For Official Use **DSTI/ICCP/REG(98)12**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

OLIS : 01-Sep-1998
Dist. : 02-Sep-1998

Or. Eng.

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

DSTI/ICCP/REG(98)12
For Official Use

Group of Experts on Information Security and Privacy

DRAFT INVENTORY OF PRIVACY INSTRUMENTS AND MECANISMS FOR IMPLEMENTING AND ENFORCING THE OECD PRIVACY GUIDELINES ON GLOBAL NETWORKS

The Secretariat has compiled this Draft Inventory of instruments and mechanisms for protecting personal data and privacy on global networks. The scope of the inventory includes instruments, such as treaties, constitutions, laws, regulations, self-regulatory codes and other guidance instruments, as well as mechanisms such as technologies, contracts, practices, institutions, and administrative, civil and criminal procedures for the implementation and enforcement of privacy principles. The inventory includes initiatives from both the public and private sectors, and at the international, regional and national levels.

This Draft should form the basis for further input to compile an inventory that is as complete and accurate as possible. The Group of Experts is invited to review this document, to provide comments on the text and to contribute material and references to assist the Secretariat in finalising the inventory. Written input is requested no later than 21 September 1998.

Anne Carblanc
Email: anne.carblanc@oecd.org Fax: (33 1) 45 24 93 32

68595

Document complet disponible sur OLIS dans son format d'origine
Complete document available on OLIS in its original format

Or. Eng.

TABLE OF CONTENTS

PREFACE

1. 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.

2. 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 who 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.

3. In that context, a Workshop entitled "Privacy Protection in a Global Networked Society" was organised with the support of the 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 type of policies for protection of personal data offered by the legislators in the European Union and the different policies of other 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.

4. 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:

- identifying and balancing the needs of the private sector and of those of users and consumers and formulating efficient strategies for "educating for privacy";

- developing "privacy enhancing technologies";

- implementing private sector-developed enforcement mechanisms for privacy codes of conduct and standards; and

- adopting model contractual solutions for transborder data flows.

5. At the end of the Workshop, participants recognised that the growth of electronic commerce requires increased consumer confidence in privacy protection, 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 human rights and to prevent interruptions in transborder data flows.

6. 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.

7. The Chair also highlighted the need to survey the available instruments (including law, self regulation, contracts, and technology) in order to assess their practical application in a networked environment and their ability to meet the objectives of the OECD Guidelines (including effectiveness, enforceability, redress and coverage across jurisdictions). Such a study would serve to identify gaps and barriers to interoperability, and provide a basis to suggest solutions to provide seamless privacy protection.

8. At its May 1998 meeting, the Group of Experts on Information Security and Privacy agreed that this *Draft Inventory of Privacy Instruments and Mechanisms for Implementing and Enforcing the OECD Privacy Guidelines on Global Networks* ("Inventory") would be prepared by the Secretariat as a separate document and for further consideration, comment and approval at the October 1998 meeting.

INTRODUCTION

9. 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.

10. Simply "browsing" on the Web can make a considerable quantity of information available to the sites visited. 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 Website being accessed)[1]. 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).

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

12. 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 include the user's name, address, home or work telephone number and e-mail address. Data relating to age, sex, marital status, occupation, income, occupation 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. Also, if a visitor is asked to send information to a Website 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".

13. "Cookies"[4] are computer files created by a Website 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 the current and subsequent visits to the Website[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 site is visited. Information which is subsequently collected about the user can then be linked to this code number.

14. Thus, although the development of global networks and digital technology has brought many social and economic benefits, it has also increased the opportunities for personal information to be misused. In particular, 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.

15. 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.

16. This Inventory is divided into two main Sections. Section I, describes the international 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 such guidelines on global networks. In addition, a list of contact details for many of the public, private, national and international privacy organisations mentioned in this Inventory is included as an Appendix.

I. GUIDANCE INSTRUMENTS

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

18. 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.

19. 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).

20. A majority of 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.

21. 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. However, public authorities may also be involved in the development, implementation and enforecement 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 Instruments and Organisations

1. Intergovernmental Legal Instruments

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

Status

22. The *Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (the "OECD Guidelines")[7] 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"[8].

23. The principles that comprise the OECD Guidelines have been applied in many countries through a variety of instruments.

Scope

24. 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"[9], 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.[10]

Basic Principles

25. 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, and 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

26. The OECD Guidelines oppose the imposition of unnecessary impediments to transborder data flows[11]. 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

27. The OECD Guidelines create a framework for future co-operation[12]. The areas of future co-operation include advising other Member countries as to their obervance of the Privacy Principles, 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 provide mutual investigative assistance, and developing principles, domestic and international, to determine the applicable law in the case of transborder flows of personal data.

Provisions on Implementation and Enforcement

28. 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[13]. This is to be accomplished by: 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

29. The OECD, through the *Information, Computer and Communications Policy Committee* (the "ICCP Committee"), continues to work in this area and provide a forum for discussing privacy and data protection issues, including the challenges presented by the emergence of global networks[14].

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

Status

30. *Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data* of 18 September 1980[15] ("Convention 108") was opened for signature by the *Committee of Ministers* of the *Council of Europe*[16] on 28 January 1981. Since then, it has been signed by 23 Countries and ratified by 21[17]. Convention 108 is a binding instrument in international law.

Scope

31. The terms of the Convention apply to automated personal data files and automatic processing of personal data in the public and private sectors[18].

Basic Principles

32. 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") such as personal data revealing personal beliefs, concerning health or relating to criminal convictions[19].

Provisions on Data Flows

33. The principles of the Convention encourage the free flow of personal data between parties to the Convention who provide equivalent protection[20].

Provisions on Further Co-operation

34. 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[21]. 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

35. Each contracting State undertakes to take the necessary measures in its domestic law to give effect to the basic principles of data protection[22], 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".

Ongoing Work

36. Through the Consultative Committee, the Council of Europe continues its work in the area of privacy protection. The Council of Europe's *Project Group on Data Protection* has also issued draft Guidelines on "The Protection of Privacy on the Internet" (May 1998)[23].

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

Status

37. The *United Nations High Commissioner for Human Rights' Guidelines for the Regulation of Computerised Personal Data Files* (Resolution 45/95 of 14 December 1990)[24] (the "UN Guidelines") 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. Article 4 of the UN Guidelines requests Member countries to take the guidelines into account in their legislation and administrative regulations.

Scope

38. 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

39. The "Principles concerning the minimum guarantees that should be provided in National Legislation" broadly reflect the basic principles in the OECD Guidelines, although, there is no specific accountability principle. The UN Guidelines add allowances for "sensitive data" within the "Principle of non-discrimination"[25].

Provisions on Transborder Data Flows

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

Provisions on Implementation and Enforcement

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

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

Ongoing Work

43. A 1997 report[26] 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

44. Directive 95/46/EC of the European Parliament and of the Council 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* (the "EU Directive")[27] is a binding instrument that must be implemented by the 15 EU Member States in October 1998.

Scope

45. The Directive applies generally to the processing of personal data by a "controller" in an EU Member State[28]. It therefore applies to data about natural, whether held by the public or private sector. Most categories of manual and computerised data processing are covered[29].

Basic Principles

46. 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[30], detailed disclosure requirements[31], registration provisions[32], "opt-out" rights for data subjects to refuse commercial solicitations[33] and redress rights[34].

Provisions on Transborder Data Flows

47. The EU Directive promotes transborder data flows within the EU, but may restrict transfers to third countries. Member States are not permitted to inhibit the free movement of personal data within the EU simply for reasons of privacy protection[35]. However, before a member state may transfer personal data

outside the EU, an "adequate" level of protection must exist in the recipient country[36]. 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 explicit consent of the data subject has been obtained[37].

Provisions on Implementation and Enforcement

48. 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 and the ability to engage in legal proceedings[38].

49. With respect to enforcement, the EU Directive covers judicial remedies, liabilities and sanctions[39]. 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 are free to adopt suitable administrative, civil or criminal sanctions.

Provisions on Further Co-Operation

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

51. 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

52. 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"[40] and "Judging Self-Regulation"[41].

(e) General Agreement on Trade in Services

53. The *General Agreement on Trade in Services* ("GATS")[42] is a multilateral agreement which aims to promote free trade in services. GATS is administered by the *World Trade Organisation* ("WTO"[43]). 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"[44].

54. [*The OECD intends to develop a section on national discrimination under the WTO agreements and the dispute resolution procedure followed by the WTO.*]

2. International Colloquia on Privacy Protection

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

(a) Annual International Conferences of the Data Protection Commissioners

56. 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 19th International Conference of Privacy Data Protection took place in Brussels[45].

(b) Conferences of the EU Data Protection Commissioners

57. 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

58. 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[46].

(d) International Organisation for Standardisation

59. The International Organisation for Standardisation (the "ISO")[47] 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*[48]. An *Ad Hoc Advisory Group on Privacy* is now studying 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. [49]

(e) International Chamber of Commerce

60. The International Chamber of Commerce (the "ICC")[50] represents international businesses all over the world and has produced a number of documents and industry codes on the protection of personal privacy and information flows. These have included a "Code of Direct Marketing" with privacy provisions[51]. The ICC is also developing privacy guidelines for Internet access providers and Web operators which will address issues such as consumer empowerment, third party verification, the use of privacy enhancing technologies and enforcement mechanisms. Finally, the ICC is currently drafting a model contract for transborder flows of personal data[52].

(f) International Federation of Direct Marketing Associations

61. The *International Federation of Direct Marketing Associations* (the "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 on-line activities.

(g) Electronic Commerce Europe

62. *Electronic Commerce Europe* ("EDE")[53] 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

63. 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*[54] ("EPIC") which is 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*[55] (the "CDT") which is a public interest organisation working for public policies that advance civil liberties and democratic values in new computer and communications technologies;

- *Privacy International*[56] which is a human rights group formed to act as a watchdog on surveillance by governments and corporations; and

- *PrivacyExchange.Org*[57] which is 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

64. The *Privacy Act 1988*[58] provides privacy protection with respect to federal government agencies in Australia. The Act establishes the office of the *Privacy Commissioner*[59] and sets out eleven *Information Privacy Principles* ("IPPs") based upon the OECD Guidelines. The Commissioner can receive complaints, conduct investigations and make determinations (including compensation orders) that are enforceable in the *Federal Court*.

Federal Approach to Privacy in the Private Sector

65. The application of the Privacy Act to the private sector (and state and local governments) is very limited. The Act applies only in relation to specific categories of information; tax file numbers and consumer credit information[60].

66. The Australian Government is currently considering whether or not to introduce general private sector privacy legislation. In March 1997, the Prime Minister proposed that in order to avoid increased regulatory burden on business, a self-regulatory approach would be followed. To provide industries with guidance for the development of voluntary codes of conduct, the Privacy Commissioner has released a set of *National Principles for the Fair Handling of Personal Information* (the "National Principles")[61]. The *Online Council*, which is comprised of a Minister from each State and Territory, is to consider the appropriateness of the National Principles in the online environment and provide feedback to the Privacy Commissioner.

67. A recent report by the *Joint Committee of Public Accounts and Audit*[62] recommends a legislative approach. It states that to ensure compliance by companies and to encourage consumer confidence, "the Australian Government [should] introduce privacy legislation ... to govern the use of personal information in the private sector"[63]. The issue is currently being considered by the *Senate Legal and Constitutional References Committee* whose report is expected shortly.

Other Federal Laws with Privacy Provisions

68. 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 (*Data-matching Program (Assistance and Tax) Act 1990*), and for specific procedures, such as the interception and disclosure of personal information by telecommunications companies (*Telecommunications Act 1997*)[64].

