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

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

OLIS : 06-Oct-1998
Dist. : 07-Oct-1998

Or. Eng.

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

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

Group of Experts on Information Security and Privacy

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

Corrigendum

Ottawa, Canada, 7-9 October 1998

This Corrigendum includes input received from the Council of Europe, the European Commission, Austria, Australia, Canada, Sweden, United Kingdom and the United States.

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

70072

Or. Eng.

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

PREFACE

3. ~~1.~~ 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 different approaches to privacy protection developed by~~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.

7. ~~2.~~ 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, or at least effective, privacy protection.

INTRODUCTION

12. ~~3.~~ Personal data is also often disclosed voluntarily. Many commercial sites ask users to complete and submit Web page forms in order to register, subscribe, join a discussion group, enter a contest, make suggestions or complete a transaction. The kind of data which are typically requested may include such information as 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".

14. ~~4.~~ Thus, at the same time that ~~although~~ the development of global networks and digital technology has brought many social and economic benefits, it has also increased challenges to privacy~~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.

I. GUIDANCE INSTRUMENTS

20. ~~5.~~ Most ~~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.

A. International Instruments and Organisations

1. Intergovernmental Legal Instruments

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

Status

6. *Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data* of 18 September 1980[1] ("Convention 108") was opened ~~to all States~~ for signature by the *Committee of Ministers* of the *Council of Europe*[2] on 28 January 1981. ~~-~~Since then, it has been signed by 23 Countries and ratified by 21[3]. Convention 108 which is opened to the accession of any State, and not only to the members of the Council of Europe, ~~-~~is a binding instrument in international law.

Basic Principles

32. ~~7.~~ The Convention's basic principles are similar to those in the OECD Guidelines, but include a principle requiring appropriate safeguards for special categories of data ("sensitive data") that reveal racial origin, political opinions or religious or other beliefs, that concern health or sexual life, or that relate to criminal convictions~~such as personal data revealing personal beliefs, concerning health or relating to criminal convictions~~[4].

Provisions on Data Flows

33. The principles of the Convention provide for ~~encourage~~ the free flow of personal data between parties to the Convention who provide equivalent protection[5].

(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")[6] is a binding instrument that must be implemented by the 15 EU Member States not later than ~~in~~ October 1998.

Scope

45. The Directive applies generally to the processing of personal data by a "controller" in an EU Member State[7]. It therefore applies to data about natural persons, whether held by the public or private sector. Most categories of manual and computerised data processing are covered[8].

Provisions on Transborder Data Flows

47. The EU Directive ensures ~~promotes~~ transborder data flows within the EU on the basis of equivalent protection provided in all Member States and allows ~~, but may restrict~~ transfers to third countries which provide adequate protection. Member States are not permitted to inhibit the free movement of personal data within the EU simply for reasons of privacy protection[9], because of the equivalent and high level of protection ensured by the Directive throughout the Community. A transfer of data outside the EU may take place to third countries which guarantee ~~However, before a member state may transfer personal data outside the EU,~~ an "adequate" level of protection ~~must exist in the recipient country~~[10]. 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[11].

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, intervention powers and the ability to −engage in legal proceedings[12].

49. With respect to enforcement, the EU Directive covers judicial remedies, liabilities and sanctions[13]. It states that persons shall be entitled to judicial remedies and compensation from data controllers for damage suffered as a result of unlawful processing. Member States have ~~are free~~ to adopt suitable administrative, civil or criminal sanctions.

Other Developments

52 a. On December 15 1997, Directive 97/66/EC[14] was adopted by the European Parliament and the Council. This Directive particularises and complements Directive 95/46/EC with respect to the processing of personal data and the protection of privacy in the telecommunications sector. It provides for the harmonisation of the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of

personal data in the telecommunications sector and to ensure the free movement of such data and of telecommunications equipment and services in the Community.

