generally include the user's IP address, domain name and geographical location, the operating system and browser being used, the Web page which was viewed immediately prior to accessing this site, and, possibly, the user's e-mail address.

181. See www.anonymizer.com.

182. Various steps may be taken by the intermediary to prevent abuses of anonymity. For example, the Anonymizer blocks access to certain sites, such as chat rooms, where abuses have occurred in the past. Also, *Infonex*, who run the Anonymizer service, logs each user's IP address, hostname and the documents requested. This information may potentially be released and used in an attempt to identify the user if *(i)* the *Anonymizer* is used to disrupt a service by, for example, "spamming" an e-mail address or newsgroup with content inappropriate for the forum; or *(ii)* a court order is issued requiring the release of the information.

183. Over 50 different payment systems have been proposed for the Internet. For a list see http://ganges.cs.tcd.ie/mepeirce/Project/oninternet.html.

184. See www.mondexusa.com.

185 A smart card is a small card which contains an embedded microcomputer. The Mondex Card has been programmed to function as an "electronic purse" which can be loaded with value and used as payment for goods or services or transferred to another Mondex Card using card readers.

186. See www.engage.com.

187. See www.doubleclick.com.

188. See www.clickstream.com.

189. While such information is arguably not by itself personal data as it does not "[relate] to an identified or identifiable individual" [Article 1(b), OECD Guidelines], it is certainly *potentially* personal data in that it may become linked to an actual identity if, for example, the user gives his or her name to the company maintaining the profiles or to a merchant who has been supplied with a personal profile.

190. For example, a survey of 1 200 US commercial Web sites by the FTC (March 1998) found that only 14 % provided any notice of their information collection practices (see www.ftc.gov/reports/privacy3/survey.htm). Similarly, a survey of the top 100 Web sites conducted in June 1997 by the Electronic Privacy Information Centre (EPIC) found that only 17% of these sites had explicit privacy policies (see www.epic.org/reports/surfer-beware.html).

191. See www.truste.org.

192. See www.bbbonline.org.

193. See www.privacyalliance.org.

194. See www.aeanet.org.

195. The TRUSTe programme is discussed in more detail in the enforcement section.

196. Examples of posted privacy policies can be found throughout the Web. See, for example, the privacy statements at Lego (www.lego.com/eng/info/privacypolicy.asp); Continental Airlines (www.continental.com/travel/policies/privacy/default.asp?SID=1DED319A40994D1BA93200181E79A5EB); Australian Legal Information Institute (www.austlii.edu.au/austlii/privacy.html); ZDNet (www.zdnet.com/findit/privacy.html); DoubleClick (www.doubleclick.com/company_info/about_doubleclick/ privacy); Reader's Digest (www.rd.com/privacy.jhtml); and Microsoft (www.microsoft.com/info/privacy.htm).

197. See, for example, the Web sites of *The Economist* (www.economist.co.uk/) and the *Financial Times* (www.ft.com) which both require user registration before all but the first few pages on the site may be accessed.

198. See www.w3.org/P3P.

199. PICS is an example of a technological platform capable of supporting digital labelling. PICS was developed by the W3C as a framework for labelling the content of Web pages to allow users (or parents of children using the Web) to set filtering rules which selectively block access to certain kinds of material. However, the PICS protocol can be applied in other ways. So, by developing a vocabulary of privacy labels, the PICS approach could also be used to label Web site privacy practices. For an example of such a vocabulary, see Joel R. Reidenberg, "The Use of Technology to Assure Internet Privacy : Adapting Labels and Filters for Data Protection" in Lex Electronica Vol.3 No.2 (http://www.lex-electronica.org/reidenbe.html).

200. For an assessment of the conditions that should be met by a technical platform for the protection of privacy, such as P3P, see the Report of the International Working Group on Data Protection in Telecommunications contained in Annex 4 of the Minutes to the 23rd meeting of the Working Group, 14-15 April 1998 in Hong Kong, China.

201. For the latest draft of the P3P protocol (April 2002) see www.w3.org/TR/P3P.

202. See www.moniker.com.

203. The Web sites managed by MatchLogic are www.grandgobosh.com, www.excite.com, www.webcrawler.com and www.quicken.com.