State and Territory Laws

69. There are many State and Territory laws which provide some form of privacy protection. In the Australian Capital Territory, for example, there is legislation dealing with privacy and the confidentiality of personal health information[65]. The *Privacy Committee Act 1975 (NSW)*[66] establishes the *New South Wales Privacy Committee* which conducts research relating to privacy issues and acts as a dispute conciliator.[67] The Committee can also receive and investigate complaints regarding violations of privacy by both the public and private sectors, but it has no decision-making powers. In South Australia a *Cabinet Administrative Instruction* (No. 1 of 1989) implements the federal IPPs as guidelines for Sate government agencies. Finally, a *Data Protection Bill* has been proposed by the Victorian Government which would have the effect of applying the National Principles in both the private and public sectors[68].

Self-Regulatory Instruments

Instruments Relating to Online Privacy

70. In February 1998, the *Internet Industry Association* released a draft voluntary *Industry Code of Practice*[69] that proposes general standards of behaviour for those involved in the Internet industry[70]. The Code reflects the OECD Guidelines and the National Principles. It is proposed that the Code would utilise a compliance icon and that an *Administrative Council* would be created for hearing complaints. A draft set of principles for consumer protection in electronic commerce, which reflect the OECD Guidelines, has also been prepared by the *National Advisory Council on Consumer Affairs*[71].

Other Initiatives

71. Other self-regulatory initiatives include:

- *Smart Card Industry Code of Conduct* developed by the *Asia-Pacific Smart Card Forum*;[72]
- *Privacy Principles for Intelligent Transport Systems* developed by *Standards Australia*; and
- The *Australian Communications Industry Forum* (the "ACIF")[73] is in the process of drafting a Code dealing with telecommunications privacy issues, such as, customer personal information and calling number display.[74] The ACIF has also published guidelines on the *Development of Telecommunications Industry Consumer Codes* (January 1998)[75] which aid the development of codes pursuant to Part 6 of the *Telecommunications Act 1997*.

AUSTRIA

Laws

Federal Comprehensive Laws

72. The *Federal Data Protection Act* (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 [76].

73. An independent Commission (the *Bundeskanzleramt*), which is a division of the *Federal Chancellery*, is responsible for enforcing the law, administering the registration system and authorising transborder data flows. The Commission acts on specific complaints, 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.

74. 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

75. There are many federal laws in Austria which relate to personal privacy. For example, the *Austrian Telecommunications Act* (1997)[77] 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)[78]. Finally, the *Genetic Engineering Act 1994* contains genetic data protection provisions.

Implementation of the EU Directive

76. A first draft of the *Datenschutzgesetz* was issued recently. This is the legislation which will implement the EU Directive in Austria. While the draft has not yet been made public, a consultation procedure has begun with other Ministries and "social partners" (such as industry groups and labour unions)[79].

Laender (State) Laws

77. 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

78. 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

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

Laws

Comprehensive Laws

80. 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 Privee*[80]. The Commission handles data processing registrations and may also advise the government on privacy matters.

81. 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 the breach of privacy obligations[81].

Other Laws with Privacy Provisions

82. 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

83. A draft law designed to implement the Directive and based on the structure of the 1992 Law, is now before the Belgian Parliament[82].

Self-Regulatory Instruments

84. 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[83].

CANADA

Laws

Federal Laws

85. The *Privacy Act* (1983)[84] applies to federal government departments 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.

86. The *Privacy Commissioner*[85] 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

87. The Canadian federal government has expressed its intention to develop privacy legislation to protect personal information in the private sector[86]. The options for legislation are canvassed in a discussion paper, "The Protection of Personal Information: Building Canada's Information Economy and Society"[87], which was published by the *Task Force on Electronic Commerce* (formed by *Industry Canada* and *Justice Canada*) in January 1998.

Other Federal Laws with Privacy Provisions

88. [*The OECD intends to develop this section as more information becomes available.*]

Provincial Laws

89. 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[88]. Various sectoral statutes provide privacy protection in areas such as personal health information[89].

90. Quebec is the only province where general legislation, the *Act Respecting the Protection of Personal Information in the Private Sector* (1993),[90] regulates the handling of personal information by private sector organisations.

Self-Regulatory Instruments

The CSA Model Code

91. 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*[91] of the

Canadian Standards Association (the "CSA") and was adopted as a National Standard by the *Standards Council of Canada* in 1996[92]. The Code reflects the OECD Guidelines, but also requires companies to identify an officer accountable for compliance and to whom complaints may be addressed.

92. The CSA has prepared a workbook, "Making the CSA Privacy Code work for You"[93], 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. An example of such a certified code is the Canadian Bankers' Association *Privacy Model Code*.[94]

Instruments Relating to Online Privacy

93. The *Canadian Association of Internet Providers'* (the "CAIP's") voluntary *Code of Conduct*[95] 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.

Other Initiatives

94. Other self-regulatory privacy initiatives include:

- *Privacy Code Guidelines* developed by the *Canadian Direct Marketing Association* (the "CDMA"); and
- *STENTOR Telecom Policy, Inc's* model telecommunications code.

CZECH REPUBLIC

Laws

Comprehensive Laws

95. The *Protection of Personal Data in Information Systems Act* became effective on 1 June 1992.[96] The Act covers computerised data on natural persons and applies to both the public and private sectors.

96. 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.

97. In anticipation of the Czech Republic joining the EU, the Government has appointed the *Office for the State Information System* (the "OSIS") to prepare new legislation that will be compatible with the EU Data Protection Directive[97]. 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

98. 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.

Self-Regulatory Instruments

99. [*The OECD intends to develop this section as more information becomes available.*]

DENMARK

Laws

Comprehensive Laws

100. The *Public Authorities Registers Act* was passed in June 1978[98]. The Act covers computerised data on natural and legal persons which are kept by or for a public authority. Disputes under the Act may be referred to the *Data Surveillance Authority* (the *Registertilsynet*)[99] whose decisions are final[100]. Under the Act, violations of the privacy law are punishable by fine or detention [101].

101. Denmark also has privacy legislation applying to the private sector. Under the *Private Registers Act*[102], credit reference agencies, data processing service bureaux and direct mail agencies are required to register with the Data Surveillance Authority, and prior notification is required for processing sensitive data. As with the Public Authorities Registers Act, the Authority's decisions are final[103] and violations are punishable by fine or detention[104].

Other Laws with Privacy Provisions

102. Specific legislation has been passed in Denmark on the right of access to information held by the media (*Media Information Databases Act* (1993)) and to restrict the use of health data in determining employment prospects (*Use of Health Data in Employment Matters Act* (1996)).

Implementation of the EU Directive

103. A proposal to implement the EU Directive was introduced to the Danish Parliament (the *Folketinget)* on 30 April 1998,[105] but lapsed when the parliamentary session ended in June. In September,

a parliamentary hearing will be held with independent experts. A new proposal is expected in October, when the new parliamentary session commences.

Self-Regulatory Instruments

104. The *Danish Consumer Ombudsman* is in the process of preparing a code of conduct for sales and marketing via electronic media which will take into account the OECD Guidelines.

FINLAND

Constitution

105. Section 8 of the *Finnish Constitution* provides that each individual's privacy, honour and domicilary peace shall be protected and that the use of personal data shall be prescribed by law.

Laws

Comprehensive Laws

106. The *Personal Data File Act* (1987)[106] covers computerised and manual records of natural persons in both the public and private sectors. There are two overseeing bodies, the *Data Protection Ombudsman*[107] who has investigative and advisory powers, and the *Data Protection Board* who hears cases pursuant to the Act and has the power to authorise the export of sensitive data to other countries. If recommendations made by the Ombudsman are not observed, the Ombudsman may refer the case to the Data Protection Board[108]. Decisions of the Board may be reviewed by the *Supreme Administrative Court*[109].

107. The Act includes civil remedies (for example, data controllers must compensate data subjects from unlawful data use) and criminal sanctions for violations[110].

Other Laws with Privacy Provisions

108. Sectoral legislation, such as the *Statistics Act* and the *Act on the Medical Research Development Centre*[111], contain privacy protection provisions. A draft *Telecommunication Marketing Act* is being prepared.

Implementation of the EU Directive

109. A *Ministry of Justice* Committee has drafted a proposal for the revision of the Personal Data File Act to conform with the EU Directive. The proposal extends the rights of data subjects and the powers of

the two data protection authorities. It also includes a provision for the approval of sectoral codes of conduct by the authorities. Work on implementing the Directive in specialised legislation is also underway.

Self-Regulatory Instruments

110. The Finnish *Rules for Electronic Consumer Trade* were prepared jointly by the *Finnish Direct Marketing Association* and the *Federation of Commerce and Trade*. The introduction notes that an electronic vendor should follow the Personal Data File Act and other data protection laws. The Rules include provisions regarding: data security; the recording of personal data about consumers (making reference to the EU Data Protection Directive); and the right to opt-out.

FRANCE

Laws

Comprehensive Laws

111. 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. Law 78/17 is supplemented by the *Penal Code*.[112]

112. 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* (the "CNIL")[113]. The data protection authority's roles include 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 complaints and queries, carries out investigations, and ensures that data subjects may exercise rights of access.

113. Unlawful processing or transfer of named data is punishable under Law 78/17 by fines and/or imprisonment[114]. 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

114. Sectoral laws with privacy provisions include, inter alia, the *Labour Code*[115], the *Law on Video Surveillance* (1995)[116], and the *Law on the Use of Medical Prescriptions for Marketing* (1996)[117].

Implementation of the EU Directive

115. A report on implementing the EU Directive was issued on 3 March 1998[118], and a Bill is being prepared by the *Ministry of Justice*. The Bill will be discussed at the ministerial level before submission to the *French Parliament*. The *National Commission for Human Rights* and the CNIL are to be consulted on the draft law.

Self-Regulatory Instruments

Instruments Relating to Online Privacy

116. The "*Charte de l'Internet"*[119] (Internet Charter) is a self-regulatory initiative for Internet actors[120]. The Charter creates an independent supervisory body, the *Internet Council* ("*Conseil de l'Internet"*), with advisory and mediation powers. The stipulations under the Charter include the right to use anonymous services, and the obligation on Internet actors to inform users of the data being collected.

Other Initiatives

117. The *SEVPCD*[121], a professional association for distance marketers, has developed a code of conduct designed to accord with the Law 78/17[122]. Only members complying 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

118. Germany's *Federal Data Protection Act* (1990)[123] 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.

119. 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[124]. 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[125].

Other Federal Laws with Privacy Provisions

120. The German Federal government has enacted a significant number of specific issue laws and regulations[126] 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*[127]).

121. Article 2 of the Federal *Information and Communication Services Act* (1997)[128] 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.

Laender (State) Laws

122. Each *Land* has its own data protection law covering its public sector, as well as its own data protection authority[129]. The Data Protection Commissioners of the Federation and the Laender hold regular conferences[130].

Implementation of the EU Directive

123. The Federal Government and Laender are currently working on new legislation to implement the EU Directive[131]. 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

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

GREECE

Constitution

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

Laws

Comprehensive Laws

126. 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[132]. 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[133].

127. The Law gives data subjects the right to be informed of, and have access to, their personal data and to apply to the Court for the suspension of certain processing operations[134]. The Law provides civil damages for losses caused in contravention of the law[135], administrative sanctions (such as fines and the cancellation of data processing licences)[136] and criminal sanctions[137].