2. International Colloquia on Privacy Protection

(d) International Organi~~z~~sation for Standardi~~z~~sation

B. National Instruments

AUSTRALIA

Laws

~~*Federal Approach to Privacy in the Private Sector*~~

65. The ~~application of the~~ Privacy Act has a limited application to the private sector. In particular, it allows the Privacy Commissioner to issue guidelines in relation to tax file numbers.~~, and t~~The Act also regulates the information handling practices of the consumer credit reporting industry. ~~(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[15].~~

65 a. A Bill to amend the Privacy Act was before the Australian Senate before a federal election was called. The Bill proposed to amend the Privacy Act to extend the coverage of the IPPs to private sector contractors holding personal information under contracts to provide services to or for a Commonwealth agency.

65 b. The Bill is being examined by the Senate Legal and Constitutional References Committee which is expected to report shortly. Its report and the Bill will be considered by the incoming government.

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")[16]. 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*[17] 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"[18]. 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 (*Taxation Administration Act 1953*~~*Data-matching Program (Assistance and Tax) Act 1990*~~), and for specific procedures, such as the interception of telecommunications and the disclosure of personal information by telecommunications companies (*Telecommunications Act 1997*)[19]. The *Data-matching Program (Assistance and Tax) Act 1990* provides privacy protections in relation to the matching of personal information relating to tax and social welfare benefits by Commonwealth Government Departments.

State and Territory Laws

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[20]. The *Privacy Committee Act 1975 (NSW)*[21] establishes the *New South Wales Privacy Committee* which conducts research relating to privacy issues and acts as a dispute conciliator.[22] 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 guidelines (based on 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[23].

Self-Regulatory Instruments

69 a. In March 1997, the Prime Minister announced that the Commonwealth would not enact legislation to provide privacy protection in the private sector.[24] The Government was concerned not to increase the regulatory burden on business. The Prime Minister made available the federal Privacy Commissioner to assist business in the development of voluntary codes of conduct.

69. b. In February 1998, the Commissioner released the *National Principles for the Fair Handling of Personal Information* (the "National Principles")[25]. The National Principles set out privacy standards that are based on the OECD Privacy Guidelines. A number of industries have or are considering implementing the National Principles in, for example, codes of conduct.

Instruments Relating to Online Privacy

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

70. In February 1998, the *Internet Industry Association* released a draft voluntary *Industry Code of Practice*[26] that proposes general standards of behaviour for those involved in the Internet industry[27]. The Code fully implements the National Principles (which are based on ~~reflects~~ the OECD Privacy 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*[28].

Other Initiatives

71. Other self-regulatory initiatives include:

- Smart Card Industry Code of Conduct developed by the Asia-Pacific Smart Card Forum;[29]
- General Insurance Information Privacy Principles developed by the Insurance Council of Australia (incorporating the National Principles);
- Privacy Principles for Intelligent Transport Systems developed by Standards Australia; and
- The Australian Communications Industry Forum (the "ACIF")[30] is in the process of drafting a Code dealing with telecommunications privacy issues, such as, customer personal information and calling number display.[31] The ACIF has also published guidelines on the Development of Telecommunications Industry Consumer Codes (January 1998)[32] 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 of* ~~(~~1978~~)~~ (*Datenschutzgesetz. BGBl. Nr. 565/1978*) regulates the use of computerised data in the public and private sectors, creates a central registration system and provides civil remedies and criminal sanctions[33].~~-~~ A new law is being prepared to implement the EU Data Protection Directive.

73. An independent Commission (the *Datenschutzkommission~~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 against public data controllers, and can impose sanctions for certain actions, such as breaches of transborder data flow authorisations. A *Council for Data Protection* also exists and may be referred to by the Commission for advice on certain matters. Complaints against private data controllers must be brought before the courts.