204. A "Robinson List" is a list of people who do not wish to receive direct marketing materials which must be followed by direct marketing businesses. An example of such a system being adopted in law can be found in Austria, see Section 268(8) of the *Industrial Code* (1994), Austrian Federal Law Gazette Nr. 194/1994.

205. The e-MPS technique for "opting-out" of e-mail marketing lists can be applied more generally. For example, an opt-out Web site has been announced in the United States. The site (www.consumer.gov), run by the Federal Trade Commission, includes instructions on how people can prevent companies from screening their credit reports, prevent drivers' license information from being sold and remove their names and addresses from marketing lists.

206. The DMA currently operates similar mail and telephone preference schemes. For an example of an operational e-MPS scheme, see http://preference.the-dma.org/products/empssubscription.shtml.

207. See www.doubleclick.net/us/corporate/privacy/privacy/default.asp?asp_object_1=&.

208. The possibility of using contracts between data controllers to ensure that personal data transferred from one country to another receive "adequate protection" under the EU Directive is explicitly recognised by Article 26(2).

209. Under the Model Contract data subjects are to have rights of access, rectification and erasure against the party receiving the data (clause 2) and the party sending the data is to terminate the contract or start arbitration proceedings if such rights are denied. In addition, damage caused to the data subject, through use of the data or upon termination of the contract, should be repaired by the party sending the data under domestic law or international private law (paragraphs 36 and 41 of the Explanatory Memorandum).

210. See the ICC Web site at www.iccwbo.org.

211. In particular, the Working Party found that the sending country's substantive data protection rules must be imposed upon the data recipient and these rules must be rendered effective by delivering a good level of compliance, providing support to individual data subjects in the exercise of their rights and providing redress for breaches of these rights.

212. Compliance and redress mechanisms are by no means independent. For example, the existence of effective redress mechanisms improves the level of compliance with privacy standards. That is, the more likely it is that a company will be punished for violating privacy norms, the less likely it is to breach those norms in the first place. However, given the complexity of modern data processing techniques and barriers which individuals face in vindicating their rights (such as cost), a mix of *ex ante* and *ex post* procedures is most likely to be effective in ensuring the desired level of privacy protection.

213. See, for example, the German Data Protection Act 1990; Principle 1 of the Canadian Standards Association Model Code (see paragraph 91); and the MITI Guidelines in Japan (see paragraph 166).

214. Such a label could be used within the P3P labelling system.

215. Various methods, such as digital authentication, are available to prevent the unauthorised use of such a certification icon. See www.verisign.com/index.html.

216. See, for example, the *Online Privacy Alliance* who "supports third-party enforcement programs that award an identifiable symbol to signify to consumers that the owner or operator of a Web site, online service or other online area has adopted a privacy policy that includes the elements articulated by the Online Privacy Alliance, has put in place procedures to ensure compliance with those policies, and offers consumer complaint resolution." See www.privacyalliance.org/resources/enforcement.shtml.

217. See www.truste.org.

218. Over the last 15 years, accounting firms have expanded their field of practice from simply auditing a company's financial performance, to auditing a company's performance across a range of "social responsibility" issues (for example, the environmental impact of a company's operations).

219. See www.aicpa.org/assurance/trustservices/index.asp?.

220. See www.privacyalliance.org.

221. For a discussion of this scheme and a critical report on the low level of new member compliance with this recommendation, see "Surfer Beware II: Notice Is Not Enough", by the Electronic Privacy Information Centre (www2.epic.org/reports/surfer-beware2.html).

222. See www.bbbonline.org.

223. Article 28 of the EU Directive which provides that each Member State shall have a "supervisory authority" with broad investigative, remedial and prosecuting powers.

224. See, for example, the notification requirements of Article 18 of the EU Directive.

225. As proposed by, for example, TRUSTe and the Australian *Internet Industry Association*.

226. See, for example, the *Privacy Code Guidelines* developed by the *Canadian Direct Marketing Association* which provide for enforcement through CDMA hearings and the possibility of expulsion from the CDMA.