Other Laws with Privacy Provisions

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

Self-Regulatory Instruments

129. 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

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

Laws

Comprehensive Laws

131. The law on the *Protection of Personal Data and Disclosure of Data of Public Interest* (1992)[138] 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[139]. The

Commissioner is responsible for observing the implementation of the Act, investigating complaints and maintaining the Data Protection Register.

132. 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)[140]. The Act also provides for remedies (including compensation) for breaches. Remedies may either be pursued through application to the Commissioner[141] or by initiating court proceedings[142].

Other Laws with Privacy provisions

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

Self-Regulatory Instruments

134. [*The OECD intends to develop this section as more information becomes available.*]

ICELAND

Laws

Comprehensive Laws

135. 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[143], and authorising the processing of data abroad.

136. Data subjects have rights of access to personal data, and can demand rectification or deletion[144]. Data subjects can also request that their names be deleted from direct mailing lists[145]. 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[146].

137. The 1989 Law contains criminal sanctions for the infringement of certain provisions[147].

Other Laws with Privacy provisions

138. [*The OECD intends to develop this section as more information becomes available.*]

Self-Regulatory Instruments

139. [*The OECD intends to develop this section as more information becomes available.*]

IRELAND

Constitution

140. The Irish Constitution recognises a right to privacy[148].

Laws

Comprehensive Laws

141. 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.

142. 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.

143. 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[149]. Civil litigation may be used by data subjects to seek compensation for violations of the Act.

Other Laws with Privacy Provisions

144. 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

145. A draft Bill to implement the EU Directive has been submitted to the Attorney-General's office and will go to Parliament towards the end of 1998. This follows the "Consultation Paper on Transposition into Irish Law" produced by the *Department of Justice Equality and Law Reform* (November 1997)[150].

Self-Regulatory Instruments

146. The *Irish Direct Marketing Association's* (the "IDMA's") Code of Conduct[151] 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, and complaints may be addressed to the IDMA Board whose powers include expulsion from the Association.

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

ITALY

Laws

Comprehensive Laws

148. Italy's *Data Protection Act* (adopted on 31 December 1996) implements the EU Directive[152]. Following the Directive, the Act covers both computerised and manual personal data of natural and legal persons in the public and private sectors. The supervisory office established to oversee the implementation of the Act is the *Guarantor of the Protection of Personal Data.* The Guarantor supervises the registration process, investigates complaints and assists in the development of sectoral codes [153].

149. The Act provides that organisations who cause damage by the unlawful processing of personal data are liable to pay damages pursuant to the Italian Civil Code[154]. Breaches of the Act may be pursued either through the courts or via the Guarantor.

150. The Guarantor may fine organisations for failing to provide information required by the Act. The Act also includes criminal sanctions (imprisonment) for violations such as unlawful processing. As a "collateral punishment" convictions are published in the press[155].

Other Laws with Privacy Provisions

151. Laws and regulations with privacy provisions include: legislative decrees pursuant to the Data Protection Act; telecommunications legislation;[156] *Labor Decree n. 39/93*[157] which establishes the *Authority for Information Technology in the Public Administration*[158] to support public agencies in the development and use of information systems; and *Law No. 59 of 15 March 1997* (supplemented by *Presidential Decree No. 513 of 10 November 1997*) which concerns the use of computerised data in the public sector.

Self-Regulatory Instruments

152. A voluntary Code of Conduct which addresses privacy on the Internet was approved by the *Associazone Italiana Internet Providers* (the "AIIP")[159] in early 1998. The AIIP is also working in

conjunction with the Italian Supreme Court and the Milan Chamber of Commerce, to establish regulatory and dispute settlement bodies, and create an online arbitration forum.

JAPAN

Laws

Public Sector Laws

153. The *Act on Protection of Computer Processed Personal Data held by Administrative Organs* (1988)[160] controls computer-processed personal data held by national agencies in Japan. The Act generally conforms to the OECD Guidelines[161]. The legislation is co-ordinated by the *Management and Co-ordination Agency*[162] (the "MCA") within the *Prime Minister's Office*. Data users are accountable to the MCA, who also provides advice on the implementation of the Act[163].

154. Under the Act, data subjects have a right of access to their personal data, and can complain to the "head" of the data user about difficulties in exercising this right.

Approach to Privacy Regulation in the Private Sector

155. The report of the *Ministry of Posts and Telecommunications'* (the "MPT's") *Study Group on Developing Legal Environment for Advanced Info-Communications Society* (March 1998) considers the establishment of a legal framework, based on the OECD Guidelines and involving a central registration system, for protecting online personal information held by the private sector[164]. The Japanese Government has also actively encouraged the adoption of codes of conduct by the private sector (see below).

Other Laws with Privacy Provisions

156. [*The OECD intend to develop this section as more information becomes available.*]

Local Authority Laws

157. 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[165].

Self-Regulatory Instruments

158. 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"[166].

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[167]. To enforce industry codes, a certification and privacy trustmark project is currently being tested by the *Japan Processing Development Center*[168].

159. The *Electronic Network Consortium*[169] (the "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.

160. 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)[170]. Guidelines have also been produced by the *Electronic Commerce Promotion Council* ("ECOM")[171]. The *ECOM Privacy Issues Working Group* has issued "Guidelines Concerning the Protection of Personal Data in Electronic Commerce in the Private Sector" (March 1998)[172] 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.

161. 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.[173]

162. Other self-regulatory privacy initiatives include:

- The MPT has produced a number of Guidelines for telecommunications operators with privacy provisions including "Guidelines for the Protection of Personal Data in the Telecommunications Industry" (1991); "Guidelines for the Protection of Personal Caller Information in the Use of Caller Identification Services"; and "Guidelines on Protection of Subscriber's Personal Information in Broadcasting" (1996); and

- The *Centre for Financial Industry Information Systems* has produced "Guidelines on the Protection of Personal Data for Financial Institutions" which are based on the OECD Guidelines.

KOREA

Laws

Public Sector Laws

163. 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

164. 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

165. Discussions are expected regarding government regulation on the protection of personal information in the private sector.

Self-Regulatory Instruments

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

LUXEMBOURG

Laws

Comprehensive Laws

167. The *Nominal Data (Automatic Processing) Act* (1979)[174] 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, and performs an advisory function. The

Minister is also assisted by an oversight authority, the *autorité de contrôle*[175]. Breaches of the privacy legislation can be referred to a prosecuting authority by the Minister.

168. The 1979 Act provides criminal sanctions (imprisonment or fines) for breaches of its provisions[176].

Other Laws with Privacy Provisions

169. 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[177].

Implementation of the EU Directive

170. A parliamentary Bill has been drafted to implement the EU Directive[178]. It was introduced to the Chamber of Deputies on 8 October 1997.

Self-Regulatory Instruments

171. [*The OECD intend to develop this section as more information becomes available.*]

MEXICO

Constitution

172. 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

173. 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[179].

Self-Regulatory Instruments

174. [*The OECD intend to develop this section as more information becomes available.*]

THE NETHERLANDS

Constitution

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

Laws

Comprehensive Laws

176. The *Data Protection Act* (1988) (as supplemented by a Royal Decree of 1993 with respect to sensitive data) applies to both the public and private sectors, and covers computerised and manual records. The Act's registration requirements are administered by the independent *Registration Chamber* (the *Registratiekamer*)[180]. The Registration Chamber has the power to investigate breaches of the law and to enforce its provisions. It does not have to act on complaint to conduct an inquiry.

177. If a request for the provision of information or the rectification of personal data is refused by a data controller, then the data subjects may apply to the *District Court* for review[181]. The Act also provides criminal sanctions for violations[182].

Other Laws with Privacy Provisions

178. There has been specific legislation in The Netherlands regarding police files (*Police Registration Act* (1991)) and medical data (*Medical Treatment Information Act* (1995)). There is also a regulation of 14 May 1994 concerning personal data about foreigners.

Implementation of the EU Directive

179. A draft Bill[183] designed to implement the EU Directive has gone before the Dutch Parliament. The Report from the Ministry of Justice in response to the initial examination of the bill is awaited, and Parliamentary debate on the bill will recommence in September/October 1998.

Self-Regulatory Instruments

180. The law in The Netherlands encourages individual business and professional sectors to develop their own codes of conduct. The Registration Chamber is responsible for approving such codes which do not become legally binding, but are intended to give guidance in interpreting the law. Some 12 codes of

conduct have been approved (examples include the *Association of Commercial Information Bureaus*, the *Banking Association*, and the *National Chipcard Platform)*[184].

NEW ZEALAND

Laws

Comprehensive Laws

181. *The Privacy Act 1993* applies to computerised and manual "personal information" held by almost all public and private organisations in New Zealand. The core of the Act is a set of 12 *Information Privacy Principles* ("IPPs") which are based on the OECD Guidelines. The Act also includes rules on data matching between government agencies[185].

182. The Act establishes the position of a *Privacy Commissioner*[186] (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 IPPs[187].

183. Neither the IPPs 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*[188] which has broad relief-granting powers.

Other Laws with Privacy Provisions

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

Self-Regulatory Instruments

185. In terms of the Internet industry, the *Internet Society of New Zealand* has developed an "Internet Service Provider Code of Practice"[189].

186. 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 IPPs 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*[190] and the *Justice Sector Unique Identifyier Code 1998*[191].

NORWAY

Laws

Comprehensive Laws

187. Norway's 1978 legislation for the protection of personal data covers both the public and private sectors and applies to manual and computerised records on natural and legal persons[192]. Subsequent amendments to the Act cover direct postings, telemarketing and consumer credit information.

188. The Act introduces a central registration system which is administered by an independent *Data Inspectorate* (the *Datatilsynet*)[193]. The Data Inspectorate enforces the Act and conducts inspections of data practices. The *Ministry of Justice* is the appeal body for decisions made by the Inspectorate.

189. Under the Act, individuals have 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 of 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[194].

Other Laws with Privacy Provisions

190. [*The OECD intend to develop this section as more information becomes available.*]

Implementation of the EU Directive

191. Following the adoption of the EU Directive, and in the light of technological developments in data collection, a government committee was appointed to consider legislative changes. The Norwegian Parliament will consider the committee's proposals for revised legislation in late 1998.

Self-Regulatory Instruments

192. [*The OECD intend to develop this section as more information becomes available.*]

POLAND

Constitution

193. Article 51 of the *Polish Constitution* confers rights of protection for personal data[195].

Laws

Comprehensive Laws

194. The *Act on the Protection of Personal Data* (1997)[196] 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)[197].

Other Laws with Privacy Provisions

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

Self-Regulatory Instruments

196. [*The OECD intend to develop this section as more information becomes available.*]

PORTUGAL

Constitution

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

Laws

Comprehensive Laws

198. The *Protection of Personal Data Act* (1991)[198] 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[199] 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.

199. The Act creates a right of access for data subjects along with the right of correction/erasure[200]. Violations of the Act[201], as well as the Constitution, are criminal offences.

Other Laws with Privacy Provisions

200. There are a number of laws and regulations containing data protection provisions in Portugal. These include the Law on computer crime (1991)[202], regulations establishing institutions such as a registry of non-donors of human organs[203] and a Centre of Identity cards[204], and regulations controlling the data bases operated by the Gendarmerie[205], the Border and Foreign Services[206] and the Criminal Police[207].

Implementation of the EU Directive

201. 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.

Self-Regulatory Instruments

202. [*The OECD intend to develop this section as more information becomes available.*]

SPAIN

Constitution

203. 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

204. The *Law on the Regulation of the Automated Processing of Personal Data* (1992)[208] covers computerised records in the public and private sectors. Its implementation is overseen by an independent public authority, the *Data Protection Agency*[209]. 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.

