Privacy Online

OECD GUIDANCE ON POLICY AND PRACTICE



OECD

Privacy Online

OECD Guidance on Policy and Practice

OECD

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Pursuant to Article 1 of the Convention signed in Paris on 14th December 1960, and which came into force on 30th September 1961, the Organisation for Economic Co-operation and Development (OECD) shall promote policies designed:

- to achieve the highest sustainable economic growth and employment and a rising standard of living in member countries, while maintaining financial stability, and thus to contribute to the development of the world economy;
- to contribute to sound economic expansion in member as well as non-member countries in the process of economic development; and
- to contribute to the expansion of world trade on a multilateral, non-discriminatory basis in accordance with international obligations.

The original member countries of the OECD are Austria, Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The following countries became members subsequently through accession at the dates indicated hereafter: Japan (28th April 1964), Finland (28th January 1969), Australia (7th June 1971), New Zealand (29th May 1973), Mexico (18th May 1994), the Czech Republic (21st December 1995), Hungary (7th May 1996), Poland (22nd November 1996), Korea (12th December 1996) and the Slovak Republic (14th December 2000). The Commission of the European Communities takes part in the work of the OECD (Article 13 of the OECD Convention).

Publié en français sous le titre :

Protection de la vie privée en ligne
ORIENTATIONS POLITIQUES ET PRATIQUES DE L'OCDE

© OECD 2003

Permission to reproduce a portion of this work for non-commercial purposes or classroom use should be obtained through the Centre français d'exploitation du droit de copie (CFC), 20, rue des Grands-Augustins, 75006 Paris, France, tel. (33-1) 44 07 47 70, fax (33-1) 46 34 67 19, for every country except the United States. In the United States permission should be obtained through the Copyright Clearance Center, Customer Service, (508)750-8400, 222 Rosewood Drive, Danvers, MA 01923 USA, or CCC Online: *www.copyright.com*. All other applications for permission to reproduce or translate all or part of this book should be made to OECD Publications, 2, rue André-Pascal, 75775 Paris Cedex 16, France.

FOREWORD

Addressed to OECD member countries, business and industry, and individual users, *Privacy Online: Policy and Practical Guidance* has been prepared under the auspices of the OECD Committee for Information, Computer and Communications Policy (ICCP) by its Working Party on Information Security and Privacy (WPISP).

Focused on the implementation of the OECD Privacy Guidelines online, the policy and practical guidance offered in this report is based on the work achieved within the OECD to fulfil the 1998 Ministerial Declaration on the Protection of Privacy on Global Networks. It reflects the OECD ministerial high-level objective to build bridges between different national approaches in order to ensure the effective protection of privacy and personal data as well as the continued transborder flow of personal data on global networks.

Intended to reinforce the impact and visibility of the action of the OECD, and the importance of the OECD Privacy Guidelines in the development and implementation of a mix of solutions for ensuring global privacy and the free flow of information, the volume is structured as follows:

- Part I provides an overview of the work achieved by the WPISP between 1998 and 2002.
- Part II offers policy and practical guidance based on this work.
- Part III includes all documents and other instruments (*e.g.* Internet-based tools) presented in Part I.

Within the OECD, the work has been coordinated by Anne Carblanc who acted as the secretary advisor to the WPISP and the ICCP.

The inventory of instruments and mechanisms contributing to the implementation and enforcement of the OECD Privacy Guidelines on Global Networks in Chapter 6 was prepared by the secretariat with contributions from member countries, international and regional organisations and the OECD Business and Industry Advisory Committee (BIAC).

The content of the Privacy Generator presented in Chapter 7 was prepared by the secretariat with contributions from member countries and the OECD Business and Industry Advisory Committee (BIAC) which also recruited companies to test the Generator. Data Protection Commissioners [notably in Canada, Hong Kong (China), New Zealand and the United Kingdom], as well as consumer groups and consumer protection experts (notably Canada's Public Interest Advocacy Centre and Denmark's Consumer Council, gave helpful input and advice. The tool itself was developed by the secretariat, including its Information and Communications Technology Service, with the support of DaimlerChrysler and Microsoft. The privacy wizards being developed by TRUSTe, AT&T and the DMA were of help in the initial stages. The OECD secretariat recognises the contributions of James Palmer, Rachael Wellby, Amanda Chandler and Steve Fuzesi, as well as the support received from Joachim Schlette, Alfred Büllesbach and Christian Lallemand, for the development of the Privacy Policy Statement Generator. Peter Lübkert of the OECD secretariat provided his advice and the technical assistance of his division. Julie Harris, also of the OECD secretariat, assisted in producing this volume.

Chapters 9 and 10 were prepared by the secretariat with contributions from the Committee on Consumer Policy (CCP) and the WPISP. The Dutch government made a special contribution to the work described in Chapter 10, which is gratefully acknowledged.

Chapter 11 was prepared by Chris Kuner, a partner in the law firm Hunton & Williams and a consultant to the OECD, on the basis of contributions received from OECD member countries and under the supervision of the secretariat.

The inventory of privacy-enhancing technologies in Chapter 12 was prepared by Lauren Hall, a consultant to the OECD, in co-operation with the secretariat. Formerly the Executive Vice President of the Software & Information Industry Association (SIIA), Ms Hall is Director of Technology Policy, Advanced Strategy and Policies, Microsoft Corporation.

Chapter 13 reports on the OECD forum on privacy-enhancing technologies and includes two studies as appendices. The first is the work of Laurent Bernat, Director, Projetweb, and the second was presented by Perri 6, Director, The Policy Programme, Institute for Applied Health and Social Policy, King's College, London, consultants to the OECD.

Chapter 14 was prepared in collaboration with a number of experts and consultants. It incorporates contributions from member countries, international and regional organisations and the Business and Industry Advisory Committee (BIAC). Particular thanks go to Elizabeth Longworth, Lawyer, Principal of Longworth Associates, New Zealand, who drafted the first version. Useful contributions were received from Lorraine Brennan, Director of Arbitration and Intellectual Property, and Legal Counsel, US Council for International Business; Alexander Dix, Data Protection and Access to Information Commissioner for Brandenburg, Germany; and Ian Lloyd, Professor of Information Technology Law and Director of the Centre for Law, Computers and Technology at the University of Strathclyde, United Kingdom.

The volume is published on the responsibility of the Secretary-General of the OECD.

TABLE OF CONTENTS

FOREWORD		3
MAIN POINTS		7
PART I. OECD WORK ON PRIVACY: AN OVERVIEW		**9**
CHAPTER 1.	INTRODUCTION	11
CHAPTER 2.	FULFILLING THE MINISTERIAL MANDATE: OECD WORK	15
PART II. POLICY AND PRACTICAL GUIDANCE FOR IMPLEMENTING PRIVACY PROTECTION ONLINE		**25**
CHAPTER 3.	POLICY AND PRACTICAL GUIDANCE FOR IMPLEMENTING PRIVACY PROTECTION ONLINE	27
PART III. REFERENCE DOCUMENTS		**35**
CHAPTER 4.	GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA	37
CHAPTER 5.	MINISTERIAL DECLARATION ON THE PROTECTION OF PRIVACY ON GLOBAL NETWORKS	43
CHAPTER 6.	INVENTORY OF INSTRUMENTS AND MECHANISMS CONTRIBUTING TO THE IMPLEMENTATION AND ENFORCEMENT OF THE OECD PRIVACY GUIDELINES ON GLOBAL NETWORKS	47
CHAPTER 7.	OECD PRIVACY POLICY STATEMENT GENERATOR	117
CHAPTER 8.	BUILDING TRUST IN THE ONLINE ENVIRONMENT: BUSINESS-TO-CONSUMER DISPUTE RESOLUTION, REPORT OF THE DECEMBER 2000 OECD CONFERENCE	147
CHAPTER 9.	LEGAL PROVISIONS RELATED TO BUSINESS-TO-CONSUMER ALTERNATIVE DISPUTE RESOLUTION IN RELATION TO PRIVACY AND CONSUMER PROTECTION	205
CHAPTER 10.	RESOLVING E-COMMERCE DISPUTES ONLINE: ASKING THE RIGHT QUESTIONS ABOUT ALTERNATIVE DISPUTE RESOLUTION	221

CHAPTER 11. COMPLIANCE WITH, AND ENFORCEMENT OF, PRIVACY PROTECTION ONLINE 227

CHAPTER 12. INVENTORY OF PRIVACY-ENHANCING TECHNOLOGIES 245

CHAPTER 13. PRIVACY-ENHANCING TECHNOLOGIES: REPORT ON THE OECD FORUM SESSION 269

CHAPTER 14. TRANSBORDER DATA FLOW CONTRACTS IN THE WIDER FRAMEWORK OF MECHANISMS FOR PRIVACY PROTECTION ON GLOBAL NETWORKS 339

ANNEX. WHERE TO FIND INFORMATION ON PRIVACY

CONTACT DETAILS FOR INTERNATIONAL AND REGIONAL ORGANISATIONS, NATIONAL GOVERNMENTAL AUTHORITIES, NON-GOVERNMENTAL ORGANISATIONS AND PRIVATE SECTOR ORGANISATIONS **379**

MAIN POINTS

International co-operation to build trust online

OECD member countries have worked since the 1998 Ottawa Ministerial Conference, in close co-operation with representatives of business, industry, consumers and civil society, to build bridges between different national approaches to privacy in order to secure effective privacy protection online and to build trust in business-to-consumer electronic commerce, based on the OECD Privacy Guidelines. Given the global nature of network technologies, international co-operation is critical for the cross-border protection of privacy and personal data online.

Building bridges and blending approaches

There is broad consensus on the important role of privacy protection in building trust in the online environment. Effectively protecting privacy online and ensuring the continued transborder flow of personal data are shared objectives. The means by which those objectives may be achieved are viewed differently in member countries. There is agreement however, that there is no single uniform solution. A mix of regulatory and self-regulatory approaches blending legal, technical and educational solutions that suit the legal, cultural and societal context in which they operate holds the promise to provide effective solutions that, beyond the objective of building bridges, go to the actual integration of different elements into viable solutions. A committed and complementary involvement of governments, businesses, and individual user or consumer groups ("participants") is also key to the successful implementation of this mixture of privacy measures: all have a role to play to help promote respect for appropriate privacy protection on global networks and thus, increase confidence in electronic commerce.

Policy and practical guidance for strengthening privacy online

Four years after Ottawa, the promotion of privacy protection online has led to an evolution of Web sites' privacy practices. Even if there is still room for improvement, progress to date in implementing privacy protection online is encouraging. All participants will need to remain actively engaged in fostering policies and practices that encourage the effective protection of privacy online. Primarily addressed to OECD member countries, this report includes policy advice and practical steps relevant to all participants, that can help ensure respect for privacy protection at the global level, based on the OECD Privacy Guidelines. It also aims at raising awareness about online privacy issues and safeguards.

A step in a continuous process

Because of continuous technical innovation in the Internet environment, and the impact of the global nature of information systems and information flows on the evolution of national cultures and perceptions related to privacy, this report should not be seen as the end of, but as a stage in, the work of the OECD to promote respect for important rights and open economies and societies, and in the particular case, to ensure effective privacy protection on global networks as well as the continued transborder flow of personal data.

Part I

OECD WORK ON PRIVACY: AN OVERVIEW

Chapter 1

INTRODUCTION

The 1980 OECD Privacy Guidelines

The OECD Privacy Guidelines have become established as the basic principles relating to international privacy protection.

The Recommendation concerning the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data was adopted by the Council of the OECD on 23rd September 1980.[1] The eight principles are:

- Collection limitation.
- Data quality.
- Purpose specification.
- Use limitation.
- Security safeguards.
- Openness.
- Individual participation, and
- Accountability.

The 1980 Privacy Guidelines are still recognised as representing an international consensus on privacy standards and providing guidance on the collection of personal information in any medium. They are still seen as a foundation for privacy protection on global networks.

Privacy protection in the global information society

The development of digital computer and network technologies, and in particular the Internet, has brought with it the promise of social and economic benefits by encouraging information exchange, allowing the creation of new products and services, and increasing individual user choice. However the integration of global networks into everyday life and technological innovation that create more opportunities for personal information to be captured, have both increased the benefits of customisation to the individual user and raised concerns over the protection of privacy and personal data.

In the digital economy, individuals may leave behind electronic “footprints” or 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. The related privacy issues arise from the fact that all this computer-processable personal information, whether automatically generated or not, can potentially be collected, stored, detailed, individualised, linked and put to a variety of uses in places geographically dispersed all around the world, possibly without user knowledge or consent.

Background to the Ministerial Mandate

In light of the OECD's drafting of the 1980 Guidelines and continuous work related to privacy, the OECD was considered an appropriate forum to foster a dialogue among governments, business and industry, the user and consumer communities and data protection authorities in order to:

- Raise issues linked to the protection of privacy and transborder flows of personal data in relation to global networks; and
- Consider various solutions that could facilitate the seamless implementation of privacy protection online and contribute towards building a trustworthy environment for the development of electronic commerce.

Broad political attention was first given to privacy online at the OECD Conference "Dismantling the Barriers to Global Electronic Commerce" held in Turku, Finland, on 19-21 November 1997, where privacy, security and consumer protection were considered critical elements for building trust in the online environment; a *sine qua non* condition for the development of electronic commerce.

A few main themes related to privacy protection in the context of global information and communication networks emerged from the OECD Workshop: "Privacy Protection in a Global Networked Society" held in Paris on 16-17 February 1998. In particular, the need to allow individuals to make relevant decisions regarding their personal data, the key issue of allowing free flow of data, the need for flexible and effective privacy protection instruments, the potential for technological solutions, the requirement for enforcement and redress and the need for better education were highlighted.

These themes were refined and further developed during the preparation of the OECD Ministerial level Conference "A Borderless World: Realising the Potential of Global Electronic Commerce" held in Ottawa on 7-9 October 1998. At the conference, ministers adopted a Declaration on the Protection of Privacy on Global Networks,[2] and launched action in this area to be pursued over the next few years.

Ministerial Declaration

The 1998 Ottawa Ministerial Declaration recognised that "the technology-neutral principles of the 1980 OECD Privacy Guidelines continue to represent international consensus and guidance concerning the collection and handling of personal data in any medium, and provide a foundation for privacy protection on global networks."

Ministers reaffirmed "their commitment to the protection of privacy on global networks in order to ensure the respect of important rights, build confidence in global networks, and to prevent unnecessary restrictions on transborder flows of personal data". They agreed to take the necessary steps to ensure, by various specified measures, the effective implementation of the OECD Privacy Guidelines on global networks. They charged the OECD with examining specific issues raised by, and with providing practical guidance to member countries on, the implementation of the Guidelines online.

Ministers also agreed to review progress made in achieving the objectives of their Declaration within a period of two years, and to assess the need for further action to ensure the protection of personal data on global networks in pursuit of these objectives. Progress in achieving the objectives of the Ottawa Ministerial Declaration was reported in 1999 at the Paris Forum and in 2001 at the Emerging Market Economies Forum in Dubai.

OECD Action Plan

The action items approved by ministers at the Ottawa conference were integrated in the OECD Action Plan, and assigned to the appropriate committees and working parties.[3] In this context, the Working Party on Information Security and Privacy (WPISP), under the auspices of the Committee for Information, Computer and Communications Policy (ICCP) focused much of its work on the implementation of the elements of the OECD six-step programme of work for online privacy protection:

- Encouraging the adoption of privacy policies.
- Encouraging the online notification of privacy policies to users.
- Ensuring that enforcement and redress mechanisms are available in cases of non-compliance.
- Promoting user education and awareness about online privacy and the means at their disposal for protecting privacy.
- Encouraging the use of privacy-enhancing technologies.
- Encouraging the use and development of contractual solutions for online transborder data flows.

All documents and other instruments (*e.g.* Internet-based tools) produced by the WPISP and declassified by the ICCP are included in this publication (see Part III). They form the basic output material upon which Part II on policy and practical guidance draws.

NOTES

1. See Chapter 4. The Recommendation concerning the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data was adopted by the Council of the OECD on 23 September 1980.

2. See Chapter 5.

3. *(i)* The Working Party on Information Security and Privacy (WPISP) worked under the auspices of the Committee for Information, Computer and Communications Policy (ICCP) on the protection of privacy and personal data; secure infrastructures and technologies, authentication and certification; and cryptography (under theme A of the Action Plan – "Building Trust for Users and Consumers"). *(ii)* The WPISP also worked in conjunction with the Committee on Consumer Policy which worked on the consumer protection aspects of electronic commerce (under theme A of the Action Plan). *(iii)* The Committee on Fiscal Affairs worked on taxation issues (under Theme B of the Action Plan – "Establishing Ground Rules for the Digital Marketplace"). *(iv)* The Trade Committee worked on the trade policy and market access aspects of electronic commerce (under Theme B of the Action Plan). *(v)* The Working Party on Telecommunication and Information Services Policies worked under the auspices of the ICCP on access to and use of the information infrastructure (under Theme C of the Action Plan – "Enhancing the Information Infrastructure for Electronic Commerce"). *(vi)* The Public Management Committee worked on the promoting global awareness of the "Y2K problem" (under Theme C of the Action Plan). *(vii)* The ICCP worked on the policy implications of the economic and social impacts of global electronic commerce (under Theme D of the Action Plan – "Maximising the Benefits"). *(viii)* The Development Assistance Committee worked on ensuring global participation (under Theme D of the Action Plan). *(ix)* The Industry Committee (currently known as the Committee on Industry and Business Environment) worked on electronic commerce and SMEs (under Theme D of the Action Plan). *(x)* The Centre for Educational Research and Innovation worked on educational software and multimedia (under Theme D of the Action Plan).

Chapter 2

FULFILLING THE MINISTERIAL MANDATE: OECD WORK

This chapter summarises the various elements of the OECD's work on ensuring privacy protection online.

Chapter 2

FULFILLING THE MINISTERIAL MANDATE: OECD WORK

OECD member countries adopted a pragmatic approach to fulfilling the Ministerial mandate. Their work has included a strong emphasis on education, gathering legal and technical information, collecting and distributing examples of efforts and experience on implementation of the Guidelines, offering a forum for discussion, building an Internet-based tool, and exploring and discussing a number of legal and technical instruments and mechanisms to ensure privacy protection online.

OECD member countries first undertook to survey, at international, regional and national levels, the variety of legal instruments, practices and technologies, either in use or being developed, to implement and enforce privacy principles in the online environment. The inventory[1] included horizontal or sectoral data protection laws, codes of conduct, industry standards and industry-led technological solutions, including privacy enhancing technologies (PETs), online educational tools, systems for labelling, certifying and attaching privacy seals, and dispute resolution schemes. It was noted that technological tools were increasingly used to protect privacy rights online. The fact that effective protection of privacy online required online participants to be not only "information technology literate", but also aware of the privacy implications of their actions was emphasised.

1) Encouraging the adoption of privacy policies

OECD member countries developed a Privacy Policy Statement Generator[2] (OECD Privacy Generator) as an educational Internet technology tool which provides organisations with support and guidance in developing policies and practices consistent with the OECD Privacy Guidelines. In particular, the generator was designed to assist organisations in developing privacy policies and statements for display on their Web sites.

The OECD Privacy Generator provides a means by which organisations can review their current privacy practices through use of a questionnaire about the practices followed by the organisation. A draft policy statement is then created by the generator which provides an indication of the extent to which the organisation's practices adhere to the OECD Privacy Guidelines. The draft statement provides a basis which may be corrected or expanded as needed to accurately reflect the privacy practices of the organisation as part of the process by which a definitive policy statement may be prepared. The generator may be adapted so that it also relates to issues of concern in particular member countries. It also offers links to relevant government and private sector organisations.

Member countries noted that, at least in some countries, the posting of a privacy policy will render an organisation legally liable for any action in breach of that policy. In all cases, the statement itself will need to be assessed against the requirements of national laws. In any event, the existence of the generator should assist national efforts to encourage organisations to adopt privacy policies whether or not they are required to do so by law.

Member countries also considered that use of the OECD Privacy Generator should promote greater consistency in privacy protection across national borders. It can help organisations to understand the requirements of privacy protection principles at national and international levels and to

build trust with other organisations and individual users online. It can also help individual users to become educated to look for privacy statements as a routine part of their online experiences.

2) Encouraging the online notification of privacy policies to users

By making the Privacy Policy Statement Generator freely available, the OECD has contributed to both organisation and individual user awareness of online privacy issues. The generator makes it easier for organisations to provide individual users with online notice of their privacy policies.[3] The inclusion of links to relevant government and private sector Web sites is intended to increase business and other organisations' as well as individual user and consumer awareness of the privacy protection framework that applies to their online activities.