227. The National Principles can operate in online or electronic environments. In May 1998, the Online Council, which comprises federal, state and territory IT Ministers, acknowledged the Principles as providing a basis for a national benchmark on privacy standards.

228. For a discussion of the enforcement powers of the FTC in relation to "unfair or deceptive acts or practices" under Section 5(a) of the Federal Telecommunications Commission Act, see www.ftc.gov/ogc/brfovrvw.htm. It should be noted that the FTC jurisdiction is limited by the requirement that the practices complained of "cause ... or [are] likely to cause *substantial injury* to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition" [15 U.S.C. Sec. 45(n)] (emphasis added).

229. See, for example, Articles 22 and 23 of the EU Directive.

230. See, for example, the Canadian-based *Sympatico* Web site (www1.sympatico.ca).

231. This is envisaged by, for example, Article 24 of the EU Directive.

232. For instance, the US *Fair Credit Reporting Act* imposes criminal sanctions on those who obtain a credit report under false pretences.

233. See, for example, *Easy i* who publish corporate educational videos and computer software relating to privacy protection (www.easyi.com/products/hwc.asp).

234. See www.coe.int.

235. See www.ftc.gov/privacy/index.html.

236. See, for example, official Web sites in Australia (www.privacy.gov.au); France (http://www.cnil.fr/), Spain (https://www.agenciaprotecciondatos.org); and the United Kingdom (www.ukonline.gov.uk/Home/Homepage/fs/en).

237. See www.the-dma.org.

238. See www.cdt.org/privacy/guide/basic/topten.html.

239. See www.epic.org/privacy.

240. See www.truste.org/partners/users_primer.html.

REFERENCES

COE (Council of Europe) (1980), "Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data of 18 September 1980", http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=108&CM=1&DF=21/07/03.

COE (2001), "Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" ETS No. 108, http://conventions.coe.int/treaty/en/Treaties/Html/181.htm.

DMA (Direct Marketing Association) (1998),"Testimony of the DMA before the Subcommittee on Communications, Committee on Commerce, Science and Transportation of The United States Senate", 17 June, www.the-dma.org.

Dix, Alexander (1996), "The German RailwayCard: A Model Contractual Solution of the 'Adequate Level of Protection' Issue?", 18th International Privacy and Data Protection Conference, Ottawa, Canada, 18-20 September, www.datenschutz-berlin.de/sonstige/konferen/ottawa/alex3.htm.

EU (European Union) (1995), "Directive 95/46/EC of the European Parliament and of the Council of the European Union of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data", OJ no.L281 of 23/11/1995, 31, European Parliament and the Council, Brussels.

EU (1997a), "Discussion Document DG XV WP 4", adopted by the Working Party 4 on 26 June 1997.

EU (1997b), "Directive 97/66/EC", European Parliament and the Council, Brussels.

EU (1998), "Judging Industry Self-regulation: When Does it Make a Meaningful Contribution to the Level of Data Protection in a Third Country?", DG XV WP 7, adopted by the Working Party 7 on 14 January 1998.

Froomkin, Michael (1996), "The Essential Role of Trusted Third Parties in Electronic Commerce", 75 Oregon L. Rev. 49.

Goldberg, Ian, David Wagner and Eric Brewer (1997), "Privacy-Enhancing Technologies for the Internet", www.cs.berkeley.edu/~daw/papers/privacy-compcon97-www/privacy-html.html.

International Working Group on Data Protection in Telecommunications (1996), "Budapest-Berlin Memorandum", www.datenschutz-berlin.de/diskus/13_15.htm.

Kang, Jerry (1998) "Information Privacy in Cyberspace Transactions", 50 Stan. L. Rev. 1193-1294, at 1224-1230.

OECD (1980) *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris, www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

UN (United Nations) (1990), “The United Nations High Commissioner for Human Rights’ Guidelines for the Regulation of Computerised Personal Data Files”, Resolution 45/95 of 14 December 1990, www.unhchr.ch/html/menu3/b/71.htm.

UN (1997) The “Report of the Secretary-General on the Question of the Follow-up to the Guidelines for the Regulation of Computerized Personal Data Files”, Report E/CN.4/1997/67 of the Economic and Social Council, 23 January.