205. The Law provides that sanctions should be determined according to the nature and size of the violation[210].

Other Laws with Privacy Provisions

206. There is a Spanish Law on public statistics[211] with privacy provisions.

Local Authority Laws

207. [*The OECD intend to develop this section as more information becomes available.*]

Implementation of the EU Directive

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

Self-Regulatory Instruments

209. The *Spanish Association of Electronic Commerce* (which is part of the *Spanish Direct Marketing Association*) has a Code of Conduct on Internet privacy[212]. 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

210. The Swedish Constitution guarantees the right of individuals to have access to documents and data held by public authorities.

Laws

Comprehensive Laws

211. A Parliamentary resolution of 16 April 1998 approved the *Personal Data Act* which implements the EU Directive in Sweden[213]. The Act becomes effective on 24 October 1998. The new Act represents a

legal framework for all processing of personal data which may be supplemented by regulations of the Government and the Data Inspection Board (the *Datainspektionen*)[214]. The Act confers on the Data Inspection Board a role of supervision and advice-giving. It will also have a right to seek rectification and impose penalties for contraventions of the Act. The penalties for violating the Act primarily comprise damages in favour of the data subject suffering loss.

Other Laws with Privacy Provisions

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

Self-Regulatory Instruments

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

SWITZERLAND

Laws

Federal Laws

214. The *Federal Law on Data Protection* (1992) (the "FLDP")[215] covers both computerised and manual data on natural and legal persons in the federal public sector and the private sector. The *Federal Data Protection Commissioner*[216] (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[217]. 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 acts as an arbitration and appeal body[218].

215. 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.

216. Data subjects may seek the usual remedies of the Swiss Civil Code[219], 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

217. 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

218. 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

219. A working group of the *Office Federal de la Justice* has formulated recommendations for Internet access providers called the *Internet Charter*[220]. The Charter includes recommendations on legal issues such as service provider liability and the disclosure of data to third parties.

Other Initiatives

220. 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

221. Turkey has a draft law on Data Protection which applies to both public and private sector data processing entities. It is 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 to oversee the application of the law.

222. According to the draft law, individuals will have rights to receive information whenever data are collected, to access data, to correct data and to object to certain types of data processing.

Self-Regulatory Instruments

223. [*The OECD intend to develop this section as more information becomes available.*]

UNITED KINGDOM

Laws

Comprehensive Laws

224. The United Kingdom's *Data Protection Act 1984*[221] covers computerised personal data of physical persons in the public and private sectors. It also establishes a central registry system which is overseen by an independent *Data Protection Registrar*[222]. The Registrar investigates complaints and advises on the application of the Act. An appeal lies to the Data Protection Tribunal against refusal of registration and enforcement notices.

225. The Registrar may issue "enforcement notices" against data users in breach of the Act. The decision to issue such a notice may be appealed to the *Data Protection Tribunal*. If a data user breaches the terms of such a notice they commit a criminal offence. It is also a criminal offence to procure or sell information knowing that the disclosure is not covered by the data user's register entry[223]. The Act also provides data subjects with civil remedies of compensation and rectification/erasure which may be enforced through the courts.

226. The law of the United Kingdom requires the Registrar to encourage the development of industry-based codes. Such codes aid in the interpretation of the law, but are not legally binding. The Registrar also publishes guidance notes; including a note on "Data Protection and the Internet".

Other Laws with Privacy Provisions

227. A number of laws in the UK have data protection implications including: the *Financial Services Act 1986*; the *Human Fertilisation and Embryology Act 1990*; the *Charities Act 1993*; and the *Criminal Justice and Public Order Act 1994*. The Government has also proposed *Freedom of Information Legislation* which will also have implications for Data Protection. *The Human Rights Bill,* currently before Parliament, will embody in domestic law the European Convention on Human Rights, including Article 8 on the right to private life.

Implementation of the EU Directive

228. The new Data Protection Act 1998 which received Royal Assent on the 16 July 1998 implements the EU Directive and should come fully into force in early 1999. Much of the detail of the new law will be contained in secondary legislation which will also come into force early next year..

229. A Data Protection Bill designed to implement the EU Directive was published in January 1998 and is currently going through the Parliamentary process[224]. Much of the detail of the new law will be contained in secondary legislation.

230. The *British Standards Institute* is working with the Data Protection Registrar to implement a data protection compliance programme in preparation for the implementation of the EU Directive[225].

Self-Regulatory Instruments

Instruments Relating to Online Privacy

231. The *Internet Service Providers Association (UK)*[226] has developed a Code of Conduct, which is voluntary for the first twelve 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

232. A number of other industry associations have produced codes of conduct that include data protection provisions[227].

UNITED STATES

Constitution

233. The US Constitution does not explicitly mention a right of privacy. However, case law has recognised that the Constitution confers such a right although primarily relating to physical privacy rather than personal information.

Laws

Federal Sectoral Laws

234. The use of personal information held by federal government agencies is regulated by the *Privacy Act* (1974)[228] 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.

235. Federal Acts with privacy implications for specific kinds of information include: [229]

- The *Fair Credit Reporting Act* (1970)[230] which regulates the use of information collected by consumer reporting agencies such as credit bureaux, medical information companies and tenant screening services. It is administered by the *Federal Trade Commission* (the "FTC")[231];

- The *Cable Communications Policy Act* (1984)[232] which regulates the use of cable television subscriber records under a regime of notice and consent;

- The *Electronic Communications Privacy Act* (1986)[233] which regulates the use of information communicated electronically. Violations of these provisions can result in imprisonment, substantial fines and/or civil liability for damages suffered or profits made as a result;

- The *Computer Matching and Privacy Protection Act* (1988)[234], the *Tax Reform Act of 1976*[235], and the *Right to Financial Privacy Act* of 1978[236] which prescribe limits on data matching and the use of information collected pursuant to statutory duties;

- The *Video Privacy Protection Act* (1988)[237] which controls the use of video rental or sale records;

- The *Telephone Consumer Protection Act* (1991)[238] which regulates unsolicited telephone calls; and

- The *Telecommunications Act* (1996)[239] which regulates the disclosure of transactional data in telecommunications services and is administered by the *Federal Communications Commission*;

State Laws

236. 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. The level of protection varies from one State to another.

Approach to Privacy Regulation in the Private Sector

237. The United States government has generally encouraged self-regulatory efforts for the protection of online privacy. Reports by government bodies and statements by officials include:

- "Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information" (June 1995)[240] by the *Information Infrastructure Task Force* (the "IITF")[241] 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)[242] 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)[243] 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;

- "A Framework for Global Electronic Commerce" (July 1997)[244] by the Clinton Administration which suggests that the government will play a more direct role if industry did not address privacy concerns through self-regulation and technology;

- "Elements of Effective Self-Regulation for Protection of Privacy" (January 1998)[245] by the NTIA and the Department of Commerce which outlines actions which the private sector can take in order to meet an acceptable level of privacy protection;

- "Report to Congress on Privacy Online" (June 1998)[246] by the FTC which emphasises the importance of notice, choice, security and access to privacy protection, suggests that substantial 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*, the Chairman of the FTC recently recommended that unless effective and broad-based self-regulation is in place by the end of 1998, legislation establishing statutory standards and creating an implementing agency should be enacted;[247] and

- A press release by Vice President Gore (July 31, 1998) which calls for an Electronic Bill of Rights as well as legislation to protect sensitive personal information and children's privacy online.[248]

Self-Regulatory Instruments

Instruments Relating to Online Privacy

238. A number of industry-based organisations have developed guidelines and codes of conduct for their members. These include:

- The *Information Technology Industry Council*[249] 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;[250]

- The *Interactive Services Association*[251] has published voluntary "Principles on Notice and Choice Procedures for Online Information Collection and Distribution by Online Operators" (June 1997)[252] which are based on a regime of notice and opt-out;

- The *Online Privacy Alliance*[253] (formed in June 1998 by 50 American Internet-related companies and associations) has produced Guidelines for Online Privacy (which urge Alliance members to have regard to the OECD Guidelines and use third party privacy seal

programmes such as *TRUSTe* and *BBBOnLine*[254]), and a set of guidelines for safeguarding children's privacy; and

- The *American Electronics Association* has announced (June 1998) self-regulation plans which include adopting a set of privacy protection elements for implementation by member companies.[255]

Other Initiatives

239. Other self regulatory initiatives include:

- The *Direct Marketing Association*[256] has established voluntary guidelines and developed *Online Guidelines* based on the principles of disclosure and opting-out;

- The *Children's Advertising Review Unit* of the *Council of Better Business Bureau* has published "Self-Regulatory Guidelines for Advertising to Children"[257] which require "reasonable efforts" be made to provide notice and choice to parents when information is collected from children online;

- The *Coalition for Advertising Supported Information and Entertainment*[258] has developed a statement of *Goals for Privacy for Marketing in Interactive Media*; and

- The *Individual Reference Services Group* (the "IRSG") agreed with the FTC in December 1997 to abide by a set of *IRSG Principles* which address the availability of information obtained through computerised database services that are used to locate, identify or verify the identity of individuals.

TABLE OF NATIONAL INSTRUMENTS

Country name	Ratification of Convention 108	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 European Union

II. MECHANISMS TO IMPLEMENT AND ENFORCE PRIVACY PRINCIPLES ON GLOBAL NETWORKS

240. 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 Website'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).

241. This part of the Inventory categorises the various mechanism 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

242. Users of global networks can act with relative anonymity by minimising the amount of personal data they disclose and/or allow to be collected[259]. 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

243. As discussed in the general introduction[260], header information and click-stream data are 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) Restricting the Creation of Cookies

244. 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 prevent the creation of cookies. Methods which may be used include the following:

- The most recent versions of the *Microsoft Explorer* and the *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 Website). Examples are the *Internet Junkbuster Proxy*[261], *Cookie Crusher*[262], *Cookie Master*[263] and *Cookie Pal*[264].

245. These techniques, however, 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.

(b) Blocking the Transfer and Collection of Automatically Generated Data

246. 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.

247. "Anonymous remailers" allow e-mail messages to be sent without revealing the identity of the sender. Some, such as *Hotmail*[265] and the *Freedom Remailer*, run by the *Global Internet Liberty Campaign*[266], operate through Web pages where an e-mail is created and sent without any information identifying the sender. Other remailers 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 are the remailers at *Replay*[267] and *Nymserver*[268]. Such remailers 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 remailer and making matches based on, for example, their length and timing information[269]. Many anonymous remailers have been forced to close down because of abuses, such as offensive messages and mass mailings.

248. An "anonymising intermediary" may be used to prevent a Website automatically collecting header information about the user[270], 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 Website able to set a cookie on the user's computer. An example of such a service is the *Anonymizer*[271].

249. 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[272].

2. Reducing or Avoiding the Need for Personal Data Disclosure

250. 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

251. 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.

252. A number of companies are developing cash-like payment mechanisms for use on global networks[273]. Two examples are *Ecash*[274], and *Mondex*[275]. Ecash provides cash-like anonymity through an encrypted payment system. Essentially, money from an account held with a participating bank can be converted into "digital coins" which can be transferred into an "electronic purse" on the user's computer. From there the coins can be transferred to other individuals or merchants doing business online. Each coin has a unique serial number and is validated by a "digital signature", which allow transactions to be verified and prevent the same coin from being spent more than once. To protect user anonymity, the user's computer (rather than the bank) may randomly assign a serial number to a coin which can be sent to the bank in a special digital envelope. The bank adds a "blind digital signature" to the envelope, debits the user's account and returns the coin without ever knowing the serial number. The user can then spend the coin, and payment will be honoured by the bank even though it cannot trace the identity of the payor.