By endorsing the OECD Privacy Policy Statement Generator, member countries took a key practical step towards encouraging openness and trust in electronic commerce among visitors to Web sites.

The positive perception by the public of online privacy policies is confirmed by a few public opinion polls and surveys. For example, a study conducted in 2000 showed that 75% of online users and consumers tended to trust Web sites more when privacy policy statements were posted on those merchants' sites.[4] Similarly, a May 2002[5] study concluded that up to $24.5 billion in online sales were likely to be lost by 2006 because of bad privacy policies: "For a business with poor online privacy policies, offline sales will slip as consumers shift to more privacy-sensitive competitors," the report said. Since 1997 however, commercial Web sites have embraced the practice of posting privacy policies in an effort to build trust on line. In March 2002, the Progress and Freedom Foundation[6] reported that 98% of 100 most frequently visited Web sites post a privacy policy, and 88% of random sites also post privacy statements.

3) Ensuring that enforcement and redress mechanisms are available to users in cases of non-compliance with privacy principles and policies

OECD member countries completed several projects addressing the issues of redress, compliance and enforcement mechanisms in the online cross-border context. Of particular interest were alternative dispute resolution (ADR) as well as the variety of alternative methods of compliance and enforcement which go beyond traditional regulatory approaches.

Alternative dispute resolution

OECD member countries undertook a series of studies on ADR, which consists of practical out-of-court methods involving a neutral third-party to resolve disputes in a quick and inexpensive way. In December 2000 the OECD,[7] in conjunction with the Hague Conference on International Law and the International Chamber of Commerce, held a conference in The Hague on "Online Alternative Dispute Resolution Mechanisms for Privacy and Consumer Protection Disputes".[8] The aim of the conference was to explore if and how online ADR mechanisms can help resolve business to consumer (B2C) disputes arising from privacy and consumer protection issues and thus improve trust for global electronic commerce. The primary focus of the conference was on low levels of harm, as well as on informal, flexible systems that allow for the necessary balancing between the type of dispute and the formality of the process for resolution (*e.g.* assisted negotiation and mediation).

A consensus emerged on some principles, such as: settling disputes at an early stage is most effective; flexibility and variety in ADR mechanisms is valuable; appropriate technological

developments may facilitate ADR; individual users need information about processes in order to participate effectively; procedural safeguards are important in some disputes.

The conference was followed up with a work programme focused on legal and educational aspects of ADR. The legal aspect of the programme aimed to generate an overview of national legal regimes applicable to B2C ADR in member countries, with a view to understanding if and how existing legal provisions impact recourse to ADR. A report[9] was developed on the basis of member country responses to a survey on existing laws and regulations related to ADR. The report highlighted that there is not a single set of rules governing ADR. Different rules have developed in different contexts. In a number of areas the existing legal framework provides guidance to potential parties to an ADR procedure at the national level. For example, many countries regulate the provision of arbitration services. However, there are fewer regulations that would generally govern the provision of less formal types of B2C ADR. What regulation there is typically addresses the provision of ADR through mechanisms established, funded or run by governments. As regards flexible and informal ADR mechanisms designed for the online world, no member country reported the existence of specific legal provisions although most expressed an interest in promoting fair and effective online ADR as a way to resolve small value B2C disputes, particularly cross-border disputes. Looking more specifically at the cross-border context, national differences appeared as to the validity of agreements to submit to ADR, the procedural principles for use during an ADR, confidentiality and security of proceedings, validity of settlement agreements arising out of an ADR, and the availability of enforcement mechanisms.

The educational part of the programme aimed to inform individual users and businesses, notably small and medium-sized enterprises (SMEs) about the availability of ADR and its potential benefits. A first set of questions was produced to help individual users determine whether online ADR can help them resolve a dispute, such as what to think about before considering ADR, how to choose a particular form of ADR, where to locate ADR providers, and what to do if ADR cannot help.[10] A second set of questions aimed at guiding SMEs is under preparation.

Finally, the OECD helped to produce further information regarding the availability of ADR by assisting the International Chamber of Commerce (ICC) to produce an inventory of ADR programmes world-wide. The resulting report and inventory are available on the ICC Web site.[11]

Compliance and enforcement mechanisms

Recognising that the higher the level of compliance, the less need there is for enforcement, and that a strong level of enforcement may motivate actors to adopt a higher level of compliance, OECD member countries undertook to survey and analyse enforcement mechanisms that are available both to address non-compliance with privacy principles and policies and to ensure access to redress.[12] The objective was to gather information through a questionnaire addressed to member countries and the private sector that would: *(1)* lead to a better understanding of how privacy safeguards, enforcement mechanisms, and potential remedies can enhance privacy as set forth in the OECD Privacy Guidelines and the Ottawa Ministerial Declaration; and *(2)* form the basis for assessing the practical application of available compliance and enforcement instruments in a networked environment and their ability to meet the objectives of the OECD Privacy Guidelines, including effectiveness and coverage across jurisdictions.

The summary and the analysis of the responses to the questionnaire[13] demonstrated that the legal landscape for privacy compliance and enforcement has changed: if government regulation remains the foundation upon which individual user trust in the area of privacy is based, regulation is increasingly combined with complementary technical, organisational, and self-regulatory mechanisms in order to attain maximum effectiveness. It was noted that many such initiatives are now underway in member

countries, and that there is every sign that their use will grow rapidly in the coming years. Moreover, the report stressed that efforts to ensure compliance before the fact impose less burden than having to rely on enforcement actions. It also demonstrated that it is critical that privacy protection be viewed in a global perspective, rather than in a purely national one, in order to better facilitate redress for privacy violations that cross national borders.

As regards complementary means to better ensure compliance with and enforcement of privacy protection, the report highlighted that OECD member countries and private sector entities have developed and continue to develop methods which tend to: make use of market-based incentives and punishments to encourage compliance with norms; use technical means as a way of better ensuring compliance (*e.g.* privacy-enhancing-technologies or online audits); offer third-party or corporate guarantees (*e.g.* trustmark programs, seals, company privacy officers or online privacy policies); adapt existing mechanisms for privacy compliance and enforcement to the online environment (*e.g.* online filing of, and ADR for privacy-related complaints); and promote technical standards, audits, security policies, and other mechanisms for better ensuring the security of data processing online.

4) Promoting user education and awareness about online privacy and the means of protecting privacy

Promoting user education and skills related to online privacy issues has been one of the objectives of OECD member countries in all areas and particularly in designing the OECD Privacy Generator and examining privacy-enhancing technologies. In this connection, it was noted that education and communication about online privacy protection may need to be tailored to the needs of different participants given the differing constraints, institutional contexts, basic assumptions and outlooks of organisations and individual users. Cultural differences need to be addressed in the formulation of strategies for improving international privacy protection whether through ADR, the use of privacy-enhancing technologies or any other measure.

5) Encouraging the use of privacy enhancing technologies

Privacy-enhancing technologies (PETs) are technological tools whose primary purpose is to help implement privacy principles, such as those contained in the OECD Privacy Guidelines, within the framework of industry-led self-regulation, legal regulation or a combination of these approaches. PETs can empower individuals to choose for themselves and to control their own personal data but they vary in their ability to respond to the different privacy concerns. There are continuous significant advances in the development and use of such technologies.[14]

Work on PETs included an inventory of these technologies, and a special Forum session.

The Inventory of Privacy-Enhancing Technologies[15] was produced to analyse the availability and variety of PETs, consider the factors affecting their adoption, analyse the relationship between technology and privacy, and form a basis for policy makers to discuss the use and deployment of such technologies. The paper[16] discussed methods of online personal data collection, analysed different types of PETs and made recommendations to the private sector for encouraging their increased development and use. Technological tools that can assist in safeguarding online privacy, PETs were shown to present a range of characteristics. Some filter "cookies" and other tracking technologies; some allow for "anonymous" Web-browsing and e-mail; some provide protection by encrypting data; some focus on allowing privacy and security in e-commerce purchases; and some allow for the advanced, automated management of users' individual data on their behalf. In essence, PETs reinforce transparency and choice, which can lead to greater individual control of data protection. However, many technologies can be used in many different ways. Different products, technologies and various

functions can serve different purposes depending on the preferences of the user and the implementation of the particular technology.

A Forum Session on Privacy-Enhancing Technologies[17] was held at the OECD in October 2001 in order to facilitate discussion *(1)* on the policy implications of PETs; *(2)* the future of such tools in the wider context of online privacy protection; and *(3)* the challenges of, and methods for**,** educating business about the importance of privacy by design and the use of PETs, and for educating individuals about the benefits and limitations of PETs. The session made it clear, in particular, that technically speaking, PETs did not offer a full range of functionalities that would provide total privacy protection in line with the OECD Privacy Guidelines (*e.g.* among the PETs surveyed (see paragraph below), only one tool addressed five of the eight privacy principles and 58 applied to only one principle).

A study and a research paper[18] included a synthesis of a survey of PETs available on the Web, and a table of the surveyed technologies, as well as a discussion of the question of when, for whom, and under what circumstances, "communication" about PETs might work, in the sense of encouraging businesses to supply such tools and individuals to use them

PETs were considered to be helpful technological tools to assist in protecting online privacy as part of a wider package of online privacy initiatives.[19] They can empower individual users seeking to control the disclosure, use and distribution of personal information online. PETs can also aid organisations in enforcing their own privacy policies and practices, and more generally, in an era of individual user concerns about online privacy, PETs are crucial tools in managing the flow of personal information on global networks.

The need to encourage both individual and corporate users to deploy and use PETs was stressed. To see greater use and deployment, it was however highlighted that PETs may require a higher degree of usability, clearer technical information and further development to cover a wider range of privacy protection areas in the future.

The early stage of any technological development being its most critical, the concept of designing privacy features and functions into technical solutions was also welcomed. This concept implies for developers to take into account, and integrate privacy protection into systems design and development, and for organisations to consider at an early stage the privacy implications of their technologies and services.

Finally education and awareness-raising about PETs were deemed absolutely critical to the further deployment and use of such tools in homes and the global marketplace. In that respect, it was noted that, for businesses and other organisations, the challenge was to persuade them that they should internalise certain costs (to invest in PETs) in a market where they fear their rivals may externalise such costs. For individual users, it was noted that the challenge of persuasion was shaped first, by the extent to which different types of individuals care about privacy risks and which risks they care about most; second, how preferences for protection against various kinds of risks are traded off against price increments; and third, how individuals will trade off their privacy preference against the cost of searching out and moving to another supplier.

6) Encouraging the use and development of contractual solutions for online transborder data flows

The 1980 Privacy Guidelines contain the following statements on transborder data flows:

> **"Part Three – Basic Principles of International Application: Free Flow and Legitimate Restrictions**
>
> 15. Member countries should take into consideration the implications for other member countries of domestic processing and re-export of personal data.
>
> 16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a member country, are uninterrupted and secure.
>
> 17. A member country should refrain from restricting transborder flows of personal data between itself and another member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A member country may also impose restrictions in respect of 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.
>
> 18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection."

To contribute to the resolution of problems related to transborder transactions, OECD member countries prepared a report on transborder data flow contracts in the online context.[20] The report[21] which was partly directed at online business to business transactions should be read with later documents such as the model contracts published by the European Commission, the Council of Europe and the International Chamber of Commerce.[22]

The effectiveness of contractual solutions was noted. However, the report also highlighted the need to address effectively the issue of the recourse of the individual under business to business transborder data flow contracts, and noted, in this respect, that the support of ancillary measures, such as notice to the individuals at the point of data collection, is important.

In relation to business to consumer contracts, the report noted that attempts to design privacy protection measures for online B2C interactions within the constraints of a contractual framework pose difficulties, notably in establishing a binding intention to contract between an individual visiting a Web site and the data controller of that Web site, and also for individuals wishing to obtain redress under a contract. Member countries therefore agreed to focus less on contractual solutions, and more on exploring how to ensure redress through online alternative dispute resolution measures.

NOTES

1. See Chapter 6.
2. See Chapter 7. The Generator is accessible at www.oecd.org/sti/security-privacy, or http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm.
3. In June 2001, Visa International obliged its online merchants to post privacy policies and encouraged the use of the OECD Generator for their creation. See http://international.visa.com/fb/merchants/news/.
4. The survey found that a combined 75% of people who have seen a privacy policy online, view notices explaining how personal information will be used, as either "absolutely essential" or "very important" (Business Week/Harris, March 2000).
5. Jupiter Research (2002), "Online Privacy: Managing Complexity to Realize Marketing Benefits," 17 May.
6. The survey "*Privacy Online: A Report on the Information Practices and Policies of Commercial Web sites"* released in March of 2002 by the Progress and Freedom Foundation studied over 5 500 Web sites and 100 of the busiest sites.
7. Work conducted by the WPISP in close co-operation with the OECD Committee on Consumer Policy (CCP).
8. See Chapter 8.
9. See Chapter 9.
10. See Chapter 10.
11. See. "Alternative Dispute Resolutions Providers: A Global Inventory", July 2002, www.iccwbo.org/home/news_archives/2002/stories/adr.asp.
12. See Chapter 11.
13. Draft prepared by a consultant to the OECD, Chris Kuner, a partner in the law firm Hunton & Williams.
14. See US Department of Commerce Workshop (September 2000), www.ntia.doc.gov/ntiahome/privacy/.
15. Draft prepared by a consultant to the OECD, Lauren Hall, Director, Technology Policy, Advanced Strategy and Policies, Microsoft Corporation, former Executive Vice President of the Software & Information Industry Association.
16. See Chapter 12.
17. See Chapter 13.
18. Drafts prepared by two consultants to the OECD: Laurent Bernat, Head Information and Strategy, Projetweb, and Perri 6, Director, The Policy Programme, Institute for Applied Health and Social Policy, King's College, London
19. The wider privacy package includes among others, development and notification of privacy policies and an increasing availability of online redress mechanisms – in addition to privacy-enhancing technologies.

20. A first draft was prepared by a consultant to the OECD, Elizabeth Longworth, Sector Director for Information and Communication Technologies, Industry New Zealand, former partner in Longworth Associates.

21. See Chapter 14.

22. See the European Commission model contracts for data transfer both for controller to controller transfers [Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, (2001) OJ L181/19) and for controller to processor transfers (Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC, (2002) OJ L6/52)].

See the final version of the ICC clauses was submitted to the European Commission on 9 August 2002, www.iccwbo.org/home/electronic_commerce/word_documents/Final%20version%20July%202002%20Model %20contract%20clauses.pdf.

See the Council of Europe/European Commission/ICC, Model contract to Ensure Equivalent Data Protection in the Context of Transborder Data Flows of November 2, 1992, with Explanatory Memorandum.

Part II

POLICY AND PRACTICAL GUIDANCE FOR IMPLEMENTING PRIVACY PROTECTION ONLINE

Chapter 3

POLICY AND PRACTICAL GUIDANCE FOR IMPLEMENTING PRIVACY PROTECTION ONLINE

OECD member countries share a strong commitment, reaffirmed by OECD ministers in 1998, "to the protection of privacy on global networks in order to ensure the respect of important rights, build confidence on global networks, and to prevent unnecessary restrictions on transborder flows of personal data".

The policy and practical guidance offered in this chapter reflects the high-level 1998 Ministerial objective to build bridges between the different approaches adopted by member countries. It builds upon the work presented in Part I.

Chapter 3

POLICY AND PRACTICAL GUIDANCE FOR IMPLEMENTING PRIVACY PROTECTION ONLINE

Blending approaches

Although many systems are hybrid approaches combining self-regulation and legislative actions, privacy protection has traditionally been approached as if there were primarily two approaches: government regulatory and legislative actions and market-based self-regulatory efforts. Early in 1998,[1] OECD member countries agreed that each of these approaches had advantages and disadvantages. Government efforts seemed to offer predictable, enforceable legal protections and redress mechanisms, and self-regulatory efforts appeared to enable organisations in different sectors to tailor detailed guidelines to work within specific circumstances. In both approaches, difficulties in adequately addressing privacy online were foreseen, particularly with respect to cross-border issues. The debate moved then to discuss what mix of instruments and techniques would be best tailored to the protection of privacy in the global online environment.

Indeed, work by the OECD, as mentioned above, suggests that the most effective privacy protection online is likely to be delivered through a mix of regulatory and self-regulatory approaches blending legal, technical and educational solutions that suit the legal, cultural and societal context in which they operate. All instruments, mechanisms, procedures and technologies have the potential to reinforce each other's efficiency and their blending holds the promise to provide effective solutions that can go beyond the objective of building bridges, to the actual integration of different elements into viable solutions. Statutory systems can be more effective with recourse to the wide range of self-regulatory measures to implement and enforce law online. Self-regulation can also be more effective with appropriate legislation and effective government enforcement back-up. That would also ensure the efficient operation of markets providing privacy protection. In all cases, enforceability is crucial as compliance with either system is not automatic.

OECD work also demonstrates that a committed and complementary involvement of all participants is key to the successful implementation of a mixture of privacy measures because the online environment challenges the implementation of traditional national policies. All participants have a role to play to help ensure the respect of privacy on global networks.

Strengthening co-operation

Considering the work already achieved and what still needs to be done to help ensure effective privacy protection both at the national and global levels, it is important that OECD member countries continue to co-operate among themselves and with the other participants, and intensify efforts to promote effective privacy protection online. In this respect, appropriate joint public and private sector actions may provide effective incentives in areas where technological and legal tools are closely interrelated. More generally, further consistent efforts aimed at online privacy protection within a compatible global policy framework should both increase individual user confidence in electronic commerce and more generally the online environment, and benefit business and other organisations indirectly by the increase in individual user and consumer confidence.

Therefore, member countries, businesses and other organisations, as well as individual users and consumers are recommended to give effect to, and disseminate the following policy and practical guidance, and non member countries are also invited to take account of it.

PRACTICAL GUIDANCE ON POLICY FOR OECD MEMBER COUNTRIES

At the national level

OECD member countries are encouraged to continue to effectively promote privacy protection online and to facilitate communication and co-operation with business, industry, user and consumer representatives to establish measures and practices to reflect the policy and practical guidance below. In particular, member countries should take further steps to help ensure:

1) The adoption of privacy policies through:

Encouraging organisations with a presence online to:

- Systematically conduct an extensive review of their privacy practices and to develop a privacy policy that would give effect to the OECD privacy principles.
- Review laws or self-regulatory schemes which may apply to their collection and use of personal data, review their practices against such regulation, and amend them where necessary to better ensure compliance.
- Reassess on a regular basis their privacy practices and policy.
- Use the OECD Privacy Policy Statement Generator.[2]

Continuing to promote the valuable use of the OECD Privacy Policy Statement Generator as an educational and facilitating tool by:

- Taking initiatives to create hyperlinks from national Web sites to the OECD Web site.
- Translating the Generator into their language.
- Using the source code[3] to implement the Generator in their language and/or to enhance it by adding a section on additional national privacy requirements.

2) The online notification of privacy policies to users through:

Encouraging organisations with a presence online to:

- Post their privacy policy online in a prominent place.
- Conduct regular audits of the accuracy and legal compliance of those policies.

3) The availability of enforcement and redress mechanisms in cases of non-compliance with privacy principles and policies through:

Encouraging the development and use of fair and effective online alternative dispute resolution mechanisms to help resolve privacy and consumer related disputes by:

- Fostering the design and offering of flexible and informal online alternative dispute resolution mechanisms that would take into account the global nature of electronic

commerce (*e.g.* functioning in multiple languages), and be able to cope with transborder disputes.

- Striving to reduce national differences in existing legal frameworks that may affect the operability of alternative dispute resolution mechanisms in the cross-border context.
- Further providing advice to individual users on how to file complaints and obtain redress for breaches of their privacy in relation to online interactions, and raising awareness of what kinds of alternative dispute resolution programmes are offered in different countries and what rules they operate under.

Actively fostering compliance with privacy principles and policies by:

- Raising organisations' awareness of the benefits of developing effective internal practices and procedures to enhance individual user trust, such as designating internal privacy officers, as well as of engaging in voluntary self-assessment of privacy practices, third-party assessment and/or trustmark programmes.

Promoting effective global solutions with regard to privacy compliance and enforcement by:

- Fostering the adoption of self-regulatory mechanisms, such as codes of conduct or trustmark programmes, able to operate on a transborder basis, consistent with the OECD Privacy Guidelines.
- Fostering the appointment of organisations' internal privacy officers by providing a legal basis for them and/or granting organisations legal incentives for their use.
- Further providing online resources for handling complaints.
- Strengthening enforcement against organisations misrepresenting compliance with privacy policies and other privacy promises to individual users.