CANADA

Laws

Federal Approach to Privacy in the Private Sector

87. The Canadian federal government ~~has expressed its intention to~~ introduced ~~develop~~ privacy legislation to protect personal information in the private sector ~~in the fall of~~ on October 1, 1998 with the legislation to be in force by the year 2000[34]. The options for legislation are canvassed in a discussion paper, "The Protection of Personal Information: Building Canada's Information Economy and Society"[35], which was published by the *Task Force on Electronic Commerce* (formed by *Industry Canada* and *Justice Canada*) in January 1998. A detailed synopsis of the responses, "Summary Report of the Responses to the Discussion Paper", was released in July 1998. The government has indicated that it will model its legislation regarding the protection of privacy on the CSA Standard (see paragraph 91).

Provincial Laws

90. Quebec is the only province where general legislation, the *Act Respecting the Protection of Personal Information in the Private Sector* (1993),[36] regulates the handling of personal information by private sector organisations, including corporations, sole proprietorships, partnerships, organizations and associations. The Act governs the collection and use of personal information and provides individuals with access and correction rights and for the resolution of disputes before the Commission d'accèés àá l'information, the agency which is responsible for oversight and redress for public sector information access and privacy rights in the province. It is noteworthy that the law has special provisions which apply to lists of names used for marketing purposes and to transfers of information about Quebec residents to third parties outside of the province.

Self-Regulatory Instruments

The CSA Model Code

92. The CSA has prepared a workbook, "Making the CSA Privacy Code work for You"[37], to assist in the development of compliant codes (which may be certified by the *Quality Management Institute*, a division of the CSA). In terms of ensuring ongoing compliance with a code, the workbook highlights the importance of independent audits by duly certified auditors. Private sector codes may be certified as complying with the CSA standard by a quality registrar and a company may cite the standard in an ISO 9000 registration. There are a variety of ways in which a company may demonstrate compliance, e.g., the~~. An example of such a certified code is the~~ Canadian Bankers' Association *Privacy Model Code*~~.~~[38] was verified by Price Waterhouse.

Other Initiatives

92 a. A number of companies and associations hve developed CSA based privacy codes, including Stentor (the alliance of telecommunications providers), the *Canadian Direct Marketing Association* ("CDMA") and the Canadian Medical Association ("CMA").

Instruments Relating to Online Privacy

~~*Other Initiatives*~~

~~8. 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.~~

THE NETHERLANDS

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*)[39]. The Registration Chamber has the power to investigate breaches of the law and to enforce its provisions. It can ~~does not have to act on complaint to~~ conduct an inquiry on its own intiative.

PORTUGAL

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)[40], regulations establishing institutions such as a registry of non-donors of human organs[41] and an Identity Card Centre ~~of Identity cards~~[42], and regulations controlling the data bases operated by the Gendarmerie[43], the Border and Foreign Services[44] and the Criminal Police[45].

SWEDEN

Constitution

210. The Swedish Constitution guarantees the right of individuals to have access to documents and data held by public authorities. It also provides that citizens shall be protected to the extent determined in detail by law against any infringement of their personal integrity resulting from the registration of information about them by means of electronic data processing.

Comprehensive Laws

211. A Parliamentary resolution of 16 April 1998 approved the *Personal Data Act* which implements the EU Directive in Sweden[46]. 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*)[47]. 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.

UNITED KINGDOM

Implementation of the EU Directive

229. ~~A Data Protection Bill designed to implement the EU Directive was published in January 1998 and is currently going through the Parliamentary process[48]. Much of the detail of the new law will be contained in secondary legislation.~~

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 with respect to government restrictions on certain activities or invasions of ~~although primarily relating to~~ physical privacy ~~rather than personal information~~.