253. *Mondex* is another electronic payment mechanism. Here funds are stored in a "smart card"[276] 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.

254. 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 facilitate money laundering, fraud and tax evasion.

(b) Digital Certificates

255. 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 [277].

256. 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.

257. 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

258. One of the reasons why Websites 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, as many online businesses have realised, 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*[278] 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" Website. Other companies which run similar systems include *DoubleClick*[279] and *Clickstream*[280].

259. 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[281] at a later date.

B. Informing Users about Online Privacy Policies

260. Although users of global networks often desire and benefit from anonymity, they may also choose to reveal 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 block the automatic transfer and collection of header information and click-stream data generated by normal Web-browsing.

261. Although the percentage of Websites which currently include statements about their privacy and personal data practices is small[282], various private bodies (such as, *TRUSTe*[283] and *BBBOnLine*[284]) and trade organisations (such as, the *Online Privacy Alliance*[285] and the *American Electronics Association*[286]) 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[287]. One important factor in determining whether or not users trust Websites 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[288].

262. The ways in which a Website 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

263. The simplest way for an organisation engaged in online activities to declare its privacy policy is via a specific page on their Website. The information contained in Website privacy policies can include[289]: who the organisation collecting the data is and how they may be contacted; who in the organisation is responsible for compliance with the privacy policy; what information is being collected and how; how the collected data will be used; what choices 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 Website.

264. To supplement the information provided in such a statement, hypertext links may be used 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 Website 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[290].

2. Terms and Conditions

265. A Website 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 Website 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[291]. 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

266. "Digital labelling" of privacy practices can provide an alternative or complementary means of notification. The basic idea is that a uniform "vocabulary" for Website 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.

267. The *Platform for Privacy Preferences* project ("P3P")[292] takes this approach. P3P is being developed by the World Wide Web Consortium (the "W3C") and is based on their *Platform for Internet Content Selection* ("PICS") framework for labelling Websites[293]. The goal of P3P is to allow Websites to simply express their privacy practices over the collection and use of personal data and to enable users to specify their own preferences[294]. The privacy vocabulary being developed currently includes a list of data categories and data practices relating to, for example, the purposes for which data is 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[295].

268. 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

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

1. Optional Data Fields and Click-Box Choices

270. One simple means of providing choice is for Websites to collect their data through online forms which distinguish between obligatory and optional data fields, and which display "click boxes" giving visitors options as to how the supplied information 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.

271. 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 Websites. *Firefly*[296] 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*[297] operate a similar system. A unique random number is assigned, using a cookie, to each user visiting one of its sites[298]. This number is used to track click-stream data relating to, for example, the kinds of advertisements viewed. Customers may also voluntarily provide personal information in return for special

offers and customised advertising. How much of this kind of personal information is disclosed, and how it is used, is therefore determined by the customer.

2. Online Negotiation of Privacy Standards through Digital Labels

272. Digital labelling and automated filtering, which were discussed above[299], may also be used to give a user new options when a Website'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

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

Preventing the Receipt of Unsolicited E-Mail Advertising

274. 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"[300]. 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[301]. The US *Direct Marketting Association* is developing such a programme and intend to make its use a condition of membership from July 1999[302]. 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

275. 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[303]and MatchLogic[304], click-stream data which are collected automatically are not treated as "personal data" over which the user is entitled to exercise control. However, there is no technical reason why users could not be given the ability to determine whether or not this information is collected and how it is used. 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[305].

D. Providing Access to Personal Data

276. 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 Website and the data subject.

E. Protecting Privacy through Transborder Data Flow Contracts

277. 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, and different social standards, with respect to privacy protection.

278. Many international standard-setting documents require special treatment for transborder data flows. For example, Part Three of the OECD Guidelines states 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 ("Convention 108")[306]. This issue is particularly topical because of Article 25(1) of the European Union Data Protection Directive, 1995 (the "EU Directive") which 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"[307]. 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 [308].

The Council of Europe Model Contract, 1992

279. The *Council of Europe Model Contract to Ensure Equivalent Data Protection in the Context of Transborder Data Flows*[309] (the "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 (the "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.

280. 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.

281. 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.

282. The remaining clauses deal with liability for the misuse of the data by the data receiver, rights of data subjects[310], dispute settlement and termination of the contract. The applicable law is left open as a matter for the parties to determine.

The Revised ICC Model Contract

283. The 1992 model contract clauses are currently being revised by the International Chamber of Commerce in light of the EU Directive's requirement of "adequate protection" in data exchanges to third countries[311]. The revision is to take into account comments of the European Commission's Working Party set up pursuant to Article 29 of the EU Directive[312]. As the draft stood in February 1998, the exporter would warrant compliance with its national laws and the importer would warrant compliance with the local law and agree to the provision of security measures, home country control, compliance with the exporter's rules, purpose restriction and constraints on third party disclosures.

An Illustrative Agreement: German Railways (Deutsche Bahn AG) and Citibank

284. In 1994, German Railways (Deutsche Bahn AG) arranged with the German subsidiary of Citibank for the production of RailwayCards (offering discounts for frequent travellers) which also function as VISA cards[313]. 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 Interterritorial Data Protection was entered into to give German citizens the same level of privacy protection as if the cards were 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

285. 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 Website complies with its posted privacy policies are emerging as a new private sector mechanism for enforcing privacy principles.

286. Irrespective of the regime in question, effective enforcement has two aspects. The first side to enforcement is comprised of those institutions and procedures 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 institutions and mechanisms which are available to enforce privacy guidelines[314].

1. Ensuring Compliance with Privacy Standards

287. 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 discussion distinguishes between four main means of ensuring compliance: requiring the 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

288. Privacy laws and self-regulatory codes may require the appointment of an internal data protection officer by data controllers[315]. Establishing the particular person within an organisation who is responsible for ensuring that the organisation complies with the applicable privacy standards reduces the risk that privacy issues will be given a low priority or will fall through a gap in the organisation's chains of responsibility. 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 Website Certification

289. Compliance reviews undertaken by third parties can help ensure that Websites follow their privacy statements. Ongoing 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[316] or a well-recognised icon[317], as a public confirmation that the they comply with their privacy statements.

290. There are different reasons why a Website may seek third party compliance reviews and certification. Sites may voluntarily submit to compliance reviews. For example, a Website 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 bad publicity which would accompany it, may provide a sufficient incentive for Websites to comply with their privacy statements. In addition, privacy laws, self-regulatory codes of conduct and/or industry organisations[318], may require an online business to seek third party certification.

291. The following are examples of businesses and professional organisations who offer certification schemes with respect to privacy practices.

TRUSTe

292. *TRUSTe* is an independent, non-profit making organisation that certifies Websites which meet the requirements of the TRUSTe programme[319]. In particular, a Website must: disclose its information management practices in an online privacy statement; adhere to these stated practices; and cooperate 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).

293. TRUSTe has also recently announced (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 transfer to third parties[320].

294. 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 Website continues to adhere to its published privacy statement the TRUSTe programme is backed by an on-going "assurance" process. In particular, TRUSTe monitors a Website'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

295. Standards authorities are another type of organisation which may act as third party certifiers by developing privacy standards and offering formal certification to compliant Websites. 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[321].

Accounting Firms

296. Privacy audits are one of the services now being carried out by large accounting firms[322]. 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[323]. 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 Website 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.

(c) Membership-Based Industry Bodies

297. Industry bodies which specify certain privacy standards as a pre-requisite for membership can play a role in ensuring that privacy standards are complied with on global networks. Examples include: the *Online Privacy Alliance* (formed in June 1998, it is a cross-industry coalition designed to address online privacy issues whose members have agreed to adopt, implement and disclose privacy policies)[324]; the Australian *Internet Industry Association* (which has proposed an Industry Code of Practice utilising a code compliance icon)[325]; 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 Websites)[326]. 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[327].

298. 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

299. 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. When empowered to perform proactive audits on their own initiative, such authorities can play an important role in ensuring compliance with privacy laws, codes of conduct and even contract-based privacy measures.

300. The "supervisory authorities" referred to in the EU Directive[328], for example, are intended to have the kinds of powers appropriate to 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)[329]. In the EU example, these powers are subject to a right of judicial appeal.

301. 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[330], 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

302. 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 may seek some form of redress or remedy. The privacy complaint resolution procedures which can be found in different OECD Member countries vary in many ways.

303. 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.

304. 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 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 prosecutorial 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

305. 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.

306. 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. Settlements between dissatisfied users and data controllers are, therefore, more likely in environments where users are able and willing to publicise unresolved complaints through, for example, the Internet[331], and where alternative remedies which are available to the data subject.

307. To facilitate the amicable resolution of privacy complaints, online businesses may take a number of proactive measures. The inclusion of a clearly defined complaints procedure in a Website's privacy statement, or in the terms and conditions of an online agreement, can assist the resolution of privacy complaints between the parties[332]. These provisions may address such issues as means of contacting the organisation, 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.

308. Legislation and self-regulatory codes which require data controllers to appoint internal data protection officers may also facilitate the resolution of complaints by providing a clear point of contact with well defined responsibilities[333].

(b) Enforcement through Private Sector Certification Schemes and Industry Bodies

309. Certification schemes and industry bodies may provide helpful avenues of redress for data subjects alleging privacy breaches by a member Website. 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.

310. 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.

311. One of the key factors affecting the likelihood of a successful resolution of a customer complaint is the kind of "sanctions" which third party certifiers and industry bodies have available to enforce compliance by errant member Websites. These may include:

- the publication of the business' name on a "bad actor" list;
- the revocation of the Website's compliance certification icon[334];
- removal from an industry body[335]; and/or
- administrative or judicial proceedings against the Website (for example, for breach of contract or misuse of trademarks).

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

TRUSTe

313. 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 Act*[336], or TRUSTe may conduct breach of contract or trademark infringement litigation against the site.

The Australian Industry Internet Association

314. In February 1998, the Australian *Internet Industry Association* released a draft *Industry Code of Practice*[337]. In the first instance, it is intended that complaints will be dealt with between the user and the Website 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 and orders by the Code's *Administrative Council* for 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

315. 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

316. 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.

317. 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.

318. 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.

319. 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.

320. 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

321. 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 standards may be complained to. For example, in the US the FTC, in its roles as an independent law enforcement authority, has broad powers to investigate and adjudicate complaints of businesses engaging in unfair and deceptive conduct[338]. The FTC has recently conducted an investigation against *GeoCities*[339] for misleading its customers as to how their personal information was being used which has resulted in the issuance of a consent order[340].

Civil Proceedings

Breaches of Privacy Legislation

322. Privacy legislation may provide data subjects with the right to a judicial remedy for the breach of the privacy principles established by the legislation[341]. Procedurally, such complaints are usually brought to court by the injured data subject.

323. 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 a 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

324. 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.

325. The breach of a privacy statement or an online agreement may give rise to a number of possible civil remedies. Essentially, by providing notification of its privacy practices a Website 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.

326. A contractual remedy may also be available to Website 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

Website 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[342]. 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 a contractual effect and be capable of giving 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.

327. The breach of a transborder data flow contract by the data controllers 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[343]. 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

328. 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. For example, 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[344].

Criminal Proceedings

Proceedings under Privacy Legislation

329. Privacy legislation may provide for criminal sanctions to be imposed in cases where there have been serious breaches of the legislation[345]. 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.

Other Criminal Proceedings

330. 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, by bodies such as the US FTC[346].

G. Educating Users and the Private Sector

331. 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.