4) The promotion of user education and awareness about online privacy and the means of protecting privacy through:

- Fostering effective education and information for organisations and individual users about online privacy protection issues and solutions, including privacy-enhancing technologies.
- Further providing online resources for raising awareness about privacy regulations and best practices.
- Raising awareness among individual users for them to better understand the technology and the privacy implications of transactions and interactions on the internet.
- Supporting academic work to analyse in more detail how to efficiently persuade organisations and individual users to use an effective complementary mix of online privacy protection solutions.

5) The use of privacy enhancing technologies and the development of privacy functions in other technologies, as appropriate through:

- Actively encouraging developers of systems and software applications to incorporate privacy into the design of information technologies.
- Actively encouraging organisations to consider at an early stage the privacy implications of their technologies and services.

Providing incentives, such as appropriate joint action with the private sector, for the further development of a sustainable market for privacy-enhancing technologies designed for individual users as well as for organisations, and encouraging a wider use of such tools.

More generally, educating and raising awareness about technical solutions and encouraging organisations to provide such user-friendly and transparent technologies to individual users – and likewise, encouraging users to utilise these technologies and to seek information and education about online privacy protection options.

At the global level

OECD member countries should reaffirm their intention to co-operate among themselves and with the other participants to implement the OECD Privacy Guidelines online in the public and private sectors. As stated by OECD Ministers in their 1998 Declaration, member countries should also consider reassessing periodically the need for any other further action to ensure the protection of personal data at the global level.

In particular, member countries should, in the context of the global online environment:

- Emphasise the importance of Part Five of the 1980 Privacy Guidelines[4] related to International Co-operation, and endeavour to establish procedures to improve bilateral and multilateral mechanisms for cross-border co-operation between public enforcement agencies in the procedural and investigative matters involved or called for in the Guidelines
- Continue to co-ordinate with the private sector and, explore how recourse to public/private partnerships could help building organisations and individual user trust online in areas where technology and regulation are closely interrelated such as online dispute resolution and privacy-enhancing-technologies.
- Promote co-operation with other international organisations as appropriate.
- Continue to explore ways to further online trust across all participants through appropriate outreach, education, co-operation and consultation.

PRACTICAL GUIDANCE FOR BUSINESSES AND OTHER ORGANISATIONS

Businesses and other organisations need not wait for encouragement by governments at the national or international levels to continue to promote and expand privacy protection online. In many cases, they can implement the above-mentioned policy and practical guidance from their own initiative. In particular, they can:

- Develop privacy policies based on the OECD Guidelines, use the OECD Privacy Policy Statement Generator and similar mechanisms as useful tools to assist in developing policies, and post their privacy policies on their home page.
- Evaluate whether the following self-regulatory tools are appropriate to their activities and where so, implement and adhere to them: trustmark programmes; codes of conduct; labelling systems; privacy icons or symbols; auditing whether by self-assessment or by a third-party; and effective redress mechanisms, including alternative dispute resolution.
- Work with government to develop innovative and flexible implementation models for existing or emerging regulatory and self-regulatory models to help assure that the legitimate

needs for information flows are considered as well as the legitimate needs for protection of personal data.

PRACTICAL GUIDANCE FOR INDIVIDUAL USERS AND CONSUMERS

Individual users and consumers can act directly or through representative groups to protect their interests by:

- Advocating businesses' and other organisations' use of effective privacy practices, clear privacy policies, privacy-enhancing technologies, as they determine that they would be useful to them as users.
- More generally seeking transparency and education; and
- Enforcing their legal rights at national law, including, where available, their rights of access and rights to a remedy where a breach has occurred.

Users should be encouraged, through proper education, to take individual responsibility for protecting their personal data, either by taking measures for self protection (such as the use of privacy-enhancing technologies, careful reading of privacy policies and availing of opt-out measures as available) or measures to resolve disputes and obtain compensation (such as utilising alternative dispute resolution systems and filing complaints with enforcement agencies).

NOTES

1. OECD Workshop on Privacy Protection in a Global Networked Society (February 1998). See www.oecd.org/ EN/documents/0,,EN-documents-43-1-no-4-no-43,00.html.

2. See Chapter 7 and http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm.

3. The OECD is making the source codes of the Generator available to OECD member countries so that they can integrate it into their national sites – and add data to it which are specific to their country. The source code can be distributed to any organisations of OECD member countries carrying out public functions for their own use. However, the source codes may not be distributed to private companies pursuing a commercial activity or a for profit activity.

4. PART FIVE. INTERNATIONAL CO-OPERATION

   "20. Member countries should, where requested, make known to other member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other member countries which comply with these Guidelines.

   21. Member countries should establish procedures to facilitate:

   - information exchange related to these Guidelines, and

   - mutual assistance in the procedural and investigative matters involved.

   22. Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data."

Part III

REFERENCE DOCUMENTS

Chapter 4

GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were adopted as a Recommendation of the OECD Council in support of the three principles that bind OECD member countries: pluralistic democracy, respect for human rights and open market economies. They came into effect on 23 September 1980.

Chapter 4

GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

(23 September 1980)

THE COUNCIL,

Having regard to articles 1(c), 3(a) and 5(b) of the Convention on the Organisation for Economic Co-operation and Development of 14th December, 1960;

RECOGNISING:

that, although national laws and policies may differ, member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;

that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices;

that transborder flows of personal data contribute to economic and social development;

that domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows;

Determined to advance the free flow of information between member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among member countries;

RECOMMENDS:

1. 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 contained in the Annex to this Recommendation which is an integral part thereof;

2. That member countries endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data;

3. That member countries co-operate in the implementation of the Guidelines set forth in the Annex;

4. That member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines.

Annex to the Recommendation of the Council of 23rd September 1980

GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

PART ONE. GENERAL

Definitions

1. For the purposes of these Guidelines:

   a) "data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;

   b) "personal data" means any information relating to an identified or identifiable individual (data subject);

   c) "transborder flows of personal data" means movements of personal data across national borders.

Scope of Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.

3. These Guidelines should not be interpreted as preventing:

   a) the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;

   b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or

   c) the application of the Guidelines only to automatic processing of personal data.

4. Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("*ordre public*"), should be:

   a) as few as possible, and
   b) made known to the public.

5. In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.

6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle

7. 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.

Data Quality Principle

8. 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.

Purpose Specification Principle

9. 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.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or
b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. 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.

Individual Participation Principle

13. 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

i) within a reasonable time;
ii) at a charge, if any, that is not excessive;
iii) in a reasonable manner; and
iv) 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.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

PART THREE. BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS

15. Member countries should take into consideration the implications for other member countries of domestic processing and re-export of personal data.

16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a member country, are uninterrupted and secure.

17. A member country should refrain from restricting transborder flows of personal data between itself and another member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A member country may also impose restrictions in respect of 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.

18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

PART FOUR. NATIONAL IMPLEMENTATION

19. In implementing domestically the principles set forth in Parts Two and Three, member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to:

a) adopt appropriate domestic legislation;
b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;
c) provide for reasonable means for individuals to exercise their rights;
d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and
e) ensure that there is no unfair discrimination against data subjects.

PART FIVE. INTERNATIONAL CO-OPERATION

20. Member countries should, where requested, make known to other member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other member countries which comply with these Guidelines.

21. Member countries should establish procedures to facilitate:

i) information exchange related to these Guidelines, and
ii) mutual assistance in the procedural and investigative matters involved.

22. Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.

Chapter 5

MINISTERIAL DECLARATION ON THE PROTECTION OF PRIVACY ON GLOBAL NETWORKS

The Declaration on the Protection of Privacy on Global Networks was adopted by Ministers at the Ottawa Ministerial Conference held on 7-9 October 1998. At its 934th session, on 19 October 1998, the Council adopted a Resolution integrating this Declaration into the instruments of the Organisation.

Chapter 5

MINISTERIAL DECLARATION ON THE PROTECTION OF PRIVACY ON GLOBAL NETWORKS

The governments of OECD member countries*:

Considering that the development and diffusion of digital computer and network technologies on a global scale offer social and economic benefits by encouraging information exchange, increasing consumer choice, and fostering market expansion and product innovation;

Considering that global network technologies facilitate the expansion of electronic commerce, and accelerate the growth of transborder electronic communications and transactions among governments, businesses, and users and consumers;

Considering that personal data should be collected and handled with due respect for privacy;

Considering that digital computer and network technologies enhance traditional methods for processing personal data, increase the ability to collect, gather and link large quantities of data, and to produce augmented information and consumer profiles;

Considering that digital computer and network technologies can also be used to educate users and consumers about online privacy issues and to assist them to maintain their anonymity in appropriate circumstances or to exercise choice with respect to the uses made of personal data;

Considering that in order to increase confidence in global networks, users and consumers need assurances about the fair collection and handling of their personal data, including data about their online activities and transactions;

Considering that it is necessary to ensure the effective and widespread protection of privacy by businesses which collect or handle personal data in order to increase user and consumer confidence in global networks;

Considering that transparent rules and regulations governing the protection of privacy and personal data and their effective implementation on information networks are key elements to increasing confidence in global networks;

Considering that different effective approaches to privacy protection developed by member countries, including the adoption and implementation of laws or industry self-regulation, can work together to achieve effective privacy protection on global networks;

Considering the need for global co-operation and the necessity of industry and business taking a key role, in co-operation with consumers and governments, to provide effective implementation of privacy principles on global networks;

---

* Including the European Communities.

Considering that the technology-neutral principles of the 1980 OECD Privacy Guidelines continue to represent international consensus and guidance concerning the collection and handling of personal data in any medium, and provide a foundation for privacy protection on global networks;

REAFFIRM the objectives set forth in:

The Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, adopted by the Council of the OECD on 23rd September 1980 (OECD Privacy Guidelines);

The Declaration on Transborder Data Flows, adopted by the Governments of OECD member countries on 11th April 1985; and

The Recommendation concerning Guidelines for Cryptography Policy, adopted by the Council of the OECD on 27th March 1997.

DECLARE THAT:

They will reaffirm their commitment to the protection of privacy on global networks in order to ensure the respect of important rights, build confidence in global networks, and to prevent unnecessary restrictions on transborder flows of personal data;

They will work to build bridges between the different approaches adopted by member countries to ensure privacy protection on global networks based on the OECD Guidelines;

They will take the necessary steps, within the framework of their respective laws and practices, to ensure that the OECD Privacy Guidelines are effectively implemented in relation to global networks, and in particular:

encourage the adoption of privacy policies, whether implemented by legal, self-regulatory, administrative or technological means;

encourage the online notification of privacy policies to users;

ensure that effective enforcement mechanisms are available both to address non-compliance with privacy principles and policies and to ensure access to redress;

promote user education and awareness about online privacy issues and the means at their disposal for protecting privacy on global networks;

encourage the use of privacy-enhancing technologies; and

encourage the use of contractual solutions and the development of model contractual solutions for online transborder data flows;

They agree to review progress made in furtherance of the objectives of this Declaration within a period of two years, and to assess the need for further action to ensure the protection of personal data on global networks in pursuit of these objectives.

FURTHER DECLARE THAT THE OECD SHOULD:

Support member countries in exchanging information about effective methods to protect privacy on global networks, and to report on their efforts and experience in achieving the objectives of this Declaration;

Examine specific issues raised by the implementation of the OECD Privacy Guidelines in relation to global networks and, after collection and distribution of examples of experiences on implementation of the Guidelines, provide practical guidance to member countries on the implementation of the Guidelines in online environments, taking into account the different approaches to privacy protection adopted by member countries and drawing on the experiences of member countries and the private sector;

Co-operate with industry and business as they work to provide privacy protection on global networks, as well as with relevant regional and international organisations;

Periodically review the main developments and issues in the field of privacy protection with respect to the objectives of this Declaration;

Take into account, *inter alia*, in its future work, the issues and suggested activities discussed in the Background Report accompanying this Declaration.

INVITE:

Non-member countries to take account of this Declaration;

Relevant international organisations to take this Declaration into consideration as they develop or revise international conventions, guidelines, codes of practice, model contractual clauses, technologies and interoperable platforms for protection of privacy on global networks;

Industry and business to take account of the objectives of this Declaration and to work with governments to further them by implementing programmes for the protection of privacy on global networks.

Chapter 6

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

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

Chapter 6

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

Background

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

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

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

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

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

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

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

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

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

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

Introduction

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

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

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

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

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

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

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

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

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

I. Legal and self-regulatory instruments

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

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

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

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

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

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

A. International and regional instruments and organisations

1. Intergovernmental legal instruments

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

Status

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

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

Scope

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

Basic principles

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

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

Provisions on data flows

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

Provisions on further co-operation

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

Provisions on implementation and enforcement

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

Ongoing work

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

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

Status

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

Scope

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

Basic principles

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

Provisions on data flows

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

Provisions on further co-operation

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

Provisions on implementation and enforcement

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

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

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

Ongoing work

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

Table 6.1. **National instruments**

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

* Denotes membership of the European Union.

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

Status

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

Scope

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

Basic principles

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

Provisions on transborder data flows

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

Provisions on implementation and enforcement

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

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

Ongoing work

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

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

Status

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

Scope

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

Basic principles

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

Provisions on transborder data flows

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

Provisions on implementation and enforcement

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

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

Provisions on further co-operation

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

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

Ongoing work

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

Other developments

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

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

(e) General Agreement on Trade in Services

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

2. International conferences and discussion forums concerning privacy protection

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

(a) Annual international conferences of data protection commissioners

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

(b) Conferences of the EU data protection commissioners

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

(c) International Working Group on Data Protection in Telecommunications

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

(d) International Organization for Standardization

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

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

(e) International Chamber of Commerce

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

(f) International Federation of Direct Marketing Associations

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

(g) Electronic Commerce Europe

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

(h) Online initiatives for privacy information exchange

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

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

B. National instruments

AUSTRALIA

Laws

Commonwealth / federal laws

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

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

Other federal laws with privacy provisions

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

State and territory laws

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

Self-regulatory instruments

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

AUSTRIA

Laws

Federal comprehensive laws

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

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

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

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

Other federal laws with privacy provisions

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

Implementation of the EU Directive

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

Laender (state) laws

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

Self-regulatory instruments

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

BELGIUM

Constitution

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

Laws

Comprehensive laws

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

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

Other laws with privacy provisions

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

Implementation of the EU Directive

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

Self-regulatory instruments

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

CANADA

Laws

Federal laws

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

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

Federal approach to privacy in the private sector

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

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

Provincial laws

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

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

Self-regulatory instruments

The CSA model code

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

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

Other initiatives

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

Instruments relating to online privacy

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

CZECH REPUBLIC

Laws

Comprehensive laws

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

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

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

Other laws with privacy provisions

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

DENMARK

Constitution

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

Laws

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

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

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

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

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

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

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

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

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

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

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

Implementation of the EU Directive

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

Self-regulatory instruments

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

Other self regulatory initiatives include:

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

FINLAND

Constitution

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

Laws

Comprehensive laws

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

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

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

Other laws with privacy provisions

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

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

Implementation of the EU Directive

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

Self-regulatory instruments

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

FRANCE

Laws

Comprehensive laws

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

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

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

Other laws with privacy provisions

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

Implementation of the EU Directive

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

Self-regulatory instruments

Instruments relating to online privacy

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

Other initiatives

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

GERMANY

Laws

Federal comprehensive laws

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

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

Other federal laws with privacy provisions

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

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

Laender (state) laws

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

Implementation of the EU Directive

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

Self-regulatory instruments

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

GREECE

Constitution

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

Laws

Comprehensive laws

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

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

Other laws with privacy provisions

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

Self-regulatory instruments

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

HUNGARY

Constitution

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

Laws

Comprehensive laws

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

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

Other laws with privacy provisions

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

Self-regulatory instruments

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

ICELAND

Laws

Comprehensive laws

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

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

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

IRELAND

Constitution

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

Laws

Comprehensive laws

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

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

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

Other laws with privacy provisions

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

Implementation of the EU Directive

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

Self-regulatory instruments

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

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

ITALY

Laws

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

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

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

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

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

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

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

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

Self-regulatory instruments

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

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

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

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

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

JAPAN

Laws

Public sector laws

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

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

Approach to privacy regulation in the private sector

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

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

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

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

Local authority laws

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

Self-regulatory instruments

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

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

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

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

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

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

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

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

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

KOREA

Constitution

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

Laws

Public sector laws

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

Other laws with privacy provisions

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

Approach to privacy in the private sector

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

Self-regulatory instruments

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

LUXEMBOURG

Laws

Comprehensive laws

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

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

Other laws with privacy provisions

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

Implementation of the EU Directive

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

MEXICO

Constitution

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

Laws

Federal laws

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

THE NETHERLANDS

Constitution

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

Laws

Comprehensive laws

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

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

Other laws with privacy provisions

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

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

Implementation of the EU Directive

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

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

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

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

Self-regulatory instruments

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

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

NEW ZEALAND

Laws

Comprehensive laws

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

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

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

Other laws with privacy provisions

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

Self-regulatory instruments

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

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

NORWAY

Laws

Comprehensive laws

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

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

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

Other laws with privacy provisions

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

Other instruments to protect personal data

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

Implementation of the EU Directive

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

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

POLAND

Constitution

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

Laws

Comprehensive laws

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

Other laws with privacy provisions

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

PORTUGAL

Constitution

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

Laws

Comprehensive laws

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

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

Other laws with privacy provisions

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

Implementation of the EU Directive

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

SLOVAK REPUBLIC

Laws

Comprehensive laws

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

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

SPAIN

Constitution

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

Laws

Comprehensive laws

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

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

Other laws with privacy provisions

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

Implementation of the EU Directive

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

Self-regulatory instruments

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

SWEDEN

Constitution

The Swedish Constitution (The Freedom of the Press Act[144]) guarantees the right of individuals to have access to documents and data held by public authorities. Furthermore, the Instrument of Government[145] provides that citizens shall be protected to the extent determined in detail by law against any infringement of their personal integrity resulting from the registration of information about them by means of electronic data processing.

Laws

Comprehensive laws

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

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

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

Other laws with privacy provisions

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

Self-regulatory instruments

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

SWITZERLAND

Laws

Federal laws

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

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

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

Other federal laws with privacy provisions

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

Cantonal (state) law

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

Self-regulatory instruments

Instruments relating to online privacy

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

Other initiatives

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

TURKEY

Laws

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

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

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

UNITED KINGDOM

Laws

Comprehensive laws

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

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

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

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

Other laws with privacy provisions

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

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

Implementation of the EU Directive

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

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

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

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

Self-regulatory instruments

Instruments relating to online privacy

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

Other initiatives

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

UNITED STATES

Constitution

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

Laws

Federal sectoral laws

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

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

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

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

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

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

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

State laws

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

Approach to privacy regulation in the private sector

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

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

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

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

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

Self-regulatory instruments

Instruments relating to online privacy

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

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

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

Seal programs

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

Other initiatives

Other self-regulatory initiatives include:

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

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

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

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

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

A. Minimising the disclosure and collection of personal data

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

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

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

(a) Management of cookies

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

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

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

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

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

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

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

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

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

2. Reducing or avoiding the need for personal data disclosure

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

(a) Anonymous payment systems

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

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

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

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

(b) Digital certificates

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

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

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

(c) Anonymous profiles

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

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

B. Informing users about online privacy policies

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

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

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

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

1. Posted privacy policies

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

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

2. Terms and conditions

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

3. Digital labels

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

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

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

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

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

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

1. Optional data fields and click-box choices

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

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

2. Online negotiation of privacy standards through digital labels

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

3. "Opting-out"

Controlling the use of personal data after collection

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

Preventing the receipt of unsolicited e-mail advertising

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

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

Opting-out of anonymous profiling

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

D. Providing access to personal data

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

E. Protecting privacy through transborder data flow contracts

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

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

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

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

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

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

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

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

The revised ICC model contract

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

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

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

F. Enforcing privacy principles

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

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

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

1. Ensuring compliance with privacy standards

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

(a) Internal data protection officers

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

(b) Third party compliance reviews and Web site certification

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

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

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

TRUSTe

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

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

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

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

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

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

Standards authorities

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

Accounting firms

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

(c) Membership-based industry bodies

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

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

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

(d) Central oversight authorities

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

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

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

2. Complaint resolution procedures for breaches of privacy standards

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

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

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

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

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

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

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

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

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

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

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

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

Sanctions that may be assessed may include:

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

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

TRUSTe

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

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

The Australian Internet Industry Association

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

(c) Enforcement through administrative, civil and criminal proceedings

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

Administrative proceedings

Central oversight agencies

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

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

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

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

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

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

Other administrative agencies

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

Civil proceedings

Breaches of privacy legislation

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

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

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

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

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

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

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

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

Alternative dispute resolution

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

Criminal proceedings

Proceedings under privacy legislation

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

Other criminal proceedings

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

G. Educating users and the private sector

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

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

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

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

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

NOTES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

15. Article 6, Convention 108.

16. Article 12.3(a), Convention 108.

17. Article 13.2, Convention 108.

18. Article 4, Convention 108.

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

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

21. Articles 3 and 4, EU Directive.

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

23. Articles 10, 11 and 12 EU Directive.

24. Article 18-21, EU Directive.

25. Articles 14, EU Directive.

26. Articles 22-24, EU Directive.

27. Article 1(2), EU Directive.

28. Article 25(1), EU Directive.

29. Article 26, EU Directive.

30. Article 28, EU Directive.

31. Article 22-24, EU Directive.

32. See www.wto.org/.

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

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

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

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

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

38. See www.iccwbo.org.

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

40. See www.epic.org.

41. See www.cdt.org.

42. See www.privacy.org.

43. See www.privacyexchange.org.

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

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

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

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

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

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

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

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

52. See www.privacy.fgov.be.

53. Articles 37-43.

54. Document available at www.lachambre.be.

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

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

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

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

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

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

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

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

63. Act No.256/1992.

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

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

66. See www.tietosuoja.fi.

67. Sections 47-48, Personal Data Act.

68 . See www.ssml-fdma.fi.