Laws

Federal Sectoral Laws

235. Federal Acts with privacy implications for specific kinds of information include: [49]

- The *Federal Trade Commission Act* (1914) which prohibits unfair or deceptive trade practices, and, thus, holds companies responsible for their representations of their privacy practices;

- The *Fair Credit Reporting Act* (1970)[50] which regulates the collection and use of information collected by consumer reporting agencies such as credit bureaus~~x~~, medical information companies and tenant screening services. It is administered by the *Federal Trade Commission* (the "FTC")[51] and it provides a private cause of action, actual and punitive damages, as well as attorneys fees, and it imposes duties on furnishers of information to credit bureaus and users of credit reports in addition to duties imposed on credit bureaus;

- The *Cable Communications Policy Act* (1984)[52] which regulates the use of cable television subscriber records under a regime of notice and consent;

- The *Electronic Communications Privacy Act* (1986)[53] 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)[54], the *Tax Reform Act of 1976*[55], and the *Right to Financial Privacy Act* of 1978[56] which prescribe limits on data matching, ~~and~~ the use of information collected pursuant to statutory duties, and government access to certain financial records;

- The *Video Privacy Protection Act* (1988)[57] which controls the use of video rental or sale records;

- The *Telephone Consumer Protection Act* (1991)[58] which regulates unsolicited telephone calls; and

- The *Telecommunications Act* (1996)[59] which regulates the disclosure of transactional data in telecommunications services and is administered by the *Federal Communications Commission*;

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)[60] by the *Information Infrastructure Task Force* (the "IITF")[61] 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)[62] 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)[63] 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)[64] 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;

- "Individual Reference Services: A Report to Congress" (December 1997) by the FTC which discussed the benefits and risks of look-up service databases used to locate, identify, or verify the identity of individuals. The report also discussed the self-regulatory principles adopted by industry members;

- "Elements of Effective Self-Regulation for Protection of Privacy" (January 1998)[65] 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;

- "Privacy Online: A Report to Congress ~~on Privacy Online~~" (June 1998)[66] 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* in July 1998, 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 authorising enforcement by a government agency;[67] 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.[68] It also gives the Office of Management and Budget responsibility for coordination of privacy issues, drawing on expertise and resources of other governmental agencies.

Other Initiatives

239. Other self regulatory initiatives include:

- The *Direct Marketing Association*[69] 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"[70] 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*[71] 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. Firms must submit to an annual third party audit with results made public.

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

1. Restricting or Eliminating the Automatic Disclosure and Collection of Personal Data

(a) Restricting the Creation of Cookies

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. However, further development of the technologies may make their use more streamlined and effective.

2. Reducing or Avoiding the Need for Personal Data Disclosure

(a) Anonymous Payment Systems

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

1. Optional Data Fields and Click-Box Choices

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*[72] 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*[73] operate a similar system. A unique random number is assigned, using a cookie, to each user visiting one of its sites[74]. 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.~~

F. Enforcing Privacy Principles

286. Irrespective of the regime in question, effective enforcement has two aspects. The first side to enforcement is comprised of those mechanisms ~~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[75].

Accounting Firms

296. Privacy audits are one of the services now being carried out by large accounting firms[76]. 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[77]. 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. The US *Individual Services Reference Group* principles provide for annual audits by a third party accounting firm.

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 Commission Act*[78], or TRUSTe may conduct breach of contract or trademark infringement litigation against the site.

The Australian Internet Industry ~~Internet~~ Association

314. In February 1998, the Australian *Internet Industry Association* released a draft *Industry Code of Practice*[79]. In the first instance, it is intended that complaints will be dealt with between the user and the Code Subscriber~~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* directing the subscriber to comply with the Code or to provide ~~for~~ corrective advertising and/or the payment of compensation. The Council may also withdraw permission for a site to use its *Code Compliance Symbol*.

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[80]. Procedurally, such complaints are usually brought to court by the injured data subject. In addition, in some common law countries, actions may also be brought based on a tort of invasion of privacy.

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[81]. 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[82]. -

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~~[83].