332. 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 standards. 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 privacy standards will be effectively implemented in practice.

333. 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, the consequences of agreeing to particular privacy standards, how to use privacy enhancing technologies, and how to set appropriate browser settings for their desired level of privacy.

334. In addition to traditional methods of public education in schools, the workplace and the media,[347] various Websites offer online advice on personal privacy protection on global networks. Such sites are run by (1) international organisations, such as the Council of Europe[348]; (2) government bodies, such as the FTC in the U.S.[349] and many central oversight authorities in other parts of the World[350]; and (3) private sector organisations, such as *Project OPEN* (the Online Public Education Network)[351], the US *Direct Marketing Association*[352], the *Center For Democracy and Technology* (the "CDT")[353], the *Electronic Privacy Information Center* ("EPIC")[354] and TRUSTe[355]. Hyper-text links can be used to provide access to these sources of privacy information from Websites which collect personal information.

APPENDIX -- CONTACT DETAILS FOR PRIVACY ORGANISATIONS

A. International Organisations

Council of Europe

Data Protection Section
Public Law Division
Directorate of Legal Affairs
Secretariat General
PO Box 431 R6
67006 Strasbourg
FRANCE
Telephone No: (33) 88 41 2445
Fax No: (33) 88 41 2764
Web: http://www.coe.fr/dataprotection

European Commission

European Commission Legal Advisory Board
Web: http://www2.echo.lu/legal/en/dataprot/dataprot.html

Organisation for Economic Co-operation and Development

Information, Computer and Communications Policy Committee
2 rue André-Pascal
75775 Paris Cedex 16
FRANCE
Telephone: (33) 1 45 24 82 00
Fax: (33) 1 45 24 93 32
Web: http://www.oecd.org/dsti/sti/it/index.htm

United Nations

United Nations High Commissioner for Human Rights
Web: http://www.unhchr.ch/hchr_un.htm

World Trade Organisation

World Trade Organisation
Web: http://www.wto.org/wto/services/services.htm

B. Data Protection Authorities

Australia

Australian Privacy Commissioner's Office
GPO Box 5218
Sydney NSW 1042
AUSTRALIA
Telephone +1300 363 992
Fax: (02) 9284 9666
E-mail privacy@privacy.gov.au

Austria

Bundeskanzleramet
Ballhausplatz 1
Vienna
1014
AUSTRIA
Telephone: (43) 1 531 15 2528
Fax: (43) 1 531 15 2690

Belgium

Commission Consultative de la Protection de la Vie Privee
Boulevard de Waterloo 115
Rue de la Regence 61
Bruxelles 1000
BELGIUM
Telephone: (32) 2 542 7200
Fax: (32) 2 542 7212
E-mail: privacy@euronet.be
Web: http://www.privacy.fgov.be/

Canada

The Privacy Commissioner of Canada
112 Kent Street, 3rd floor
Ottawa, Ontario
K1A 1H3
Telephone: 001 613 995-2410
Fax: 001 613 995-1501
Web: http://infoweb.magi.com/~privcan/

The Office of the Information and Privacy Commissioner/Ontario:
Information and Privacy Commissioner/Ontario
80 Bloor Street West
Suite 1700
Toronto, Ontario
M5S 2V1
CANADA
Telephone: (416) 326-3333
Fax: (416) 325-9195
Web: http://ipc.on.ca/

Information & Privacy Commissioner of British Columbia
1675 Douglas Street, 4th Floor
Victoria, British Columbia
V8V 1X4
CANADA
Telephone: (250) 387-5629
Fax: (250) 387-1696
E-mail: oipc@gems5.gov.bc.ca
Web: http://www.oipcbc.org/

Information & Privacy Commissioner of Alberta
410, 9925-109 Street
Edmonton, Alberta
T5K 2J8
CANADA
Telephone: (403) 422-6860
Fax: (403) 422-5682
E-mail: ipcab@planet.eon.net

Ombudsman of Manitoba
500 Portage Avenue, Suite 750
Winnipeg, Manitoba
R3C 3X1
CANADA
Telephone: (204) 786-6483
Fax: (204) 942-7803

Ombudsman of New Brunswick
703 Brunswick Street
P.O. Box 6000
Fredericton, New Brunswick
E3B 5H1
CANADA
Telephone: (506)453-2789
Fax: (506) 457-7896

Department of Justice of Newfoundland
Confederation Building
P.O. Box 8700
St. John's, Newfoundland
A1B 4J6
CANADA
Telephone: (709) 729-5942
Fax: (709) 576-2129

Information and Privacy Commissioner of the Northwest Territories
P.O. Box 262
Yellowknife, Northwest Territories
X1A 2N2
CANADA
Telephone : (403) 873-8631
Fax: (403) 920-2511

Review Officer of Nova Scotia
3-1601 Lower Water Street
P.O. Box 1692, Postal Unit M
Halifax, Nova Scotia
B3J 3S3
CANADA
Telephone: (902) 424-4448
Fax: (902) 424-3919

Commission d'accès à l'information- Quebec
900 René-Lévesque Boulevard East, Suite 315
Quebec City, Quebec
G1R 2B5
CANADA
Telephone (418) 528-7741
Fax: (418) 529-3102
E-mail : Cai.Communications@cai.gouv.qc.ca
Web: http://www.cai.gouv.qc.ca.

Information & Privacy Commissioner of Saskatchewan
2220-12 Avenue, Suite 500
P.O. Box 1037
Regina, Saskatchewan
S4P 3B2
CANADA
Telephone: (306) 787-8350
Fax: (306) 757-4858

Ombudsman and Information & Privacy Commissioner of the Yukon
P.O. Box 2703
Whitehorse, Yukon Territory
Y1A 2C6
CANADA
Telephone: (403) 667-8468
Fax: (403) 667-8469

Denmark

Registertilsynet
Christians Brygge 28, 4 Fl
DK-1559
Copenhagen V
DENMARK
Telephone: (45) 33 14 38 44
Fax: (45) 33 13 38 43
Web: http://www.registertilsynet.dk.

Finland

Finnish Data Protection Ombudsman
Albertinkatu 25, 3.krs
PO Box 315
SF-00181 Helsinki
FINLAND
Telephone: (358) 0 182 57830
Fax: (358) 0 182 67835
Web: http://www.tietosuoja.fi

France

Commission Nationale de l'Informatique et des Libertes
21 Rue Saint-Guillaume
75007 Paris
FRANCE
Telephone: (33) 1 4544 4065
Fax: (33) 1 4549 0455
E-mail: CNIL@world-net.sct.fr
Web: http://www.cnil.fr

Germany

Der Bundesbeauftragte fur den Datenschutz
Riemenschneider Str. 11,
53175 BONN
GERMANY
Telephone: (49) 228 819 95 10
Fax: (49)228 819 95 50
E-Mail: poststelle@bfd.bund400.de

For the addresses of the Laender data protection authorities, see:
http://www.datenschutz-berlin.de/sonstige/behoerde/aufsicht.htm

Greece

Greek Data Protection Authority
12, Vlaoritou Street
EL-10671 ATHENS
Telephone: (30) 1 361 31 17
Fax: (30) 1 362 90 47

Hungary

Parliamentary Commissioner for Data Protection and Freedom of Information
1054 Budapest
Tüköry u. 3.
HUNGARY
Telephone: (36) 1 269 3537
Fax: (36) 1 269 3529

Iceland

Icelandic Data Protection Commission
Arnarhvoll
150 Reykjavik
ICELAND
Telephone: (354) 1 609010
Fax: (354) 1 27340

Ireland

Irish Data Protection Commissioner
Mr. Fergus Glavey
Block 4, Irish Life Centre
Talbot Street
Dublin 1
IRELAND
Telephone: + 353 1 874 8544
Fax: + 353 1 874 5405
E-Mail: fergus_glavey@dataprivacy.irlgov.ie

Italy

Italian Guarantor of the Protection of Personal Data: Garante per la protezione dei dati personali
Via della Chiesa nuova 8
00186 Rome
ITALY
Telephone: 00 396 68892134/5/6/7/8/9
Fax: 00 396 68892140
E-Mail: mc7796@mclink.it

Luxembourg

Commission consultative à la protection des données
Ministère de la Justice
16 boulevard Royal
2934 LUXEMBOURG
Telephone: (352) 478 4546
Fax: (352) 227 661

The Netherlands

Registratiekamer
Prins Clauslaan 20
P O Box 93374
2509 AJ Den Haag
NETHERLANDS
Telephone: (31) 70 3811300
Fax: (31) 70 3811301
E-Mail: mail@registratiekamer.nl

New Zealand

Office of the Privacy Commissioner of New Zealand
PO Box 466
Auckland
NEW ZEALAND
Telephone: (64) 9 302 2160
Fax: (64) 9 302 2305
Web: http://www.knowledge-basket.co.nz/privacy/welcome.htm

Norway

Norwegian Data Inspectorate: Datatilsynet
Postboks 8177 Dep
0034 OSLO
NORWAY
Telephone: +47 22 42 19 10
Fax: +47 22 42 23 50
E-Mail: postkasse@datatilsynet.no
http://www.datatilsynet.no

Poland

Generalny Inspektor Danych Osobowych
Sejm RP ul. Wiejska 4/6/8
PL 00-950 Warszawa
POLAND

Portugal

Comissao Nacional de Porteccao de Dados Pessoais Informatizados
Rua de Sao Bento 148
1200 Lisboa
PORTUGAL
Telephone: (351) 1 396 6190
Fax: (351) 1 397 6832
E-Mail: cndpi@mail.telepac.pt

Spain

Spanish data protection agency: Agencia de Protection de Datos
Paseo de la Castellana 41, 5
E-28046 Madrid
SPAIN
Telephone: (34) 1 308 4017
Fax: (34) 1 308 4692
Web: http://www.ag-proteccionadatos.es

Sweden

Datainspektionen
Box 8114
S-104 20 Stockholm
SWEDEN
Telephone: (46) 8 657 6100
Fax: (46) 8 652 8652
Email: datainspektionen@din.se
Web: http://www.din.se

Switzerland

Eidgenössischer Datenschutzbeauftragter
Webergutstrasse 5
3052 Zollikofen
CH - 3003 Berne
SWITZERLAND
Telephone: +41 31 322 4395
Fax: +41 31 3259996
Web: http://www.edsb.ch

United Kingdom

The UK Data Protection Registrar
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
ENGLAND
Telephone: +44 1625 545700
Fax +44 1625 24510
E-Mail: data@wycliffe.demon.co.uk
Web: http://www.open.gov.uk/dpr/dprhome.htm

C. Non-Governmental Organisations

Asia-Pacific Smart Card Forum

G.P.O. Box 1966
Canberra ACT 2601
AUSTRALIA

Center For Democracy and Technology

Web: http://www.cdt.org/

Electronic Privacy Information Center

Web: http://www.epic.org/

Privacy International

Web: http://www.privacy.org/

PrivacyExchange.Org

Web: http://www.PrivacyExchange.org/

NOTES

1. See Jerry Kang, "Information Privacy in Cyberspace Transactions", 50 STAN. L. REV. 1193-1294, at 1224-1230 (1998).

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 http://www.four11.com/).

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 http://www.cookiecentral.com/

5. Cookies are useful because they allow a user and a Website 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. Document available at http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-en.HTM

8. From the text of the *Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.*

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

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

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

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

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

14. Recent and ongoing 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 (expected October 1998); and a "Ministerial Declaration on the Protection of Privacy on Global Networks" (being prepared for the Ministerial Conference, *A Borderless World: Realising the Potential of Global Electronic Commerce* (Ottawa, 7-9 October 1998)). See http://www.oecd.org/dsti/sti/it/index.htm

15. Document available at http://www.coe.fr/eng/legaltxt/108e.htm

16. See http://www.coe.fr/index.asp

17. Figures as at December 1997. The Table of National Instruments (see page 50) shows those OECD Member countries which have ratified Convention 108.