69. Articles 226-16 to 226-24.

70. See www.cnil.fr.

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

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

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

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

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

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

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

78. Section 21(1).

79. Sections 43 and 44.

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

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

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

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

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

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

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

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

88. Articles 11-14.

89. Article 23.

90. Article 21.

91. Article 22.

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

93. Articles 11-15.

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

95. Articles 17 and 18.

96. Article 33.

97. Article 14(1).

98. Article 22.

99. Article 33.

100. Articles 37-39.

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

102. Sections 21-23.

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

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

105. The Guidelines were originally issued in April 1989.

106. Articles 22 and 23 of the Guidelines.

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

108. See www.ecom.or.jp.

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

110. 31 March 1979.

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

112. Articles 32-39.

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

114. Bill No. 4357.

115. Article 214, Federal District Penal Code.

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

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

118. Sections 97-109, Privacy Act.

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

120. Sections 46-53, Privacy Act.

121. Section 85, Privacy Act.

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

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

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

125. See www.datatilsynet.no.

126. Article 51 states:

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

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

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

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

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

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

128. Articles 50-54.

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

130. Article 8(h).

131. Articles 27, 29 and 30.

132. Articles 34-41.

133. Law 109/91 of 17 August 1991.

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

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

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

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

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

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

140. See www.ag-proteccionadatos.es.

141. Articles 43 and 44 of the Law.

142. Law No. 28/94.

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

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

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

146. Act No. 1998:204.

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

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

149. 19 June 1992.

150. See www.edsb.ch.

151. Article 11 of the FLDP.

152. Article 23 of the FLDP.

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

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

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

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

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

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

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

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

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

162. See www.ispa.org.uk.

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

164. 5 U.S.C. § 552a (1994).

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

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

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

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

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

170. See www.itic.org.

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

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

173. See www.the-dma.org

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

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

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

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

178. See www.hotmail.com.

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

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

181. See www.anonymizer.com.

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

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

184. See www.mondexusa.com.

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

186. See www.engage.com.

187. See www.doubleclick.com.

188. See www.clickstream.com.

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

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

191. See www.truste.org.

192. See www.bbbonline.org.

193. See www.privacyalliance.org.

194. See www.aeanet.org.

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

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

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

198. See www.w3.org/P3P.

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

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

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

202. See www.moniker.com.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

217. See www.truste.org.

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

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

220. See www.privacyalliance.org.

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

222. See www.bbbonline.org.

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

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

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

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

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

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

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

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

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

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

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

234. See www.coe.int.

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

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

237. See www.the-dma.org.

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

239. See www.epic.org/privacy.

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

REFERENCES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Chapter 7

OECD PRIVACY POLICY STATEMENT GENERATOR

This chapter presents the main pages of the free online Internet-based tool, the OECD Privacy Policy Statement Generator, available at http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm.

WHAT IS THE OECD PRIVACY STATEMENT GENERATOR?

WHY DEVELOP A PRIVACY POLICY AND POST A POLICY STATEMENT ON YOUR WEB SITE?

Internet research has repeatedly shown that many consumers are reluctant to engage in electronic transactions because of concerns about the privacy of their personal data. Privacy policies and accurate public statements outlining such policies are a vital step towards encouraging openness and trust in electric commerce among visitors to Web sites. They can help visitors to make informed choices about entrusting an organisation with personal data and doing business with it.

BACKGROUND TO THE OECD GENERATOR

The OECD Privacy Guidelines represent an international consensus on how best to balance effective privacy protection with the free flow of personal data. Openness is a key principle of the Guidelines, which are flexible and allow for various means of compliance.

To help implement the Guidelines in the electronic world, the OECD has developed the OECD Privacy Policy Statement Generator in co-operation with industry, privacy experts and consumer organisations. The Generator, which has been endorsed by the OECD's 30 member countries, aims to offer guidance on compliance with the Guidelines and to help organisations develop privacy policies and statements for display on their Web sites.

It is hoped that by making the Generator freely available online, it will help:

- Foster awareness of privacy issues amongst Web site owners.
- Increase awareness among visitors about privacy practices on the Web sites which they browse.
- Encourage user and consumer trust in global networks and electronic commerce.

Use of the OECD Generator does not, however, necessarily imply that a Web site complies with the OECD Privacy Guidelines.

Contents

Start Here

- Developing a Privacy Policy and Statement
- Limitations and Conditions of Use
- Start the questionnaire
- Help, including Technical Notes

Other resources

- Access the OECD Privacy Guidelines
- Access the OECD Privacy Inventory
- Access the Privacy Resource

Sponsors

- Daimler Chrysler
- Microsoft bCentral
- Microsoft Consulting Services France

WHAT IS THE OECD PRIVACY POLICY STATEMENT GENERATOR?

The Generator is first and foremost an educational tool.

It provides guidance on conducting an internal review of existing personal data practices and on developing a privacy policy statement. It gives links to private sector organisations with expertise in developing a privacy policy. It offers links to governmental agencies, non-governmental organisations and private bodies that give information on applicable regulations.

The Generator makes use of a questionnaire to learn about your personal data practices. A Help Section provides explanatory notes and practical guidance. Warning flags appear where appropriate. Your answers are then fed into a pre-formatted draft policy statement. You must assess this statement: is it an accurate reflection of your personal data practices and policy?

Note that the OECD does not guarantee that such a draft privacy policy statement meets applicable legal or self-regulatory requirements. The statement merely reflects the answers given to the Generator's questions. However, the draft statement will furnish an indication of the extent to which your privacy practices are consistent with the **OECD Privacy Guidelines**.

LIMITATIONS AND CONDITIONS OF USE OF THE OECD GENERATOR

The Generator is freely available to all private and public organisations on the OECD Web site and via links in member and other countries. If you find the Generator on the Web site of a government agency or that of a similar body, it may contain an extra section designed to help comply with that country's specific national requirements.

The OECD has developed the OECD Generator as a tool to provide users with useful input in the development of a privacy policy and statement.

Users are expected to deal fairly and in good faith with the Generator and the substance of the statements which it produces.

Use of the Generator does not, and should not, imply any seal of approval or endorsement by the OECD of the privacy policy and statement developed by users. Users may however, indicate that they have used the OECD Generator as part of the process of developing their privacy policy and statement, and if they do so, should provide a link to:
http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm

- Read Developing a Privacy Policy and Statement first.
- Start the Questionnaire

© 2000 OECD & Microsoft Corporation. All Rights Reserved

DEVELOPING A PRIVACY POLICY AND STATEMENT

HOW TO DEVELOP A PRIVACY POLICY

STEP 1. To ensure that you answer the questions contained in the Generator accurately, you need to know what your personal data practices are. Therefore, before completing the questionnaire, it is essential to carry out an **extensive internal review** of your current **personal data** practices. For example:

- Do you collect personal data?
- What kinds of personal data do you collect?
- How are they collected? From individuals, from third parties, from public bodies or authorities? Are individuals aware that their personal data are being collected?
- Who in your organisation is responsible for deciding what personal data are collected and how?
- Why do you collect personal data?
- How are they used?
- Who controls personal data once they are collected?
- Are personal data disclosed to third parties, and if so, why?
- How and where are they stored?
- Do you have standards, guidelines and regulations which apply to your collection and use of personal data?
- Do you allow visitors access to the personal data you have about them?
- What happens if a visitor has a query about their personal data? What if they are not satisfied with how you deal with their query?

Further guidance on carrying out an internal review can be found on the Web sites of SIIA, USCIB, or CSA Model Code CAN/CSA-Q830.

You may also wish to consult:

www.jipdec.or.jp/security/privacy/index-e.html
www.research.att.com/projects/p3p/propgen
www.the-dma.org
www.truste.org/wizard

STEP 2. Once you have reviewed your current personal data practices:

- You should review laws or (self) regulatory schemes which may apply to your collection and use of personal data. **Governmental agencies**, **non-governmental organisations** or **private bodies** may provide you with help in this respect.

It is recommended that you review your current practices against such regulations and amend them where necessary to ensure compliance.

USING THE GENERATOR TO CREATE A PRIVACY POLICY STATEMENT

STEP 3. Once you have determined your current personal data practices and reviewed those practices against relevant regulatory requirements, you are in a position to complete the Generator questions. The Help Section provides explanations of terms used, guidance on what is consistent with the **OECD Privacy Guidelines**, and, where appropriate, additional information on other national, regional or international instruments. It is important to read the **technical notes** before answering the questions.

After you have completed the questionnaire as accurately as possible, a draft privacy policy statement is automatically generated. It proposes pre-formatted sentences based on your answers/choices.

ASSESSING THE DRAFT PRIVACY POLICY STATEMENT

STEP 4. Next, you should make sure:

- That the draft privacy statement accurately reflects your organisation's personal data practices.
- That the draft privacy statement complies with applicable national, regional and international laws or (self) regulatory schemes.
- That errors are corrected and that the privacy statement reads smoothly.

PLACING YOUR PRIVACY POLICY STATEMENT ON YOUR WEB SITE

STEP 5. Once you are satisfied that your privacy policy statement accurately reflects your personal data practices and complies with applicable regulations, you need to consider how to make your statement publicly available. Regulations to which you may be subject may require a specific location for such a statement, such as your homepage, or at the point(s) where personal data are collected. In the absence of specific regulatory requirements, you may wish to consider creating a link between your homepage and your privacy statement, or between pages where you collect personal data and your privacy statement. The OECD Privacy Guidelines recommend that individuals should be able to gain access to information about personal data practices without unreasonable effort as to time, knowledge and expense. You may also wish to create links to relevant Web sites to make visitors aware of any relevant regulations.

REMEMBER: ***Once your privacy statement is publicly posted, you may be legally liable if you fail to abide by your privacy policy statement or if that statement does not comply with local laws.***

By following the above steps, you can help ensure that your policy statement will not misrepresent your privacy practices or fail to comply with applicable regulations.

EXAMPLE PRIVACY POLICY STATEMENT

The OECD online privacy policy statement was revised using the OECD Generator. This example is not intended to be a "model" statement. It is intended only to provide an indication of what you can expect your final privacy statement to look like.

- What is the OECD Generator?

Limitations and Conditions of Use

- Start the Questionnaire

Help for using the OECD Privacy Generator

Technical notes on using the Generator

The OECD Privacy Generator is a questionnaire that is a tool to help you to advertise your privacy policy on the Web site(s) of your organisation by generating a Web page (in HTML format). This Web page can be downloaded when you complete the Generator questionnaire and reflects the answers you provide. After appropriate modifications, the Web page can be included on your organisation's Web site(s).

The questionnaire begins by a **Login** page, permitting you to indicate which task you want to achieve:

- **Create** a new Statement, for which you will be given a **Statement ID** and asked for a **Password**.
- **Modify** an existing Statement by giving its **Statement ID** and **Password**.
- **Delete** an existing Statement by giving its **Statement ID** and **Password**.

During Statement creation or modification, you will be asked a series of questions that you should answer based on your own organisation's practices in relation to privacy. These questions are grouped into 11 sections which you can access through the **Back** and **Next** button available at the bottom of each page.

The **Next** button also saves the current page. For this reason, it is important to click the **Next** button to ensure that the contents of the current page will not be lost.

A **Help** button is provided at the beginning of each section. It provides a link to full and detailed guidance on the questions in the section. Each **Help** Section is in two parts; the first provides an explanation of the relevant OECD Principle, and the second provides further guidance through hyperlinks on specific terms in the questions. Reading the relevant **Help** section before attempting to answer the questions of a given section will ensure that you understand the question correctly and are able to answer in a way that accurately reflects your privacy practices.

The Generator keeps the answers you have given to questions in any page of the questionnaire permanently, thereby making it possible to modify or delete them later or at any time. To do so, you simply have to keep the **Statement ID** and the **Password** you gave when creating the Policy. Ensure that you only use the **Next** and **Back** buttons located at the end of each page of the Generator to navigate between questionnaire pages, as the Generator validates and stores the answers during these steps.

Note: Unless you delete it, the information you provide and the answers you give will be kept on the OECD server to allow you to return to and modify your draft statement. However, the OECD will not access or use such information and answers for any purpose.

At the end of most pages of the questionnaire a **Preview** button appears. Clicking on this button will enable you to view the draft privacy statement generated from the responses that you have given. The privacy statement will appear in a new window. After viewing the **Preview** page you should close the window to return to the questionnaire.

Note: The draft privacy statement generated by the preview function will not include the responses from the current page, unless the contents of the page have been saved by clicking the **Next** button.

At the end of the questionnaire, you will be able to download your Draft Privacy Statement produced by the Generator by clicking on the "**Download Statement**" button :

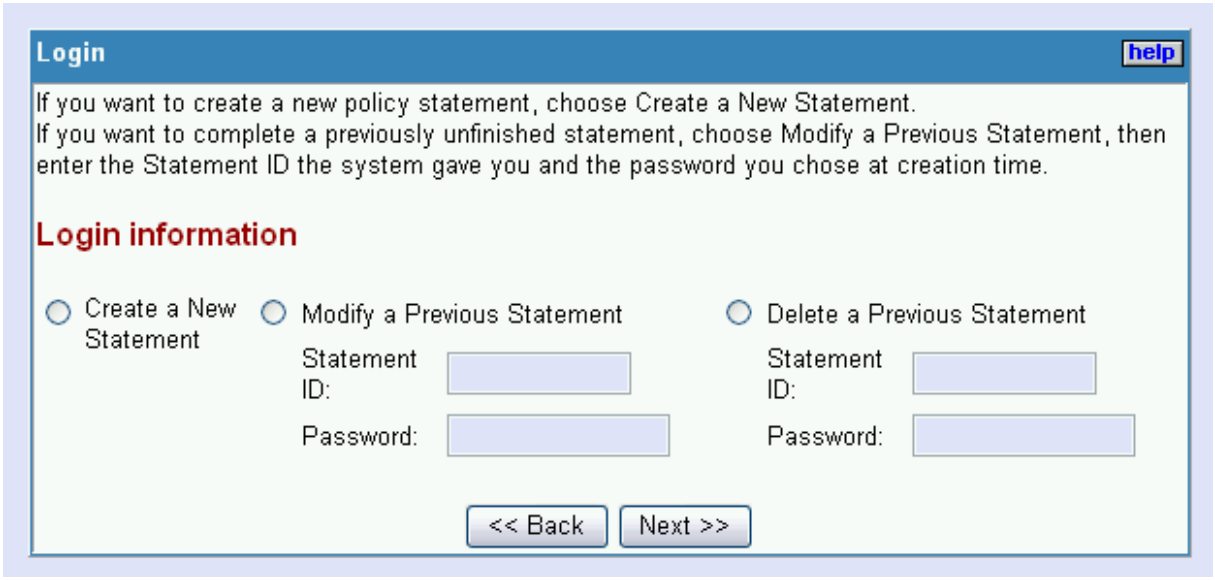
- Choose the **Save As** option in the download option windows of your browser.
- Change the name of the page as an appropriate HTML page (with **.htm** or **.html** suffix).
- Choose a location to save the Statement file.
- Click on the **OK** button.

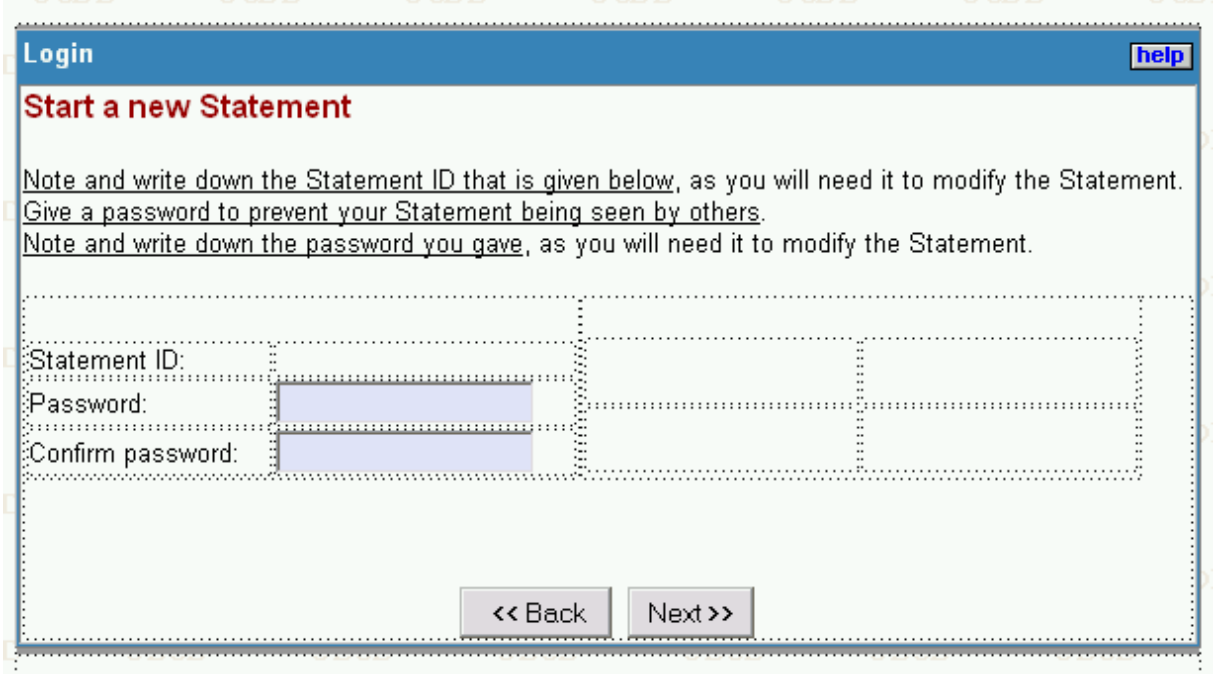
Additional notes

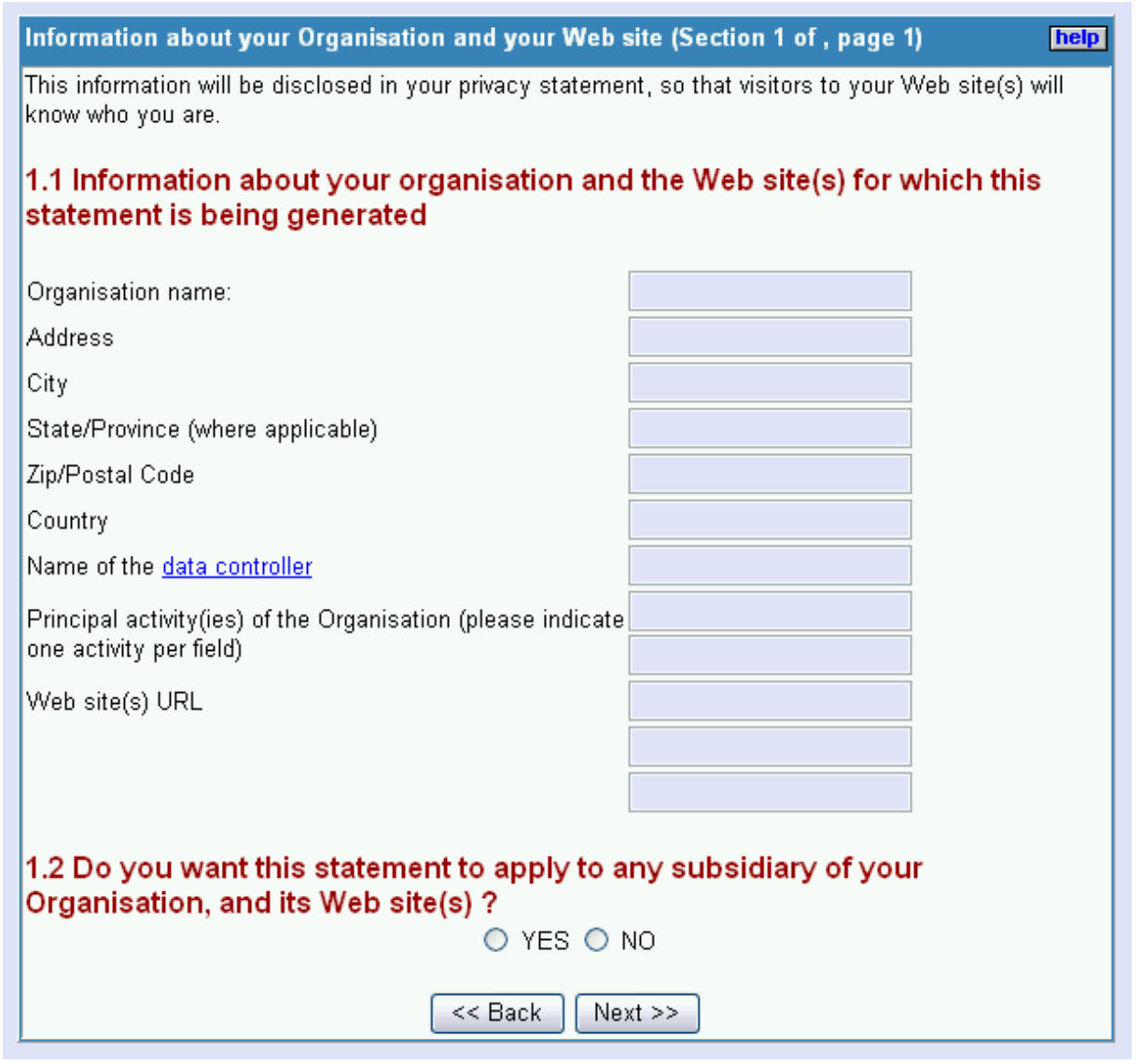
If the Generator is left inactive for a period of four hours, you will have to re-enter your login details in order to access the answers you have entered, and all unvalidated answers will be lost.