G. Educating Users and the Private Sector

334. In addition to traditional methods of public education in schools, the workplace and the media,[84] 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[85]; (2) government bodies, such as the FTC in the U.S.[86] and many central oversight authorities in other parts of the World[87]; and (3) private sector organisations, such as *Project OPEN* (the Online Public Education Network)[88], the US *Direct Marketing Association*[89], the *Center For Democracy and Technology* (the "CDT")[90], the *Electronic Privacy Information Center* ("EPIC")[91], "Call for Action" -and TRUSTe[92]. 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

B. Data Protection Authorities

Australia

Australian Privacy Commissioner~~'s Office~~
GPO Box 5218
Sydney NSW 1042
AUSTRALIA
Telephone: +1300 363 992 (from within Australia)
Fax: + 61 2 ~~(02)~~ 9284 9666
E-mail: privacy@privacy.gov.au
Web: http://www.privacy.gov.au/

Austria

Datenschutzkommission~~Bundeskanzleramt~~
Ballhausplatz 1
1014 Wien~~Vienna~~
~~1014~~
AUSTRIA
Telephone: + ~~(~~43 1 531 15 2528
Fax: + 43 1 531 15 2690
E-Mail: georg.lechner@bka.gv.at

United States

Federal Trade Commission
Washington, D.C. 20580
Telephone: +1 202 326-2222
Fax: +1 202 326-2496
E-Mail: crc@ftc.gov
Web: http://www.ftc.gov

C. Non-Governmental Organisations

Asia-Pacific Smart Card Forum

G.P.O. Box 1966
Canberra ACT 2601
AUSTRALIA
Web: http://www.aeema.asn.au/Divisions/apscf.htm

NOTES

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

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

3. Figures as at December 1997. The Table of National Instruments (see page 13) shows those OECD Member countries which have ratified Convention 108.

4. Article 6, Convention 108.

5. Article 12, Convention 108.

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

7. 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)

8. Articles 3 and 4, EU Directive.

9. Article 1(2), EU Directive.

10. Article 25(1), EU Directive.

11. Article 26, EU Directive.

12. Article 12, EU Directive.

13. Article 28, EU Directive.

14. Document available at http://www2.echo.lu/legal/en/dataprot/protection.html

15. 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

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

17. "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

18. ~~Recommendation 17. Chapter 7, Paragraph 75.~~

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

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

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

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

23. 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

24. A recent report by the *Joint Committee of Public Accounts and Audit* ("Internet Commerce - To Buy or not to Buy?", June 1998, see http://www.aph.gov.au/house/committee/jpaa/elecom/report/contents.htm) recommends a legislative approach. It states (recommendation 17, chapter 7, paragraph 75) 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". The issue is expected to be considered by the incoming government following the federal elections scheduled for 3 October, 1998.

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

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

27. Clauses 8 and 9 of the draft Code.

28. "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

29. The Code is available at http://www.aeema.asn.au/apscfcode.htm~~Copies of the Code are available from the Asia-Pacific Smart Card Forum, G.P.O. Box 1966, Canberra ACT 2601, AUSTRALIA.~~

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

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

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

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

34. 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).

35. 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

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

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

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

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

40. Law 109/91 of 17 August 1991.

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

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

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

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

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

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

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

48. 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

49. 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).

50. 15 U.S.C. § 1681-1681(u), as amended is available on the FTC website at http://www.ftc.gov/os/statutes/fcra.htm

51. 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 modified in order to refer to the Federal Trade Commission Act)

52. 47 U.S.C. § 551.

53. 18 U.S.C. § 2510.

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

55. 26 U.S.C. § 6103 (1989) & Supp. 1996

56. 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).

57. 18 U.S.C. § 2710.

58. 47 U.S.C. § 227.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

75. 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.

76. 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).

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

78. See paragraph (321)

79. See paragraph 69 c. The National Principles can operate in online or electronic environments. In May *1998, the* Online Council, which comprises federal, state and territory IT Ministers, acknowledged the Principles as providing a basis for a national benchmark on privacy standards.

.

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

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

82. For instance, the US *Fair Credit Reporting Act* imposes criminal sanctions on those who obtain a credit report ~~without a permissible purpose~~under false pretenses.

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

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

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

87. 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).

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

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

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

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

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