18. 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

19. Article 6, Convention 108.

20. Article 12, Convention 108.

21. Article 13.2, Convention 108.

22. Article 4, Convention 108.

23. Alternative title: "Draft Guidelines for the protection of individuals with regard to the collection and processing of personal data on the information highways, which may be incorporated in or annexed to Codes of conduct". Document available at http://www.coe.fr/dataprotection

24. Document available at http://www.unhchr.ch/html/menu3/b/71.htm

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

26. 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 1997. Document available at http://www.unhchr.ch/html/menu4/chrrep/6797.htm

27. OJ no.L281 of 23/11/1995, 31. Available at http://www.2echo.lu/legal/en/dataprot/directiv/direct.html

28. 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)

29. Articles 3 and 4, EU Directive.

30. 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.

31. Articles 10 and 11, EU Directive.

32. Article 14, EU Directive.

33. Articles 18-21, EU Directive.

34. Articles 22-24, EU Directive.

35. Article 1(2), EU Directive.

36. Article 25(1), EU Directive.

37. Article 26, EU Directive.

38. Article 12, EU Directive.

39. Article 28, EU Directive.

40. Discussion Document DG XV WP 4, adopted by the Working Party on 26 June 1997.

41. See "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 14 January 1998.

42. Document available at http://www.wto.org/wto/services/gatsintr.htm

43. See http://www.wto.org/

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

45. Proceedings available at http://www.privacy.fgov.be/conference/index.html

46. Document available at http://www.datenschutz-berlin.de/diskus/13_15.htm The paper was referred to by the European Union Article 29 Working Party in a recommendation in December 1997.

47. ISO was established in 1947. See http://www.iso.ch/

48. See paragraph 91.

49. 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.

50. See http://www.iccwbo.org/

51. Document available at http://www.iccwbo.org/Commissions/Marketing/marketcod.htm

52. See paragraph 283.

53. See http://www.ec-europe.org/

54. See http://www.epic.org/

55. See http://www.cdt.org/

56. See http://www.privacy.org/

57. See http://www.PrivacyExchange.org/

58. A copy of the Privacy Act and other Australian privacy legislation is at http://www.austlii.edu.au/~graham/PLPR_australian_guide.html/#legislation.

59. See http://www.privacy.gov.au/

60. The Privacy Act allows the Privacy Commissioner to issue *Tax File Number Guidelines* which apply to all public and private sector collectors of Tax File Numbers. It also regulates the information handling practices of the consumer credit reporting industry. Proposals have been put forward to amend the Privacy Act to extend the coverage of the IPPs to private sector contractors holding personal information under contracts with Commonwealth agencies. See http://www.privacy.gov.au/private/index.html

61. Document available at http://www.privacy.gov.au/news/p6_4_1.html

62. "Internet Commerce - To Buy or not to Buy?", June 1998. Document available at http://www.aph.gov.au/house/committee/jpaa/elecom/report/contents.htm

63. Recommendation 17. Chapter 7, Paragraph 75.

64. For a discussion of this and other legislation, see http://www.privacy.gov.au/act/index.html

65. *Health Records (Privacy and Access) Act 1997 (ACT)*. The Commonwealth Privacy Act also applies to government agencies in the Australian Capital Territory.

66. A copy of the Act is available at http://www.austlii.edu.au/au/legis/nsw/conso_act/ pca1975202.

67. See http://www.privacy.gov.au/links/p8_1.html

68. The Victorian Government's discussion paper regarding the Bill is available at http://www.mmv.vic.gov.au/DIR0123/mmv_www.nsf/f425c9fab93058ed4a2565570043d653/75500028edecb6084a2566330022a8c0/$FILE/priv.pdf

69. The draft Code is available at http://www.iia.net.au/news/980201.html

70. Clauses 8 and 9 of the draft Code.

71. "Consumer Protection in Electronic Commerce – Draft Principles and Key Issues", October 1997. Document available online at http://www.dist.gov.au/consumer/eleccomm/draft/index.html

72. Copies of the Code are available from the Asia-Pacific Smart Card Forum, G.P.O. Box 1966, Canberra ACT 2601, AUSTRALIA.

73. See http://www.acif.org.au

74. Press release available at http://203.27.21.60/media-releases/media-releases.htm#TOC16

75. Document available at ftp://ftp.standards.com.au/acif/G505.pdf

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

77. Federal Law Gazette I Nr.100/1997. Unofficial translation available at http://www.bmv.gv.at/

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

79. Information (in German) on the Datenschutzgesetz and other privacy-related initiatives in Austria is given at the site of the ARGE DATEN - Austrian Society for Privacy and Data Protection: http//www.ad.or.at

80. See http://www.privacy.fgov.be/

81. Articles 37-43

82. Document available at http://www.lachambre.be

83. Document available at http://www.ispa.be/fr/c040201.html

84. Document available at http://canada.justice.gc.ca/stable/EN/Laws/Chap/P/P-21.html

85. See http://infoweb.magi.com/~privcan/

86. In 1995 the *Canadian Information Highway Advisory Council* recommended legislation for both public and private sectors in Canada (see http://strategis.ic.gc.ca/SSG/ih01015e.html) and the *Uniform Law Conference of Canada* has been working on a draft *Uniform Protection of Personal Information Act* since 1995 (see http://www.law.ualberta.ca/alri/ulc/current/edata.htm).

87. Document available (in English and French) at http://strategis.ic.gc.ca/privacy Public responses to the proposals are available online at http://strategis.ic.gc.ca/SSG/pv01171e.html

88. 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 Brunswkick 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

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

90. Document available (in french) at http://www.cai.gouv.qc.ca/loi.htm

91. The Committee was comprised of representatives of industry and the Canadian Government.

92. CAN/CSA-Q830-96. The CSA Standard can be viewed/ordered at http://www.csa.ca/home/index.html

93. Publication PLUS 8300 (December 1996). This document can be ordered from the CSA Website: http://www.csa.ca/home/index.html

94. Document available at http://www.cba.ca/eng/Publications/pubs_privacy.htm

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

96. Act No.256/1992.

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

98. The Act has since been amended to provide for the reporting of public debts to private credit reference agencies (Consolidation Act No. 654 of 20 September 1991).

99. See http://www.registertilsynet.dk

100. Article 15, Public Authorities Registers Act.

101. Article 29, Public Authorities Registers Act.

102. Consolidation Act No. 622 of 2 October 1987, as amended by Act No. 386 of 20 May 1992, Act No.30 of 1 June 1994 and Act No. 1093 of 21 December 1994.

103. Article 25, Private Registers Act.

104. Article 27(1), Private Registers Act.

105. Document available (in Danish) at http://www.folketinget.dk/19972/lovforslag_som_fremsat/L82.htm

106. Act no. 471/ 1987

107. The Ombudsman's Office is at http://www.tietosuoja.fi. For address see Schedule of Resources.

108. Section 35, Personal Data File Act.

109. Section 38, Personal Data File Act.

110. Sections 42-46, Personal Data File Act.

111. Act Nos 62/1994 and 1073/1992 respectively.

112. Articles 226-16 to 226-24.

113. See http://www.cnil.fr

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

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

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

117. Ordonnance No. 96-345 of 24 April 1996.

118. See the French Prime Minister's press release at http://www.premier-ministre.gouv.fr/PM/030398.HTM

119. Document available at http://www.planete.net/code-internet/ccode2.html

120. Internet actors who commit themselves to the charter (mainly concerns users and ISPs) and based on French territory

121. Syndicat des Entreprises de Vente par Correspondance et à Distance, Website at http://www.sevpcd.com

122. Code de Déontologie sur la protection des données à caractère personnel, available online at http://www.sevpcd.com/generale/re/docs/code_md.doc

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

124. Section 21(1)

125. Sections 43 and 44

126. Federal regulations (in German) available at http://www.datenschutz-berlin.de/gesetze/bund.htm

127. Document available (in German) at http://www.datenschutz-berlin.de/gesetze/medien/tdsve.htm#nr1

128. Otherwise known at the IuKDG (01.8.1997), an outline of which is available at http://www.iukdg.de

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

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

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

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

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

134. Articles 11-14

135. Article 23.

136. Article 21.

137. Article 22.

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

139. See http://www.mkogy.hu/adatved_biztos/

140. Articles 11-15.

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

142. Articles 17 and 18.

143. Article 33.

144. Article 14(1).

145. Article 22.

146. Article 33.

147. Articles 37-39.

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

149. Sections 21-23.

150. Document available at http://www.irlgov.ie/justice/Publications/Law/consult.PDF

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

152. Law No. 675/95 regarding the protection of individuals and legal persons regarding the processing of personal data as amended by Legislative Decrees no.123 of 9 September 1997 and no.255 of 28 July 1997.

153. Duties of the Guarantor are set out in Article 31 of the Law.

154. Article 18.

155. Penalties contained in Articles 34-39.

156. See the legislation (in Italian) at http://www.privacy.it/normativ.html

157. G.U. n. 42 del 20/2/93.

158. The *Autorità per l'informatica nella Pubblica Amministrazione.* See http://www.aipa.it/english/index.asp

159. See http://www.aiip.it

160. Document available at http://www.somucho.go.jp/gyoukan/kanri/b_11e.htm

161. "The Asian Status with respect to the Observance of the OECD Guidelines and the EU Directive" by Stephen Lau, Privacy Commissioner for Personal Data, Hong Kong. Speech presented to the 19th International Conference Privacy Data Protection Commissioners, see the Conference website at http://www.privacy.fgov.be/conference/authors.html

162. See http://www.sumucho.go.jp

163. Articles 21 and 22.

164. Summary available at http://www.mpt.go.jp/policyreports/english/group/communications/info_com.html

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

166. The Guidelines were originally issued in April 1989. The March 1997 version is available in English at http://www.miti.go.jp/

167. Articles 22 and 23 of the Guidelines.

168. See http://www.jipdec.or.jp/kyotu_page/outline.htm

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

170. Document available at http://www.fmmc.or.jp/associations/cba/index.html

171. See http://www.ecom.or.jp/

172. Document available at http://www.ecom.or.jp/eng/output/wg12/wg12guidline.htm

173. Document available at http://www.telesa.or.jp/e_guide/e_guid01.html

174. 31 March, 1979.

175. 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.

176. Articles 32-39.

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

178. Bill No.4357.

179. Article 214, Federal District Penal Code.

180. See http://cwis.kub.nl/~dbi/regkamer/overzich.htm

181. Section 34.

182. Sections 50-54.

183. Bill no. 25 892 - Personal Data Protection Act - *Wet bescherming persoonsgegevens*

184. See "Self-Regulation: Some Dutch Experiences, Privacy and Self-Regulation in the Information Age", US Department of Commerce, June 1997. See http://www.ntia.doc.gov/reports/privacy/selfreg3.htm

185. Sections 97-109, Privacy Act.

186. See http://www.knowledge-basket.co.nz/privacy/welcome.htm. The functions of the Commissioner are set out in Section 13, Privacy Act.

187. Sections 46-53, Privacy Act.

188. Section 85, Privacy Act.

189. Document available at http://www.isocnz.org.nz/code.htm

190. Document available at http://www.knowledge-basket.co.nz/privacy/health/hipcnc.htm

191. Document available at http://www.knowledge-basket.co.nz/privacy/justice.htm

192. Act no.48 of 9 June 1978 relating to Personal Data Registers, etc.

193. See http://www.datatilsynet.no/

194. Articles 38-40 of the Norwegian Act contain penalties and compensation provisions in respect of violations of the Act.