The Generator uses session (also called temporary) cookies to maintain the link between the user and the OECD server during the use of the Generator. This cookie is **not** permanently stored on your computer and is **not** used to store any information related to the user. Be sure that your Internet browser is configured to accept (at least temporary) cookies.

When creating a new Statement, the Generator asks you for a password so that other users cannot access your information. Be sure not to leave a blank password, which would allow other users to access your statements. The OECD server does not use a secure connection for the Generator. Network traffic between the user and the OECD server is not encrypted.


Login
help
If you want to create a new policy statement, choose Create a New Statement.
If you want to complete a previously unfinished statement, choose Modify a Previous Statement, then enter the Statement ID the system gave you and the password you chose at creation time.
Login information
Create a New Statement
Modify a Previous Statement
Statement ID:
Password:
Delete a Previous Statement
Statement ID:
Password:
<< Back
Next >>


Login
help
Start a new Statement
Note and write down the Statement ID that is given below, as you will need it to modify the Statement.
Give a password to prevent your Statement being seen by others.
Note and write down the password you gave, as you will need it to modify the Statement.
Statement ID:
Password:
Confirm password:
<< Back
Next >>



Information about your Organisation and your Web site (Section 1 of , page 1) help

This information will be disclosed in your privacy statement, so that visitors to your Web site(s) will know who you are.

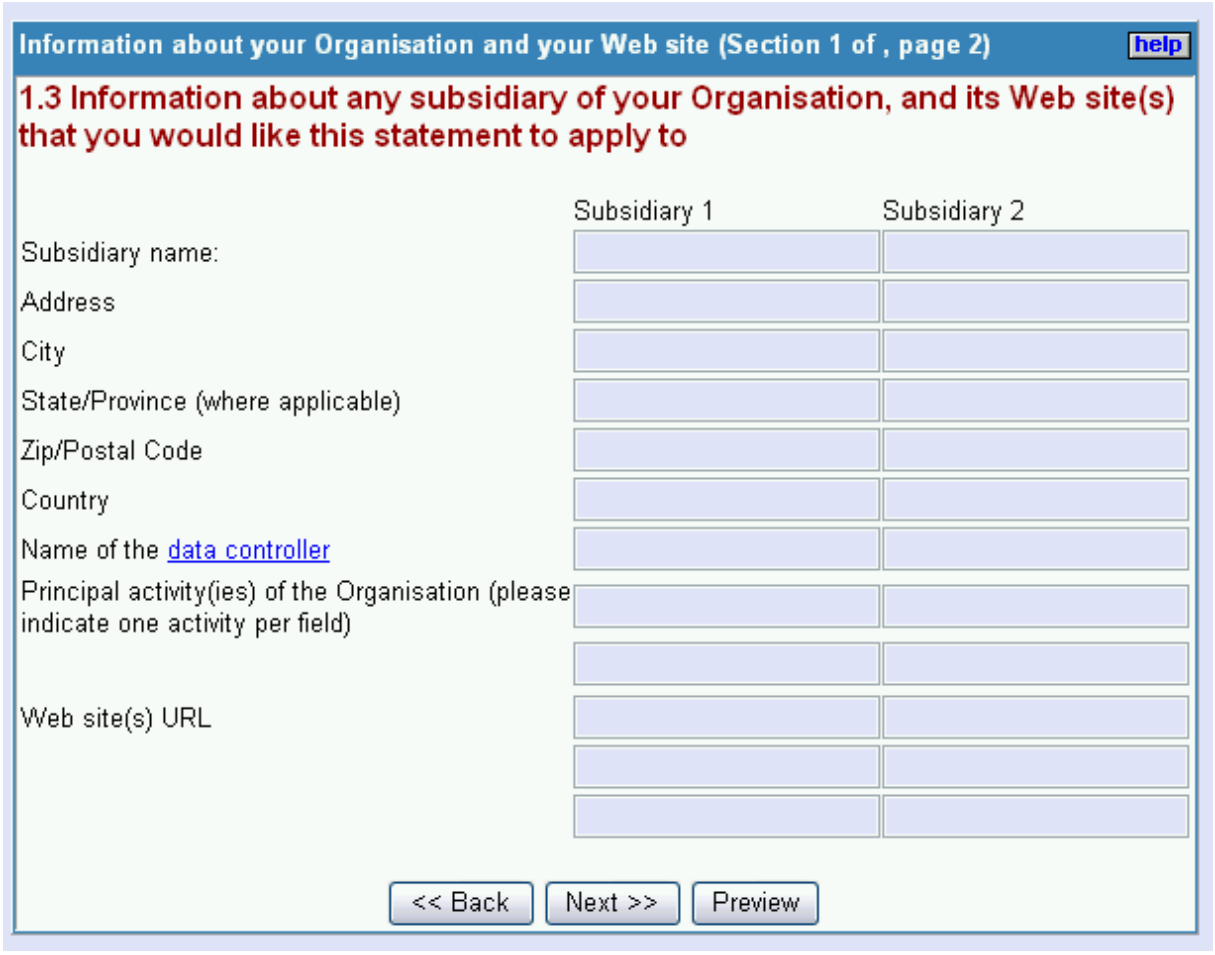
1.1 Information about your organisation and the Web site(s) for which this statement is being generated

Organisation name:	
Address	
City	
State/Province (where applicable)	
Zip/Postal Code	
Country	
Name of the data controller	
Principal activity(ies) of the Organisation (please indicate one activity per field)	
Web site(s) URL	

1.2 Do you want this statement to apply to any subsidiary of your Organisation, and its Web site(s) ?

○ YES ○ NO

<< Back Next >>

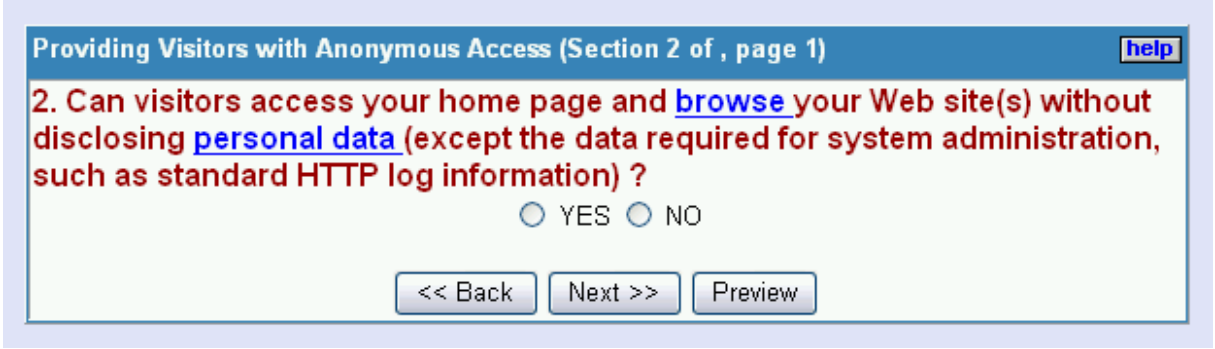


Information about your Organisation and your Web site (Section 1 of , page 2) help

1.3 Information about any subsidiary of your Organisation, and its Web site(s) that you would like this statement to apply to

	Subsidiary 1	Subsidiary 2
Subsidiary name:		
Address		
City		
State/Province (where applicable)		
Zip/Postal Code		
Country		
Name of the data controller		
Principal activity(ies) of the Organisation (please indicate one activity per field)		
Web site(s) URL		

<< Back Next >> Preview



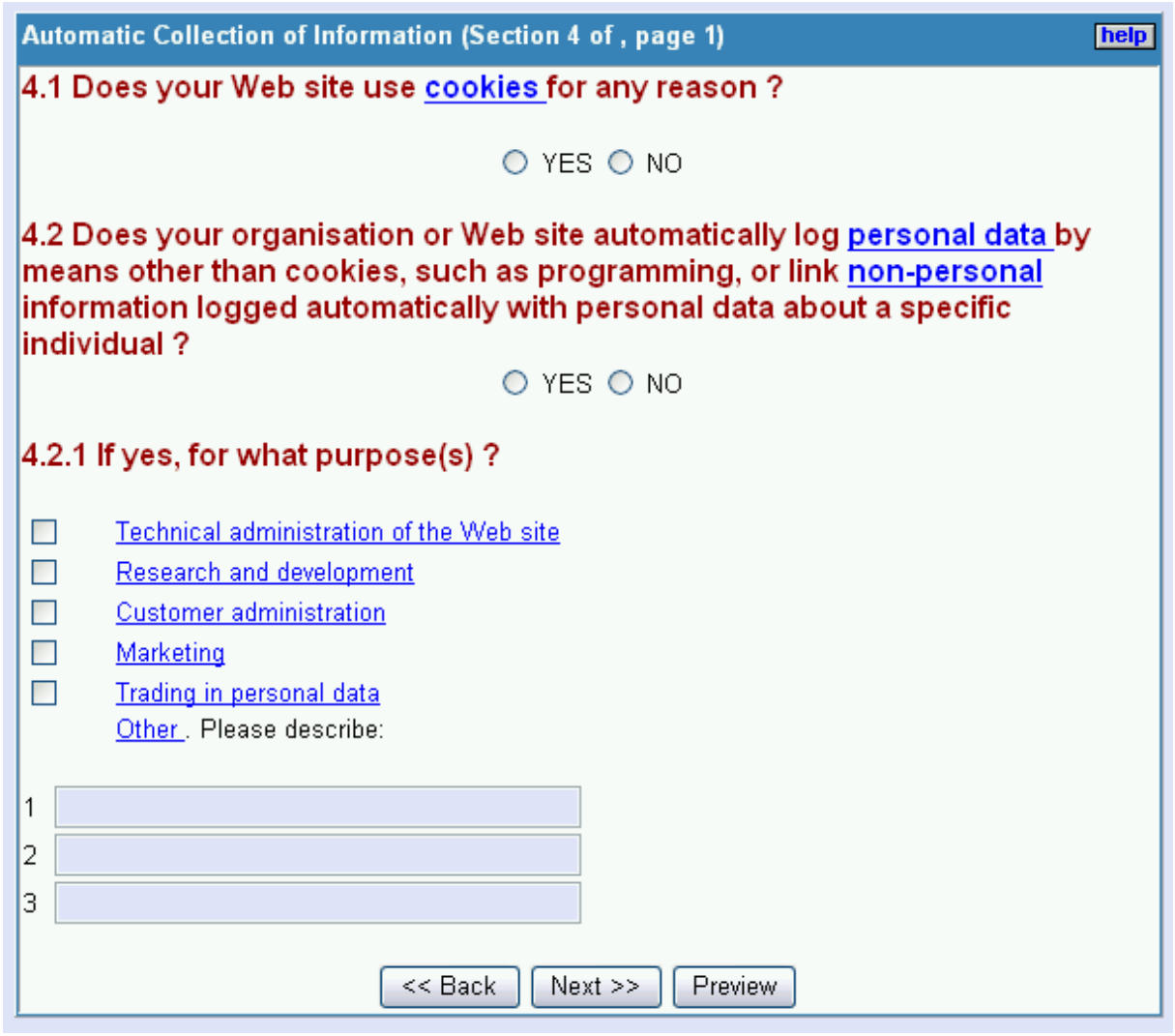
Providing Visitors with Anonymous Access (Section 2 of , page 1) help

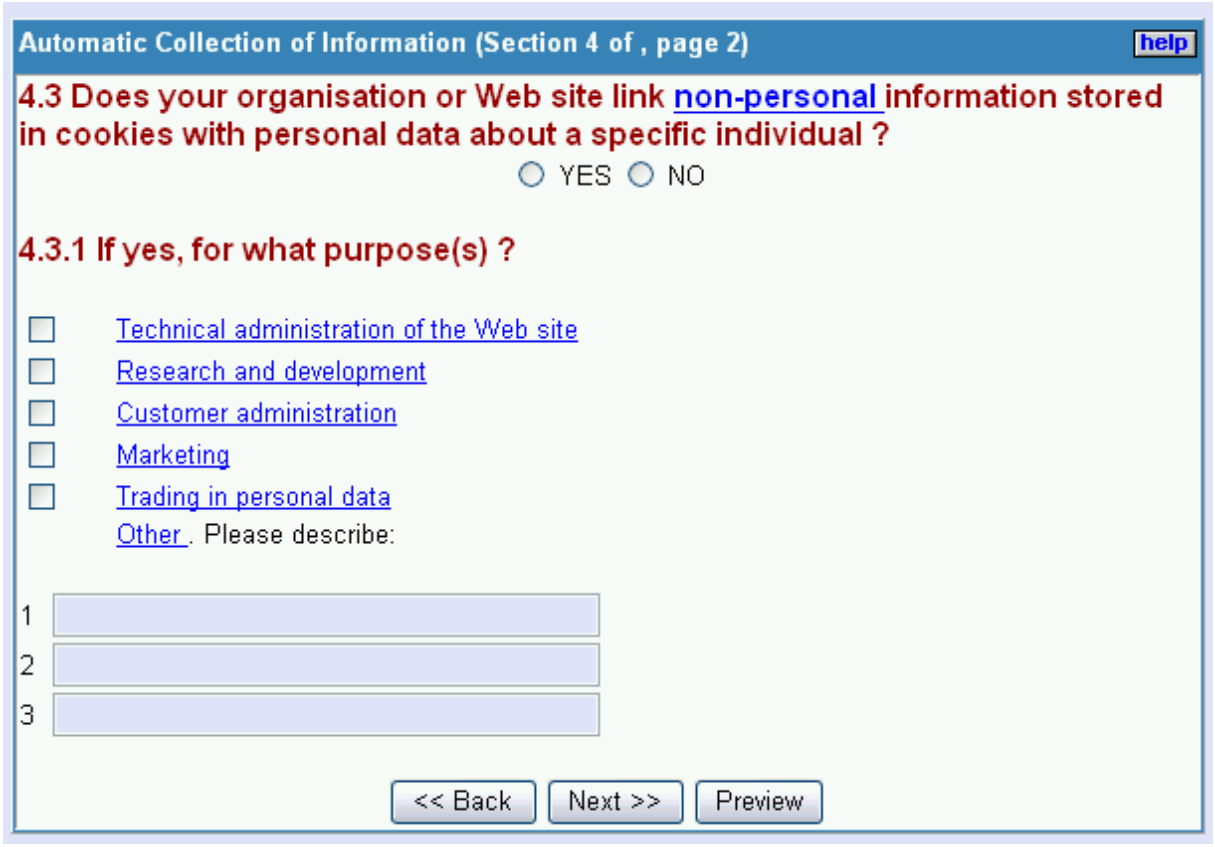
2. Can visitors access your home page and browse your Web site(s) without disclosing personal data (except the data required for system administration, such as standard HTTP log information) ?

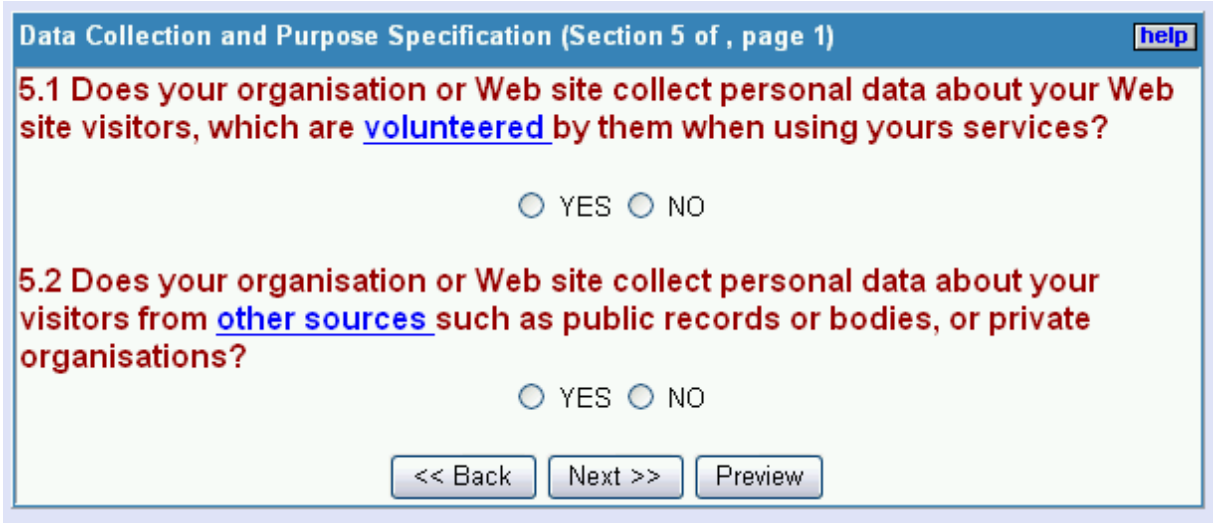
○ YES ○ NO

<< Back Next >> Preview


Linkage Characteristics of your Web Site (Section 3 of , page 1)
help
3.1 Can visitors communicate with other visitors or post data so that others may access it, via your Web site ?
YES NO
3.2 Does your Web site use a third party Web service provider (e.g. a company that collects personal data to distribute advertisements) that collects personal data about your visitors ?
YES NO
3.2.1 If yes, please specify the name of the third party:
1
2
3
<< Back
Next >>
Preview


Automatic Collection of Information (Section 4 of , page 1)
help
4.1 Does your Web site use cookies for any reason ?
YES NO
4.2 Does your organisation or Web site automatically log personal data by means other than cookies, such as programming, or link non-personal information logged automatically with personal data about a specific individual ?
YES NO
4.2.1 If yes, for what purpose(s) ?
Technical administration of the Web site
Research and development
Customer administration
Marketing
Trading in personal data
Other . Please describe:
1
2
3
<< Back
Next >>
Preview


Automatic Collection of Information (Section 4 of , page 2)
help
4.3 Does your organisation or Web site link non-personal information stored in cookies with personal data about a specific individual ?
YES NO
4.3.1 If yes, for what purpose(s) ?
Technical administration of the Web site
Research and development
Customer administration
Marketing
Trading in personal data
Other . Please describe:
1
2
3
<< Back
Next >>
Preview


Data Collection and Purpose Specification (Section 5 of , page 1)
help
5.1 Does your organisation or Web site collect personal data about your Web site visitors, which are volunteered by them when using yours services?
YES NO
5.2 Does your organisation or Web site collect personal data about your visitors from other sources such as public records or bodies, or private organisations?
YES NO
<< Back
Next >>
Preview

Data Collection and Purpose Specification (Section 5 of , page 2) help

You have indicated in question(s) 4.2, 4.3, 5.1 and/or 5.2 that you collect personal data. Please choose all that apply in the tables below.

5.3.1 Primary personal data/Business information

- ☐ volunteered by each visitor
- ☐ collected from public records or bodies
- ☐ collected from private organisations

Primary personal data	Technical administration of the Web site	Research & development	Customer Administration	Marketing	Trading in personal data
Name	☐	☐	☐	☐	☐
Gender	☐	☐	☐	☐	☐
Address	☐	☐	☐	☐	☐
E-mail address	☐	☐	☐	☐	☐
Phone/Fax number	☐	☐	☐	☐	☐
Other (describe)	☐	☐	☐	☐	☐

Business Information	Technical administration of the Web site	Research & development	Customer Administration	Marketing	Trading in personal data
Employer/organisation	☐	☐	☐	☐	☐
Job title	☐	☐	☐	☐	☐
Address	☐	☐	☐	☐	☐
E-mail address	☐	☐	☐	☐	☐
Phone/Fax number	☐	☐	☐	☐	☐
Other (describe)	☐	☐	☐	☐	☐

5.3.2 Other personal details and profiling data

- ☐ volunteered by each visitor
- ☐ collected from public records or bodies
- ☐ collected from private organisations

	Technical administration of the Web site	Research & development	Customer Administration	Marketing	Trading in personal data
Personal details	☐	☐	☐	☐	☐
Physical description	☐	☐	☐	☐	☐
Family characteristics	☐	☐	☐	☐	☐
Education and skills	☐	☐	☐	☐	☐
Life style or personal tastes	☐	☐	☐	☐	☐
Financial resources	☐	☐	☐	☐	☐
Other (describe)	☐	☐	☐	☐	☐

5.3.3 Identifiers

- ☐ volunteered by each visitor
- ☐ collected from public records or bodies
- ☐ collected from private organisations

	Technical administration of the Web site	Research & development	Customer Administration	Marketing	Trading in personal data
On-line identifiers	☐	☐	☐	☐	☐
Financial identifiers	☐	☐	☐	☐	☐
Identifiers assigned by Public bodies	☐	☐	☐	☐	☐
Biometrics identifiers	☐	☐	☐	☐	☐
Other (describe)	☐	☐	☐	☐	☐

5.3.4 Specific Data

- ☐ volunteered by each visitor
- ☐ collected from public records or bodies
- ☐ collected from private organisations

	Technical administration of the Web site	Research & development	Customer Administration	Marketing	Trading in personal data
Racial or ethnic origin	☐	☐	☐	☐	☐
Political opinions	☐	☐	☐	☐	☐
Religious or philosophical beliefs	☐	☐	☐	☐	☐
Trade union membership	☐	☐	☐	☐	☐
Health/Medical data	☐	☐	☐	☐	☐
Sex life	☐	☐	☐	☐	☐
Police/Judicial data such as civil/criminal actions brought by or against the visitor	☐	☐	☐	☐	☐
Other (describe)	☐	☐	☐	☐	☐

<< Back | Next >> | Preview

Data Collection and Purpose Specification (Section 5 of , page 3) help

5.4 Is there any other purpose for which you collect and use personal data?

○ YES ○ NO

5.4.1 If yes, please describe the other purpose(s) for which you collect and use personal data (e.g. We collect and use personal data for the additional purpose of...)?

1
2
3

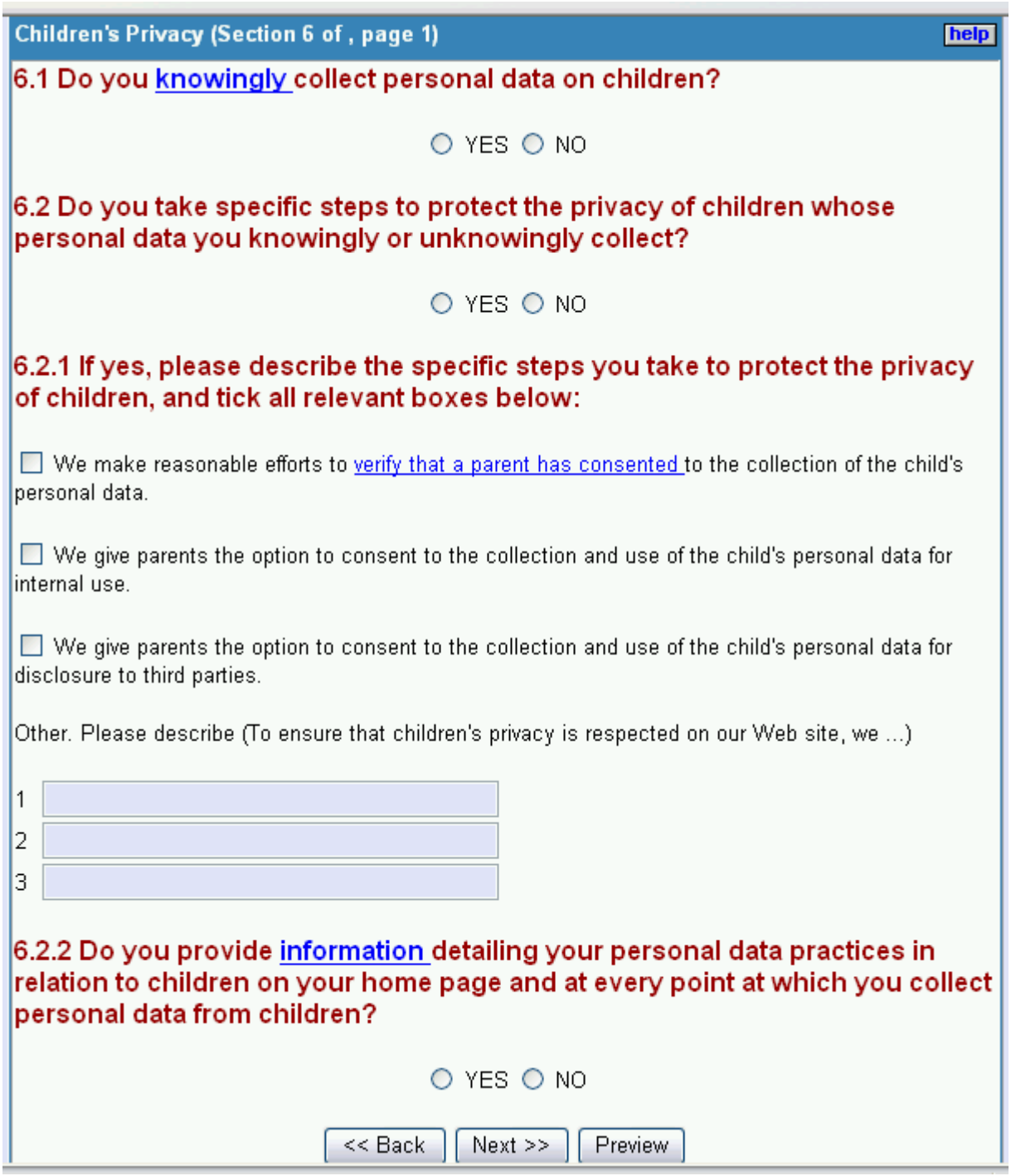
5.5 When you wish to use your visitor's personal data for purposes other than those indicated in previous sections of this questionnaire, do you give your visitors the opportunity to consent to those new purposes?

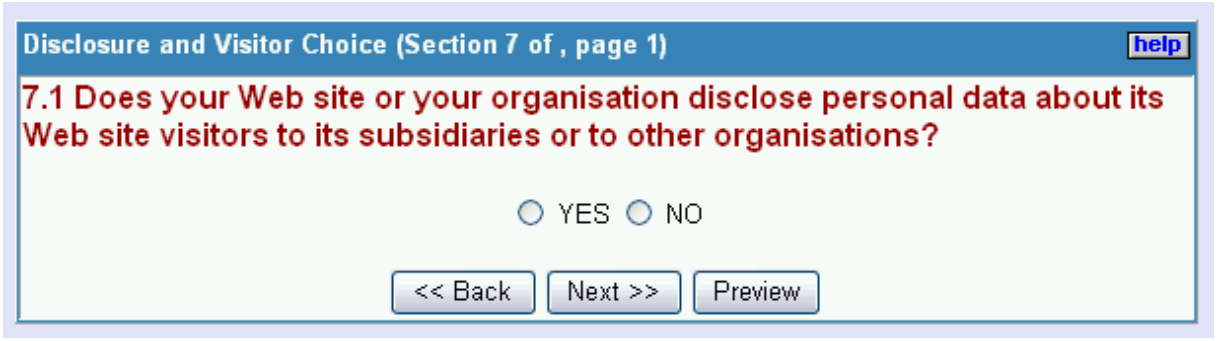
○ YES ○ NO

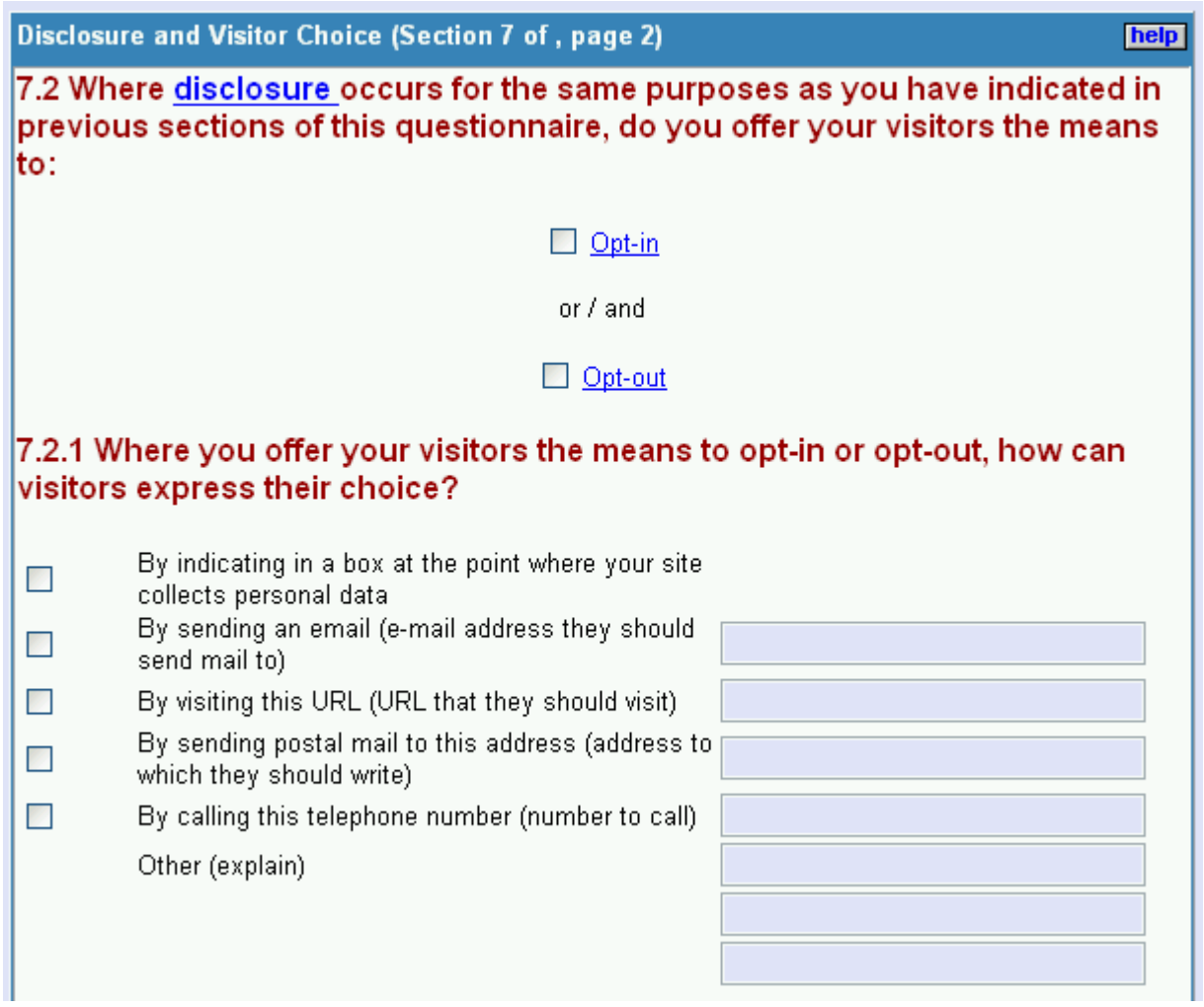
5.5.1 If yes, how can visitors express their choice?

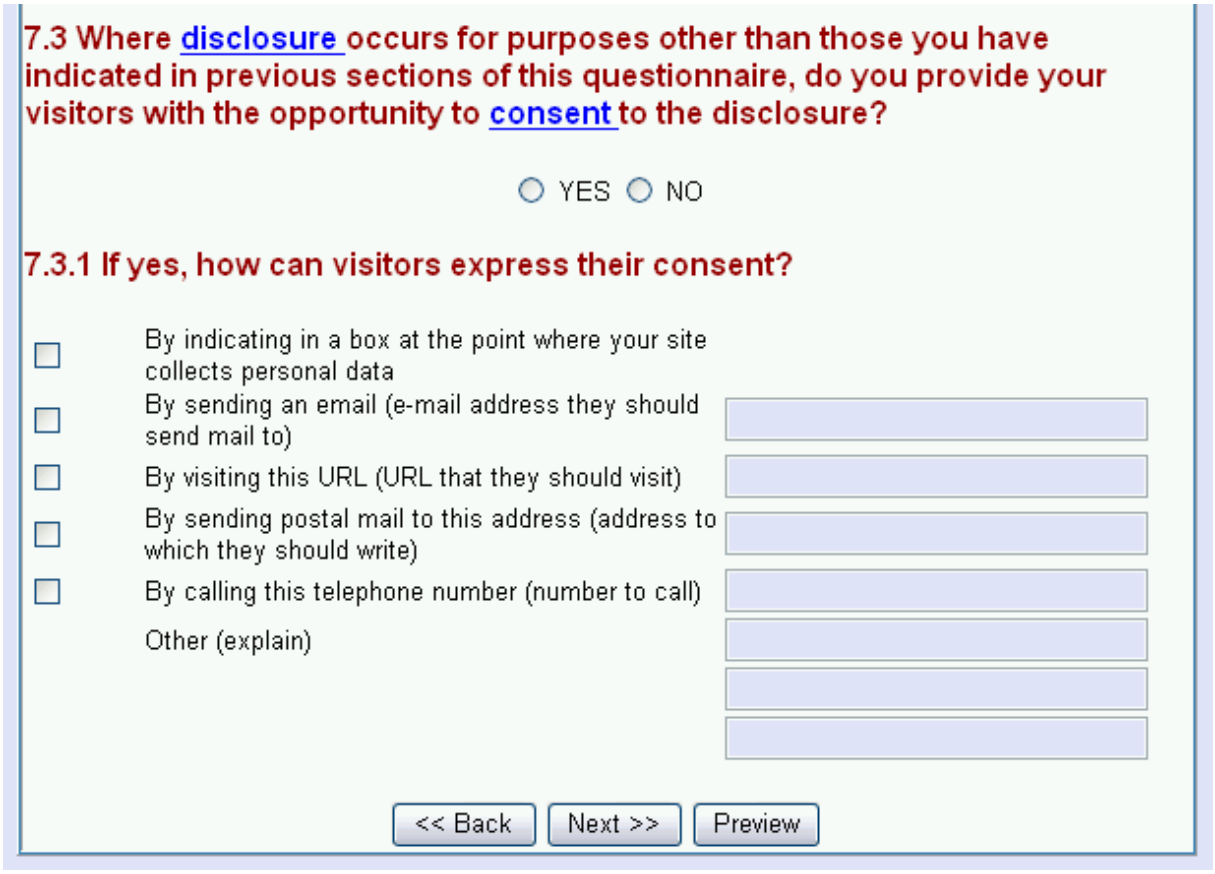
- ☐ By indicating in a box at the point on the site where personal data is collected
- ☐ By sending an email (e-mail address they should send mail to)
- ☐ By visiting this URL (URL that they should visit)
- ☐ By sending postal mail to this address (address to which they should write)
- ☐ By calling this telephone number (number to call)
- Other (explain)

<< Back | Next >> | Preview


Children's Privacy (Section 6 of , page 1)
help
6.1 Do you knowingly collect personal data on children?
YES NO
6.2 Do you take specific steps to protect the privacy of children whose personal data you knowingly or unknowingly collect?
YES NO
6.2.1 If yes, please describe the specific steps you take to protect the privacy of children, and tick all relevant boxes below:
We make reasonable efforts to verify that a parent has consented to the collection of the child's personal data.
We give parents the option to consent to the collection and use of the child's personal data for internal use.
We give parents the option to consent to the collection and use of the child's personal data for disclosure to third parties.
Other. Please describe (To ensure that children's privacy is respected on our Web site, we ...)
1
2
3
6.2.2 Do you provide information detailing your personal data practices in relation to children on your home page and at every point at which you collect personal data from children?
YES NO
<< Back
Next >>
Preview


Disclosure and Visitor Choice (Section 7 of , page 1)
help
7.1 Does your Web site or your organisation disclose personal data about its Web site visitors to its subsidiaries or to other organisations?
YES
NO
<< Back
Next >>
Preview


Disclosure and Visitor Choice (Section 7 of , page 2)
help
7.2 Where disclosure occurs for the same purposes as you have indicated in previous sections of this questionnaire, do you offer your visitors the means to:
Opt-in
or / and
Opt-out
7.2.1 Where you offer your visitors the means to opt-in or opt-out, how can visitors express their choice?
By indicating in a box at the point where your site collects personal data
By sending an email (e-mail address they should send mail to)
By visiting this URL (URL that they should visit)
By sending postal mail to this address (address to which they should write)
By calling this telephone number (number to call)
Other (explain)


7.3 Where disclosure occurs for purposes other than those you have indicated in previous sections of this questionnaire, do you provide your visitors with the opportunity to consent to the disclosure?
YES
NO
7.3.1 If yes, how can visitors express their consent?
By indicating in a box at the point where your site collects personal data
By sending an email (e-mail address they should send mail to)
By visiting this URL (URL that they should visit)
By sending postal mail to this address (address to which they should write)
By calling this telephone number (number to call)
Other (explain)
<< Back
Next >>
Preview

Confidentiality / Security (Section 8 of , page 1) help

8.1 Do you give visitors to your Web site the option of using a secure transmission method to send personal data to you?

○ YES ○ NO

8.2 Please indicate the types of personal data you allow visitors to send via a secure transmission method, by ticking the appropriate boxes:

- ☐ Primary personal data (such as name and contact details)
- ☐ Other personal and profiling data (such as physical description, leisure activities)
- ☐ Identifiers (such as credit card details, Web site password)
- ☐ Specific personal data (such as racial or ethnic origin, religious beliefs, medical data)

Other. Please describe :

1
2
3

8.3 Does your Web site have security policies, rules or technical measures in place to protect visitor's personal data which are under your control from:

8.3.1 Unauthorised access	○ YES ○ NO
8.3.2 Improper use or disclosure	○ YES ○ NO
8.3.3 Unauthorised modification or alteration	○ YES ○ NO
8.3.4 Unlawful destruction or accidental loss	○ YES ○ NO

8.4 Are your employees and data processors obliged to respect the confidentiality of visitors' personal data?

○ YES ○ NO

8.5 Does your organisation and Web site ensure that visitors' personal data will not be disclosed to state institutions and authorities except where required by law or other regulations?