195. 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.

196. 29 August 1997, Dz.U. nr 133, poz. 833. The Act came into force on 30 April 1998. For information on the law and the data protection authority see http://www.kul.lublin.pl/~fajgiel/Odo/En/en_index.html

197. Articles 50-54.

198. 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.

199. Article 8(h).

200. Articles 27, 29 and 30.

201. Articles 34-41.

202. Law 109/91 of 17 August 1991.

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

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

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

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

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

208. 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. For information on implementation of the Law in the public sector see http://www.map.es/csi/pg5v10.htm

209. See http://www.ag-proteccionadatos.es

210. Articles 43 and 44 of the Law.

211. Law No. 28/94.

212. Code available (in Spanish) at http://www.aece.org/protec.htm

213. The new Act will be available at http://www.regeringen.se/info_rosenbad/

214. Data Inspection Board website at http://www.din.se.

215. 19 June, 1992.

216. See http://www.edsb.ch/

217. Article 11 of the FLDP.

218. Article 23 of the FLDP.

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

220. Document available at http://www.planete.net/code-internet/suisse.html

221. Ass supplemented by Orders in 1987, 1990 and 1997. The Data Protection Act is available at http://www.hmso.gov.uk/acts/acts1984/1984035.htm

222. See http://www.open.gov.uk/dpr/dprhome.htm

223. Amendment introduced by the Criminal Justice and Public Order Act 1994.

224. Document available at http://www.parliament.the-stationery-office.co.uk/pa/pabills.htm See also the Data Protection Registrar's comments on the Bill, at http://www.open.gov.uk/dpr/eurotalk.htm

225. See http://www.open.gov.uk/dpr/bsi.htm

226. See http://www.ispa.org.uk/

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

228. 5 U.S.C. § 552a (1994).

229. Other miscellaneous federal laws with provisions on privacy include: *Family Educational Rights and Privacy Act* (1974); *Automated Telephone Consumer Protection Act* (1991); *Drivers Privacy Protection (Boxer-Moran) Act* (1994); *Child Abuse Prevention and Treatment Act* (1994); *Fair Debt Collection Practices Act*; and *Health Insurance Portability and Accountability Act* (1996).

230. 15 U.S.C. § 1681-1681(u), as amended is available on the FTC website at http://www.ftc.gov/os/statutes/fcra.htm

231. See http://www.ftc.gov/ The FTC also has a general jurisdiction regarding "unfair or deceptive acts or practices in or affecting commerce" under section 5(a) of the *Federal Trade Act*. This may include unfair or deceptive information practices. See footnote 338.

232. 47 U.S.C. § 551.

233. 18 U.S.C. § 2510.

234. Pub. L. No. 100-503, 102 Stat. 2507, 5 U.S.C. §§ 552a(a)(8)-(13), (e)(12), (o)-(r), (u)

235. 26 U.S.C. § 6103 (1989) & Supp. 1996

236. Pub. L. No. 95-630, 12 U.S.C.A. §§ 3401-22, 92 Stat. 3697, as amended Pub. L. No. 101-647, 101 Stat. 4908, 12 U.S.C.A. §§ 3401-22 (1989 & Supp.1997).

237. 18 U.S.C. § 2710.

238. 47 U.S.C. § 227.

239. Pub. L. No. 104-104, 110 Stat. 56 (1996).

240. Document available at http://www.iitf.nist.gov/ipc-pubs/niiprivprin_final.html

241. See http://www.iitf.nist.gov/

242. Document available at http://www.ntia.doc.gov/ntiahome/privwhitepaper.html#B11

243. Document available at http://www.iitf.nist.gov/ipc/privacy.htm

244. Document available at http://www.whitehouse.gov/WH/New/Commerce/summary-plain.htm

245. Document available at http://www.ntia.doc.gov/reports.html

246. Document available at http://www.ftc.gov/reports/privacy3/index.htm

247. Congressional testimony of Robert Pitofsky, Chairman of the FTC, 21 July, 1998. Document available at http://www.ftc.gov/os/9807/privac98.htm

248. Document available at http://www.cdt.org/privacy/gore_press.980811.html

249. See http://www.itic.org/

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

251. See http://www.isa.net/

252. Document available at http://www.isa.net/policy/privacy_guidelines_online.html

253. See http://www.privacyalliance.org/ Members include Microsoft, AOL, IBM, DMA, Time Warner, American Express, Procter and Gamble.

254. See paragraph 297.

255. See the press release at http://web1.aeanet.org/homepage/pressrel/22be.htm

256. See http://www.the-dma.org/

257. Document available at http://www.bbb.org/advertising/caruguid.html

258. See http://www.commercepark.com/AAAA/casie/

259. 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.

260. See paragraphs 9.-13.

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

262. See http://www.thelimitsoft.com/cookie.html

263. See http://www.barefootinc.com/cmaster.htm

264. See http://www.kburra.com/cpal.html

265. See http://www.hotmail.com/

266. See http://www.gilc.org/speech/anonymous/remailer.html

267. See http://www.replay.com/remailer/replay.html

268. See http://www.nymserver.com/

269. See "Privacy-Enhancing Technologies for the Internet", Ian Goldberg, David Wagner & Eric Brewer, document available at http://www.cs.berkeley.edu/~daw/privacy-compcon97-www/privacy-html.html

270. 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.

271. See http://www.anonymizer.com/

272. 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 (1) 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 (2) a court order is issued requiring the release of the information.

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

274. See http://www.digicash.com/index.html

275. See http://www.mondex.com/

276 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.

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

278. See http://www.engagetech.com/

279. See http://www.doubleclick.com/

280. See http://www.click-stream.com/webfaw.html

281. While such information is arguably not by itself personal data as it does not "[relate] to an identified or idenitifiable 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.

282. For example, a recent survey of 1200 US commercial Website by the FTC (March 1998) found that only 14 percent provided any notice of their information collection practices (see http://www.ftc.gov/reports/privacy3/survey.htm). Similarly, a survey of the top 100 Websites conducted in June 1997 by the Electronic Privacy Information Center ("EPIC") found that only 17 percent of these sites had explicit privacy policies (see http://www.epic.org/reports/surfer-beware.html).

283. See http://www.truste.org/

284. See paragraph 297.

285. See http://www.privacyalliance.org/

286. See http://web1.aeanet.org/homepage/pressrel/22be.html

287. The TRUSTe programme is discussed in more detail in the enforcement section at paragraphs 292.-294. and 313.

288. See paragraph **Error! Reference source not found.**-330.

289. Examples of posted privacy policies can be found throughout the Web. See, for example, the privacy statements at Lego (http://www.lego.com/professionals/privacypolicy.asp); Conintental Airlines (http://www.flycontinental.com/privacy.html); Australian Legal Information Institute (http://www.austlii.edu.au/austlii/privacy.html); ZDNet (http://www.zdnet.com/findit/privacy.html); DoubleClick (http://www.doubleclick.com/company_info/about_doubleclick/privacy/); Reader's Digest (http://www.readersdigest1.com/privacy/privacy.html); and Icon CMT (http://www.icon.com/use.html); Microsoft (http://register.microsoft.com/regwiz/include/security.htm).

290. See paragraphs 289.-296.

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

292. See http://www.w3.org/P3P/

293. 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 Website 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).

294. 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.

295. For the latest draft of the P3P protocol (July 1998) see http://www.w3.org/TR/WD-P3P10-syntax/

296. See http://www.firefly.com/

297. See http://www.preferences.com/

298. The Websites managed by MatchLogic are www.grandgobosh.com, www.Harrispoll.com, www.excite.com, www.webcrawler.com and www.quicken.com.

299. See paragraphs 266.-268.

300. 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.

301. The e-MPS technique for "opting-out" of e-mail marketing lists can be applied more generally. For example, an opt-out World Wide Website has been announced in the US. The site (http://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. See news item at http://www.usatoday.com/life/cyber/tech/ctc714.htm

302. See the "Testimony of the DMA before the Subcommittee on Communications, Committee on Commerce, Science and Transportation of The United States Senate" (June 17, 1998), available at http://www.the-dma.org/ The DMA currently operates similar mail and telephone preference schemes. For an example of an operational e-MPS scheme, see http://www.dm1.com/Epreference/epref.html

303. See paragraph 258.

304. See paragraph 271.

305. See http://www.doubleclick.com/company_info/about_doubleclick/privacy/

306. See http://www.coe.fr/eng/legaltxt/108e.htm

307. This provision is due to be implemented in Member countries by October 1998.

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

309. See http://www.coe.fr/dataprotection/ectype.htm for a copy of the Report, Model Contract and Explanatory Memorandum.

310. 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).

311 See the ICC Website at http://www.iccwbo.org

312. 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. See http://www.open.gov.uk/dpr/500598pa.htm

313 For a full discussion, see the remarks of Dr. Alexander Dix, Data Protection Deputy Commissioner Berlin, Germany at the 18th International Privacy and Data Protection Conference, Ottawa, Canada (September 18-20,1996). Available at http://www.datenschutz-berlin.de/sonstige/konferen/ottawa/alex3.htm.

314. 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.

315. 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 158.).

316. Such a label could be used within the P3P labelling system. See paragraphs 266.-268.

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

318. 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 Website, 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 http://www.privacyalliance.org/resources/enforcement.shtml

319. See http://www.truste.org/

320. See http://www.truste.org/users/pr/childseal.html

321. See paragraph 91.

322. Over the last ten 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).

323. See http://www.aicpa.org/webtrust/index.htm

324. See http://www.privacyalliance.org/

325. See paragraph 70..

326. 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 Center (http://www2.epic.org/reports/surfer-beware2.html).

327. See http://www.bbbonline.org/

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

329. Article 28(3) of the EU Directive.

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

331. Historically the World Wide Web community has been actively involved in policing the behaviour of its participants. By publicising breaches of privacy rights through the network, individuals and groups of consumers may be able to generate sufficient adverse publicity to force firms to change their data management practices. This is an important informal mechanism for enforcing privacy rights.

332. Such procedures may, of course, be relevant to other kinds of complaints as well.

333. See paragraph 288.

334. As proposed by, for example, TRUSTe and the Australian *Internet Industry Association* (see paragraph 70.).

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

336. See paragraph 321.

337. See paragraph 70..

338. 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 http://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).

339. See http://www.geocities.com/

340. See the FTC's news release at http://www.ftc.gov/opa/9808/geocitie.htm

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

342. See, for example, the Canadian-based *Sympatico* Website (http://www1.sympatico.ca/).

343. See paragraph 284.

344. See paragraphs 279.-282.

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

346. See paragraph 321.

347. See, for example, *Easy i* who publishes corporate educational videos and computer software relating to privacy protection (http://www.easyi.co.uk/published.asp).

348. See http://www.coe.fr/dataprotection/elignes.htm

349. See http://www.ftc.gov/privacy/index.html

350. See, for example, official Websites in Australia (http://www.privacy.gov.au/); France (http://www.cnil.fr/), Spain (http://www.ag-protecciondatos.es/); and the UK (http://www.open.gov.uk/dpr/dprhome.htm).

351. See http://www.isa.net/project-open/priv-broch.html

352. See http://www.the-dma.org/

353. See http://www.cdt.org/privacy/topten/online.html

354. See http://www.epic.org/privacy/

355. See http://www.truste.org/users/privacyonline.html