○ YES ○ NO

<< Back | Next >> | Preview

Individual Participation / Access (Section 9 of , page 1) help

9.1 Can a visitor find out from your organisation or Web site whether you are keeping personal data relating to him or her?

○ YES ○ NO

9.1.1 If yes, how can a visitor find out whether your organisation or Web site is keeping personal data about him or her?

☐	By sending an email (e-mail address they should send mail to)	
☐	By visiting this URL (URL that they should visit)	
☐	By sending postal mail to this address (address to which they should write)	
☐	By calling this telephone number (number to call)	
	Other (explain)	

9.2 Can a visitor obtain from your organisation or Web site an intelligible copy of the personal data that you keep about him or her?

○ YES ○ NO

9.2.1 If yes, how can a visitor obtain an intelligible copy of the personal data that you keep about him or her?

☐	By sending an email (e-mail address they should send mail to)	
☐	By visiting this URL (URL that they should visit)	
☐	By sending postal mail to this address (address to which they should write)	
☐	By calling this telephone number (number to call)	
	Other (explain)	

9.2.2 How long does it usually take for the visitor to obtain the information?

- ☐ Almost instantaneously online
- ☐ Within a week
- ☐ Within a month
- ☐ Longer (specify):

9.2.3 Do you make a specific charge ?

○ YES ○ NO

9.2.4 Please specify the amount of the charge:

9.3 Do you allow a visitor to challenge the data that you hold?

○ YES ○ NO

9.3.1 If a challenge is successful, can the visitor have their personal data (as may be appropriate to the particular case):

- ☐ Erased
- ☐ Rectified or amended
- ☐ Completed

9.4 Do you reserve the right to refuse to provide the data?

○ YES ○ NO

9.4.1 If yes, do you give reasons for refusing to provide information to a visitor?

○ YES ○ NO

9.4.2 Can a visitor challenge your refusal to provide personal data that you hold?

○ YES ○ NO

9.5 Do you require proof of identity before providing the personal data?

○ YES ○ NO

<< Back | Next >> | Preview

Privacy Compliance (Section 10 of , page 1) help

You have indicated that you do not collect personal data about your visitors by any means and from any source. If this does not accurately reflects your information practices, please reconsider your answers to 4.2, 4.3, 5.1 and 5.2. Answering "Yes" to any of these questions will enable you to complete the full questionnaire.

10.1 Are there any national privacy laws or self-regulatory schemes applicable to your Web site or organisation?

○ YES ○ NO

10.1.1 If yes, is your privacy policy compliant with the applicable national privacy law or self-regulatory schemes ?

○ YES ○ NO

10.1.2 Please mention the main privacy instrument(s) your policy is compliant with (title and country in each field):

1
2
3

10.2 Are there any global or regional privacy regulatory or self-regulatory schemes applicable to your Web site or organisation?

○ YES ○ NO

10.2.1 If yes, is your privacy policy consistent with a global or regional regulatory privacy instrument or self-regulatory privacy scheme?

○ YES ○ NO

10.2.2 Please mention the main global or regional regulatory privacy instrument(s) or self-regulatory scheme(s) your policy is consistent with (title and origin in each field):

1
2
3

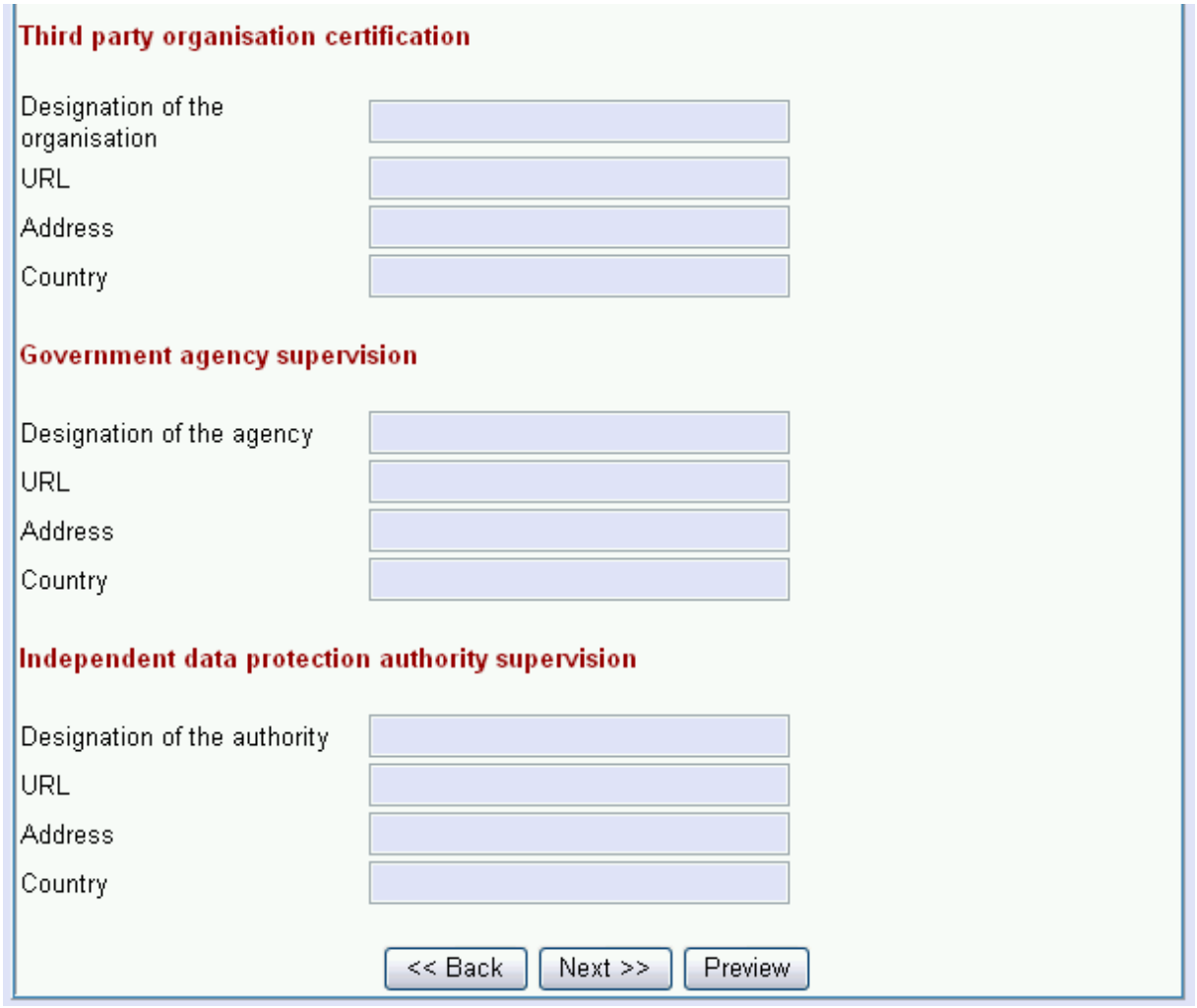
10.3 In order to demonstrate that your privacy policy accords with the applicable regulation indicated above, are you:

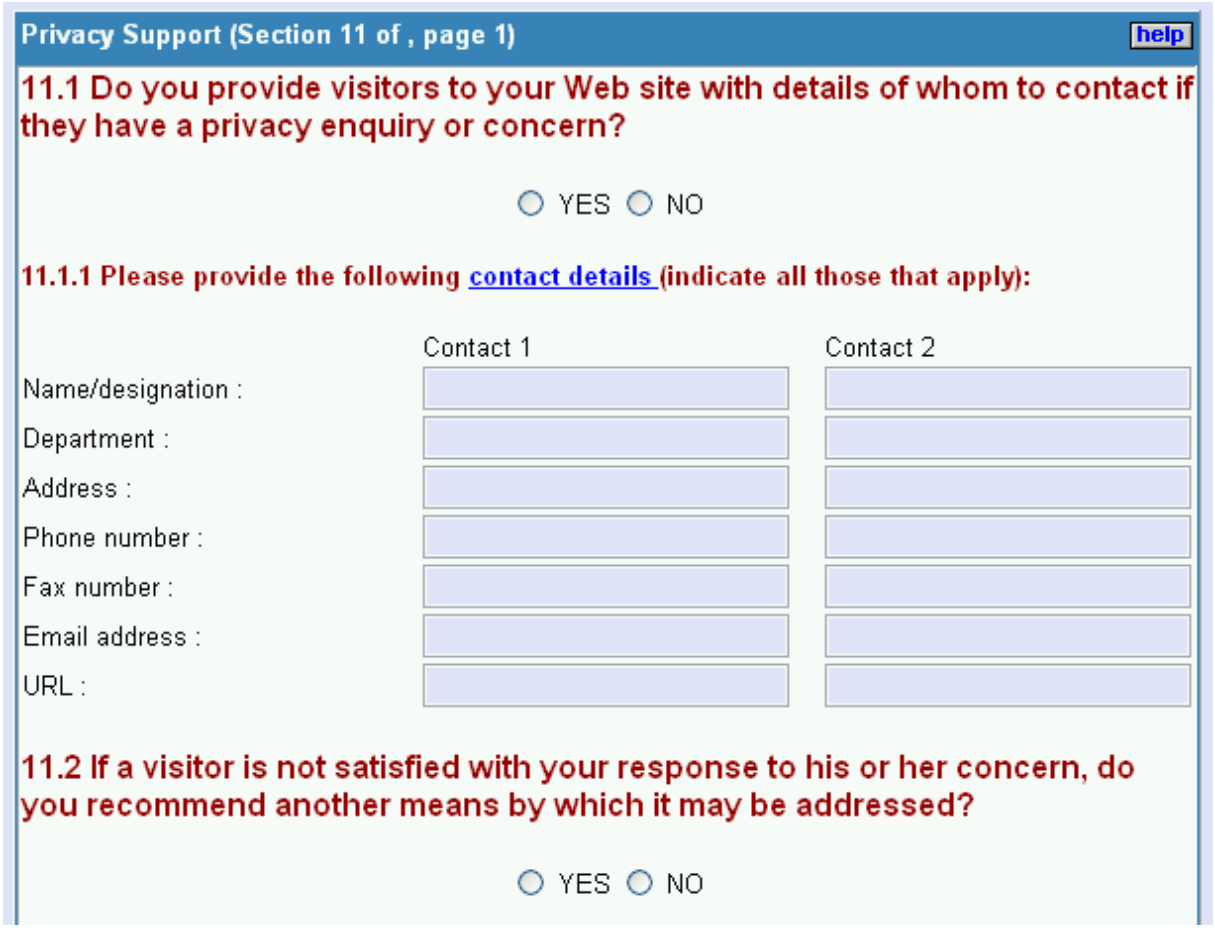
- ☐ Voluntarily committed to a self- assessment procedure
- ☐ Voluntarily committed to a third party organisation certification
- ☐ Subject to supervision by a government agency
- ☐ Subject to supervision by an independent data protection authority

10.3.1 Please indicate the following details for all that apply above:

Self-assessment procedure

Name or designation of the privacy policy person or service	
URL	
Address	
Country	


Third party organisation certification
Designation of the organisation
URL
Address
Country
Government agency supervision
Designation of the agency
URL
Address
Country
Independent data protection authority supervision
Designation of the authority
URL
Address
Country
<< Back
Next >>
Preview



Privacy Support (Section 11 of , page 1) help

11.1 Do you provide visitors to your Web site with details of whom to contact if they have a privacy enquiry or concern?

○ YES ○ NO

11.1.1 Please provide the following contact details (indicate all those that apply):

	Contact 1	Contact 2
Name/designation :		
Department :		
Address :		
Phone number :		
Fax number :		
Email address :		
URL :		

11.2 If a visitor is not satisfied with your response to his or her concern, do you recommend another means by which it may be addressed?

○ YES ○ NO

11.3 What other means of addressing visitor's concerns do you recommend?

☐ If your organisation or Web site provides users with the option of using any third party dispute resolution mechanisms related to your collection or use of their personally identifiable information, please list the name and how to contact and use those services

Name :

Contact details (e.g. URL):

Pre-conditions (e.g. costs):

☐ Contact with the relevant government agency or department. Please give name and contact details :

Name :

Contact details (e.g. URL):

☐ Contact with the relevant data protection authority. Please give name and contact details :

Name :

Contact details (e.g. URL):

☐ Other. Please describe (if visitors are not satisfied with our response to their concern, we recommend that visitors contact).

Name :

Contact details (e.g. URL):

<< Back | Next >> | Preview

Downloading Your Draft Privacy Statement

help

Now that you have completed the questionnaire, a draft privacy policy statement will be generated based on the answers that you have provided. Please read what follows and preview your whole draft statement at the bottom of this page before downloading it.

1. Assessing the Contents of Your Draft Privacy Policy Statement

You should ensure that the draft privacy statement:

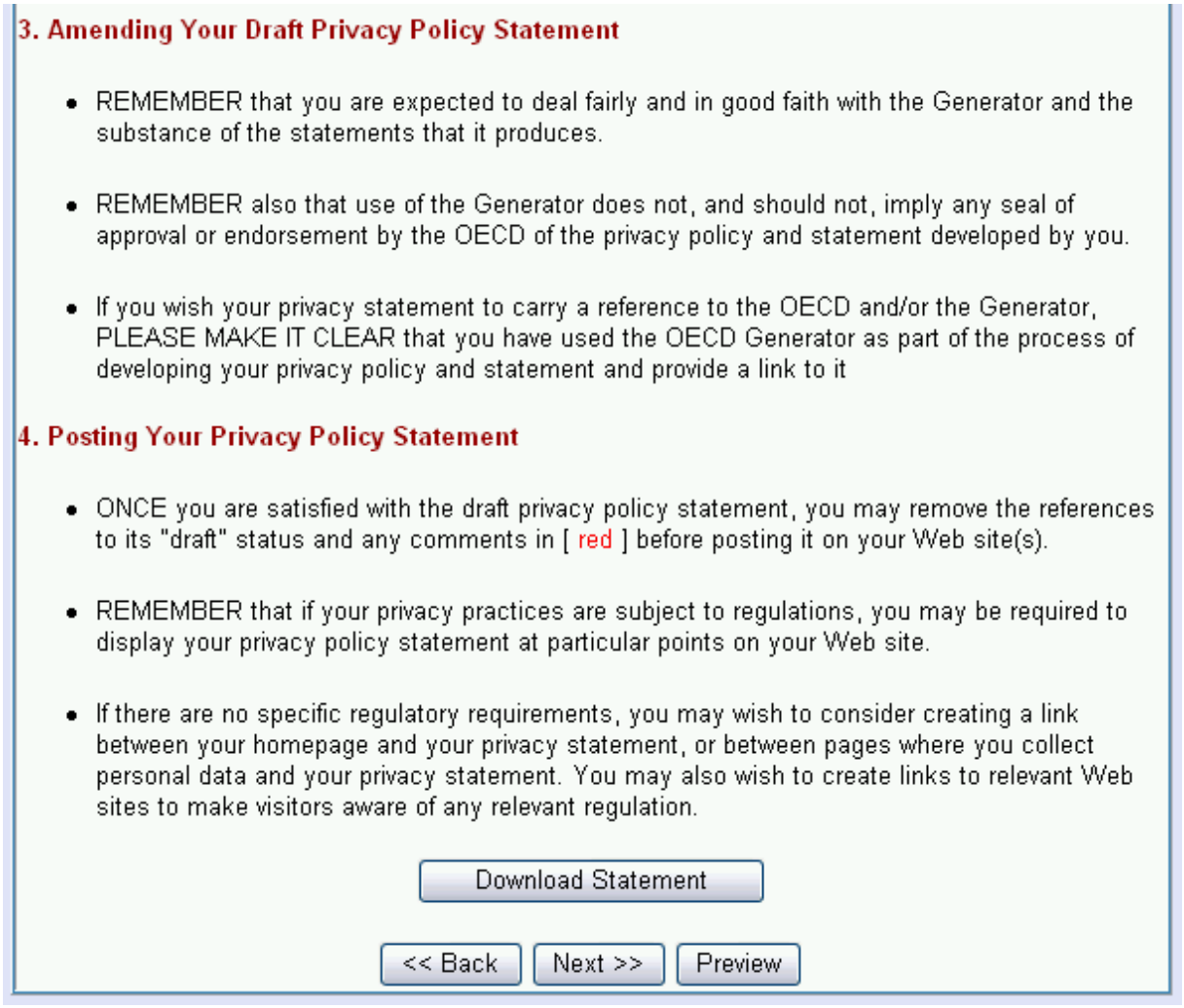
- accurately reflects your organisation's privacy practices
- complies with any national, regional and international laws, or (self) regulatory schemes that apply to your organisation
- reads fluently and that any errors are corrected.

2. Assessing Your Draft Privacy Policy Statement's Compliance with the OECD Guidelines

Your draft privacy policy statement will be generated according to the answers that you have provided to the questions.

If you have given answers that are inconsistent with the OECD Privacy Guidelines, these will be indicated at the end of your draft privacy policy statement. These comments will be in [red] to make them obvious.

If such a comment appears at the end of your draft privacy policy statement, you may want to return to the relevant question in the questionnaire and reconsider your privacy practices. When your practices are changed and implemented, you should reconsider your answers and update your privacy policy statement.



What to do next

You have now completed the Privacy Policy Generator. We hope that you have found it helpful in establishing your privacy policy statement.

Please remember that, unless you choose to delete them, the information you provide and your answers to the questions asked will be kept on the OECD server, so that you may, if you wish, return to and modify your statement. However, the OECD will not access or use your information and answers for any purpose.

Chapter 8

BUILDING TRUST IN THE ONLINE ENVIRONMENT: BUSINESS-TO-CONSUMER DISPUTE RESOLUTION - REPORT OF THE DECEMBER 2000 OECD CONFERENCE

This chapter summarises a conference on business-to-consumer (B2C) online dispute resolution with the Hague Conference on Private International Law (HCPIL) and the International Chamber of Commerce (ICC), held on 11-12 December 2000 in The Hague. The objectives of the Conference were to: *(i)* provide an opportunity for presenting, discussing and disseminating information on the diverse range of existing online alternative dispute resolution (ADR) mechanisms; *(ii)* explore whether and how online ADR can help resolve B2C disputes arising from privacy and consumer protection issues and thus improve trust for global electronic commerce; and *(iii)* discuss the role of stakeholders in fostering the development of appropriate and effective online ADR mechanisms. The primary focus of the conference was on B2C disputes involving small values and/or low levels of harm, as well as on informal, flexible systems that allow for the necessary balancing between the type of dispute and the formality of the process for resolution (*e.g.* assisted negotiation and mediation). The report on the conference is preceded by the orientation document that was issued prior to the conference to assist participants in discussing the issues to be explored.

Chapter 8

BUILDING TRUST IN THE ONLINE ENVIRONMENT: BUSINESS TO CONSUMER DISPUTE RESOLUTION - REPORT OF THE DECEMBER 2000 OECD CONFERENCE

Presentation of the conference (orientation document and agenda overview)

The online environment is playing an important role in the global market. Both consumers and business will derive significant benefit from online interactions. With these benefits and the expected increase of business-to-consumer (B2C) national and international interactions, come new challenges. Of particular significance are the challenges of identifying the competent forum and applicable law, and of obtaining redress across borders. Given that traditional court-based dispute settlement mechanisms may not provide effective redress for electronic commerce interactions, there is a need to examine alternative dispute resolution (ADR[1]) mechanisms both those in existence and under development as ways to fairly and effectively settle disputes.

Online ADR mechanisms hold the promise of providing speedy, low cost redress for a large number of the small claims and low-value transactions arising from B2C online interactions. In addition, new and developing technologies might provide innovative and potentially more effective dispute resolution, either alone or in combination with existing mechanisms.

This Conference on B2C Online Dispute Resolution is organised by the OECD[2] with the Hague Conference on Private International Law (HCOPIL) and the International Chamber of Commerce (ICC). The views of consumers are represented by Consumers International (CI).

Objectives

Building on discussions and information shared to date in various fora, the conference will:

- Provide an opportunity for presenting, discussing and disseminating information on the diverse range of existing online ADR mechanisms (day 1).
- Explore whether and how online ADR can improve trust for global electronic commerce by helping to resolve B2C disputes arising from privacy and consumer protection issues; this will include identifying what stakeholders view as important elements for fair and effective online ADR mechanisms, recognising that these elements, which are of various types (socio-economic, legal, technical), may vary depending on the type of mechanism and/or dispute.
- Discuss the role of stakeholders in fostering the development of appropriate and effective online ADR mechanisms (day 2).

Analysis and future work by co-organisers

Based on the two-day discussion, the Conference is expected to help all stakeholders outline their further direction for work in this area. The OECD secretariat will draft proposals for future work by the OECD in the field of online B2C alternative dispute resolution, which will be presented to the

OECD Working Party on Information Security and Privacy, and the Committee on Consumer Policy at their meetings in early 2001.

Conference procedure

The conference has been organised to facilitate discussion among session participants and with the audience. Under the guidance of moderators, most sessions will begin with brief presentations followed by reactions and comments from panellists, as well as question/answer and active participation of the audience. A wide range of stakeholders, including representatives of business, users and consumers, and government will participate in the Conference. Academics and ADR providers will also participate.

A report of the Conference will be published in early 2001.

Background materials

This Orientation Document is intended to assist Conference participants in discussing the issues to be explored. It highlights the focus for each session, suggests questions to be considered, and provides brief summaries of presentations. Related documents are attached as follows:

- A list of online ADR mechanisms as identified by the OECD (based on independent research and materials provided by the ICC and CI) as of October 2000 (Appendix A).
- A list of possible procedural, substantive and other elements that might exist in ADR mechanisms (Appendix B).
- Various papers and recommendations related to B2C ADR systems produced thus far by the:
    - European Commission (EC) (Commission Recommendation 98/257/EC on the principles applicable to the bodies responsible for out-of-court settlement of consumer disputes).
    - Trans Atlantic Consumer Dialogue (TACD) (Alternative Dispute Resolution in the Context of Electronic Commerce Recommendation, February 2000).
    - European Commission (EC) (Out-of-Court Dispute Settlement Systems for E-Commerce: The Report from the Workshop held in Brussels on 21 March 2000).
    - US Government (USG) (Summary of June 2000 Public Workshop "Alternative Dispute Resolution for Consumer Transactions in a Borderless Online Marketplace," November 2000).
    - Asia Pacific Economic Co-operation (APEC) E-Commerce Steering Group (Consumer Protection in Electronic Commerce: Report and proposals for action following the APEC workshop on consumer protection held in Bangkok on 20 July 2000).
    - Global Business Dialogue for Electronic Commerce (GBDe) (Alternative Dispute Resolution Paper, September 2000).
    - Consumers International (CI) (Disputes in Cyberspace Report, December 2000).
- Reports and documents related to ADR and trustmark seal programmes:
    - Report from September 1999 Geneva Roundtable on Electronic Commerce and Private International Law, April 2000.
    - Electronic Commerce and Consumer Protection Group's Guidelines for Merchant-to-Consumer Transactions, released 6 June 2000.

- Inventory of ADR mechanisms produced by the ICC in "Out-of-court settlement of disputes concerning e-commerce consumer transactions: An inventory of current approaches, September 2000".
- Report on "Web seals: a review of Online Privacy Programs" produced by the Data Protection Commissioners of Ontario, Canada, and Australia in September 2000.
- BBBOnline Code of Online Business Practices, released 24 October 2000.

- Articles and comments submitted voluntarily by the public in anticipation of the discussions at the Conference.

Introduction to ADR

"ADR refers to a broad range of mechanisms and processes designed to assist parties in resolving differences. These alternative mechanisms are not intended to supplant court adjudication, but rather to supplement it."[3] Generally, an ADR process involves a series of procedures, some of which may vary depending upon the form of resolution.[4] The most common forms of resolution are negotiation, facilitation or conciliation, mediation, and arbitration.

Though there is not full consensus - in the academic or business fields - on the precise definitions of ADR mechanisms and processes, most experts view ADR as a spectrum of approaches that fits within the broader spectrum of "dispute resolution" different ways of settling disputes, including corporate consumer complaint services, ADR, and litigation. ADR mechanisms differ on a sliding scale from the most flexible to the most formal in terms of the rules of procedure, the role of the neutral in facilitating or deciding an outcome, whether the outcome is non-binding or binding on all parties or on one of them, and, where the outcome is binding, whether this was prescribed in advance, either before or after the dispute arose.

At the extreme ends of the ADR spectrum rest assisted negotiation[5] (the most informal) and arbitration[6] (the most formal, or most "court-like"). For example, in assisted negotiation, decisions remain in the hands of the parties at all times and outcomes are agreed upon. While in arbitration, whether before or after the dispute arises, parties agree to be bound by the final decision of the third-party arbitrator. Between assisted negotiation and arbitration are a large variety of forms of mediation, from neutral evaluation to hybrid forms such as mediation-arbitration (med-arb).

ADR is used off-line to resolve many different types of disputes, from local disputes between neighbours to international commercial transactions. Not surprisingly, ADR mechanisms are being developed in the online environment to resolve a wide range of disputes (*e.g.* domain names, insurance, privacy, family, employment and commercial) between parties (B2B, B2C, C to C, G to B and G to C) involved in electronic interactions. These online mechanisms are not only used for disputes arising online; rather a dispute arising in the offline environment could be resolved using an online ADR mechanism.

Online ADR exists in a variety of contexts, including within a particular online marketplace (*e.g.* online auction sites), as part of a trustmark or seal programme, or on an independent basis. These differences may have an effect on consumer access to ADR and business compliance with the outcome.

In recent surveys and inventories, the OECD, ICC and CI have identified more than 40 online ADR mechanisms, most of them offering B2C dispute resolution.[7] These online ADR mechanisms vary in terms of procedural and technical aspects. It is however possible to distinguish those which are "fully automated", in that outcomes are generated by a computer program and not with human

intervention, from most others which vary from flexible to formal. While 26 of the online ADR providers offer informal, non-binding types of dispute settlement, such as assisted negotiation, mediation, or ombuds-type services, 14 offer more formal, binding arbitration procedures; 11 feature automated dispute resolution, and 14 offer multiple ADR methods.

Focus

This conference will explore the use of online ADR systems for disputes involving small values and/or low levels of harm that arise between businesses and consumers online with a primary focus on informal, flexible systems that will allow for the necessary balancing between the type of dispute and the formality of the process for resolution (see shaded area in figure below). For example, the cost or the complexity of the procedure should not be disproportionate with what is at stake.

Figure 8.1. **Main ADR forms and processes**

<table>
<tr><th>Corporate complaint services</th><th>Assisted negotiation</th><th>Mediation</th><th>Arbitration</th><th>Litigation</th></tr>
<tr><td></td><td>– Facilitation
– Conciliation</td><td>On a Sliding Scale:
– Automated, or not
– More or less active guidance by the neutral
– Voluntary or mandatory participation
– No obligation on the parties to agree, before entering ADR, that the outcome will be binding</td><td>– Voluntary or mandatory submission
– Automated or not
– Final and binding</td><td></td></tr>
<tr><td colspan="4">→→→→→→→→→→
Informal to formal ADR</td><td></td></tr>
</table>

Source: OECD.

Day 1: Overview of ADR in relations to the online environment

Welcome and keynote

Building trust is an important policy issue related to the new economy and global information society. In particular, a key element to building trust is ensuring users and consumers effective redress for disputes arising from interactions and transactions in the online environment.

The OECD mandate to explore redress for users and consumers is clearly stated in the OECD 1998 Ministerial Declaration on Protection of Privacy on Global Networks[8] and Consumer Protection in the Context of Electronic Commerce[9,] which serve as part of the blueprint for the OECD's work in electronic commerce. The mandate is further clarified by the 1999 Guidelines on Consumer Protection in the Context of Electronic Commerce, where OECD member countries stress the importance of providing consumers with "meaningful access to fair and timely alternative dispute resolution and redress without undue cost or burden".[10] Similarly, the need for appropriate dispute resolution mechanisms in disputes over privacy has been highlighted in the OECD Report on Transborder Data Flow Contracts in the Wider Framework of Mechanisms for Privacy Protection on Global Networks.[11]

Consequently, the OECD programme of work for 2000-2001 places great emphasis on exploring how privacy and consumer protection disputes can effectively be resolved using online ADR.

Welcome remarks

A.H Korthals, Minister of Justice, The Netherlands

Keynotes

Why is ADR a key element for building trust in the online environment?

Herwig Schlögl, Deputy Secretary-General, Organisation for Economic Co-operation and Development

The importance of global partnership in the development and support of ADR

Maria Livanos Cattaui, Secretary General, International Chamber of Commerce

In or out of court? Challenges for the Hague Conference

Hans van Loon, Secretary General, Hague Conference on Private International Law

Introductory remarks by Day 1 Chair

Peter Ford, Chair, OECD Working Party on Information Security and Privacy

Session 1: Taking stock - Overview of recent discussions about online ADR

Several entities have either developed principles for B2C ADR systems or expressed views on essential elements of such ADR systems. In an effort to provide a forum, at a global level, for exploration of ADR and to foster co-operation among the stakeholders, this session takes stock of the work that has been undertaken on this issue by other fora. Representatives from the European Commission (EC), United States (US), Asian Pacific Economic Co-operation (APEC), Global Business Dialogue (GBDe), and Consumers International (CI) will present the findings from their fora's examination of online ADR.

While there are areas of common ground on principles for online ADR, further discussion needs to take place. This session is expected to outline similarities and differences in the various approaches to date in order to facilitate the Conference discussion on challenges to be met and gaps to be bridged in terms of essential elements for fair and effective online ADR.

Moderator: Risaburo Nezu, Director, Directorate for Science, Technology and Industry, OECD

Presenters:

Carina Tornblom, Head of Unit, Directorate General for Health and Consumer Protection, European Commission will present the approach of the European Commission based on the 1998 Commission Recommendation on the principles applicable to the bodies responsible for out-of-court settlement of consumer disputes and the workshop, which was held in March 2000.

James Dorskind, Acting General Counsel, US Department of Commerce will provide insight into the recently released report from the joint Federal Trade Commission-Department of Commerce public workshop "Alternative Dispute Resolution for Consumer Transactions in a Borderless Online Marketplace," which was held in Washington, DC on 6-7 June 2000.[12]

Yuko Yasunaga, Deputy Director, Commerce Policy Division, Japan Ministry of International Trade and Industry (APEC) will present the results of the APEC Consumer Protection Workshop, which was held in July 2000 in Bangkok, Thailand.[13]

Constanze Picking, Senior Manager Trade and E-Business, DaimlerChrysler AG will present the GBDe Alternative Dispute Resolution Paper, issued in September 2000.[14]

Louise Sylvan, President, Consumers International will present a recent report from Consumers International on disputes in cyberspace. The presentation will also cover the principles adopted by the Trans-Atlantic Consumer Dialogue in February 2000.

Session 2: Illustrating business-to-consumer complaints in the online environment

This session will provide information and statistics on the types of complaints received from users and consumers in relation to their interactions and transactions online. The information will be presented by consumer and data protection authorities and consumer representatives in an effort to clarify the types and volume of disputes arising from B2C online interactions and transactions. The purpose of this session is to educate all stakeholders on where to focus their efforts in exploring redress mechanisms and discussing online ADR mechanisms.

Presenters:

Michelle Childs, Head of Policy, Consumers Association, United Kingdom will present the statistics on the types of complaints received by Consumers Association in the United Kingdom as well as by the other consumer organisations, affiliated with the WebTrader scheme, from Belgium, Italy, France, The Netherlands, Portugal, and Spain.

Stephen Lau, Privacy Commissioner for Personal Data, Office of the Privacy Commissioner for Personal Data Hong Kong, China will discuss the nature of consumer complaints in Hong Kong relating to the handling of personal data on the Internet which might be in contravention with the data protection principles enshrined in the Hong Kong Personal Data (privacy) Ordinance.

Marcie Girouard, Assistant Deputy Commissioner, Industry Canada.

Maneesha Mithal, Attorney, Bureau of Consumer Protection, US Federal Trade Commission will present statistics on B2C complaints received by their respective agencies. The statistics will mainly be drawn from Consumer Sentinel, a fraud complaint database for use by law enforcement officials in the US, Canada, and Australia. In its less than five years of operation, the database now contains more than 44 000 Internet-related complaints, many of which have a cross-border component. For example, one in eight complaints received by the US and Canadian organisations involve foreign consumers or companies.

Session 3: Dispute resolution at the earliest stage – internal customer complaints handling and customer refunds

In the offline world, business internal complaints handling systems assist in effectively preventing and resolving disputes between business and consumers. It is anticipated that online business internal customer complaint handling systems will be as effective in the online environment. Similarly, chargeback regimes implemented by the payment card industry can provide significant benefits to certain consumers by providing customer refunds; some of these protections are required by law and some are provided voluntarily as a result of marketplace considerations. This session will explore how internal customer complaint handling and customer refunds (as a result of chargeback systems) could resolve complaints and disputes that arise in the B2C online environment. This session will also examine the scope of application and effectiveness of these mechanisms to resolve customer complaints in the online environment as compared to the offline environment.

Moderator: Hugh Stevenson, Associate Director, Bureau of Consumer Protection, US Federal Trade Commission

Panellists:

Jean Ann Fox, Director of Consumer Protection, Consumer Federation of America

Peter Møller Jensen, Manager, European Union Relations, Visa International

Eric Mickwitz, Finnish Consumer Ombudsman

Michel Van Huffel, Directorate General for Health and Consumer Protection, European Commission

Presenters:

Charles Underhill, Acting Chief Operating Officer, Better Business Bureau, will address how the BBB's codes of conduct and other initiatives assist in promoting effective internal complaints handling by businesses. He will present statistics on the rates of success with the conciliation phase of the BBB's third-party complaint handling system and data from similar programs. The presentation will also highlight a new initiative by the BBB to encourage internal complaints handling.

Alastair Tempest, Director General, Federation of European Direct Marketing (FEDMA) will explain FEDMA's role as a clearinghouse for European e-merchants with a particular focus on how FEDMA's Code of Conduct on e-Commerce & Interactive Marketing and other initiatives ("the Ring of Confidence") help in ensuring consumer redress, particularly across national borders.

Helen Bridges, Counsel, American Express Services, Europe, will present American Express's chargeback policy and consumer card member protections for online transactions.

Suggested questions

Are statistics available on the number and types of resolutions reached as result of internal complaints handling and customer refunds through payment cards? What are the incentives to encourage business to handle complaints internally? How does online customer complaint handling differ from customer complaint handling by telephone, in writing, or in person? How widely available online are chargeback protections? Are there other innovative mechanisms arising in the online environment that will assist in resolving disputes early or assist in avoiding disputes, like feedback/rating systems, insurance, and escrow systems?

Session 4: Online alternative dispute resolution mechanisms

Global networks and electronic commerce significantly increase the possibility for individuals and companies to interact and transact easily 24 hours a day, 7 days a week, over great distances, regardless of geographic borders, local cultures and legal frameworks. Such benefits, however, raise challenges as to how potential disputes arising from both sides can be resolved in an equally easy way, effectively, and with guarantees of equity and fairness. A pragmatic approach aimed at providing individuals and businesses with accessible and potentially more efficient means to settle disputes that cannot otherwise easily be resolved offers an interesting alternative.

This session will explore through presentations of online ADR mechanisms, already existing or under development, the variety of approaches for solving disputes arising online. In an effort to focus on distinctive procedural and other elements that exist in these various mechanisms and to facilitate the discussion on day 2, the discussion has been divided into three parts. The first discussion is devoted to fully automated mechanisms where outcomes are generated without human intervention. The second and third discussions will examine mechanisms that vary from flexible to formal with regard to procedure and intervention of a neutral. Finally, the fourth discussion, by exploring systems under development, will focus on objectives and methodology necessary for setting up an online ADR mechanism.

Moderator: Bernard Clements, Head of Unit, Joint Research Centre, European Commission

Panellists:

John Borking, Deputy Privacy Commissioner for the Netherlands

Dana Haviland, Partner, Wilson Sonsini Goodrich & Rosati

Ethan Katsh, Director, Center for Information Technologies and Dispute Resolution, University of Massachusetts

Pippa Lawson, Counsel, Public Interest Advocacy Centre

Odile Nicholas-Etienne, *Union Federale des Consommateurs*

Charles Underhill, Acting Chief Operating Officer, Better Business Bureau

I. Fully automated online resolution mechanisms

(*e.g.* outcome generated by computer)

Most fully automated ADR systems are designed to settle cash-based disputes, such as insurance claims, and require the parties, before entering a negotiation, to be bound by the generated outcome, if the dispute settles. A small number of automated programs, however, allow parties to choose at the outset whether or not to be bound by the outcome[15]. This session will explore whether automated systems could help settle non-financial B2C disputes arising in the area of privacy and consumer protection.

Presenter:

Richard Belczynski, Vice President, International and Commercial Division, ClickNSettle will present the fully automated system of the ClickNSettle business model, where the outcome is generated by computer. The presentation will also include the types of disputes that can be and have been resolved using ClickNSettle and the geographic distribution of the parties that have engaged in resolution by ClickNSettle. (www.clicknsettle.com).

II. Flexible resolution mechanisms

(*e.g.* negotiation/mediation)

Presenters:

Colin Rule, Chief Executive Officer, Online Resolution, Inc. will present a summary of their various online resolution methods with particular emphasis on a new online resolution platform, *Resolution Room*. This new service is an interactive environment for mediation that combines several communications tools, including e-mail, blind bidding, and chat capabilities. The system is designed to resolve two-party and multi-party disputes. (www.onlineresolution.com)

Cara Cherry Lisco, Director, SquareTrade Online Dispute Resolution Network, will present an overview of a scalable online tool and dispute resolution service set up in February 2000. She will show how SquareTrade has been effectively inserted as the underlying neutral recourse mechanism in nearly 2 million transactions a week as the preferred provider of dispute resolution for eBay[16] users. She will also discuss lessons learned from its successful handling of more than 17 000 disputes from more than 80 countries in multiple languages including English, German, and Spanish. (www.squaretrade.com)

III. Formal resolution mechanisms

(*e.g.* mediation/arbitration)

Presenters:

Erik Wilbers, Senior Counsellor, WIPO Mediation and Arbitration Center will present practical conclusions, based on the online dispute resolution experience of the WIPO Center, that may be of benefit in creating appropriate methods for the resolution of consumer disputes. Over the past few years, the WIPO Arbitration and Mediation Center has gained experience in the design and application of online dispute resolution procedures. Using online methods, the Center this year has administered over 1 600 domain name disputes. It has also undertaken work in the development of more generic applications that lend themselves to the arbitration of all types of disputes under the WIPO Rules. (www.wipo.org)

Fabien Gélinas, Vice President and General Counsel, e-Resolution, will discuss the company's online arbitration model for domain name and other disputes. He will examine the arbitration process in the B2C area and draw some analogies and contrasts to online settlement of B2C disputes. The presentation will also address questions of the enforcement of an arbitration decision and the applicability of arbitration for B2C dispute resolution, based on eResolution's experiences. (www.eresolution.com)

IV. ADR mechanisms under development

Presenters:

Duncan McDonald, American Institute for Contemporary German Studies (AICGS) will present the AICGS proposal to create a network of US-EU universities to act as mediators to deal with consumer bewilderment about dispute management, ADR providers, and statutory rights. Emphasis will be on tackling the variety of legal and other issues that must be dealt with to set up and implement an effective cross-border scheme.

Vincent Tilman, Researcher, *Centre de Recherches Informatique et Droit* (CRID) will describe ECODIR, a cross-border online ADR project currently under development. The project, subsidised by the European Union, aims to provide consumers with an online mediation/arbitration support system to settle disputes arising from the use of the Internet. The project is led by the CRID, University of Namur, in co-operation with a consortium of European and North American Universities, mediation centres and private partners. The presentation will highlight the objectives, methodology, and the development schedule of ECODIR and will address particularly the challenges involved in deploying such a system for a cross-border, multi-lingual environment.

Christopher Kuner, Of Counsel, Morrison & Foerster, LLC will provide an overview of future International Chamber of Commerce (ICC) policy on B2C ADR in electronic commerce. The presentation will be based on a position paper, under formulation by the ICC, on ADR in B2C transactions. The position paper is intended both to identify some of the salient policy principles that the ICC believes should govern this area, and to provide an outline of the concrete actions the ICC could take to become involved in it.

Suggested questions:

What are the experiences of users and consumers when using ADR mechanisms? Are there particular types of disputes that are not conducive to resolution through online ADR? Are there categories of disputes that would better be resolved through the use of a particular type of online ADR? Other questions may be based on appendixes A and B (list of online ADR mechanisms and list of possible procedural and substantive elements that exist in ADR mechanisms).

Day 2: Reaching effective online ADR at a global level

Building on the presentations from day 1, the discussion will explore the various challenges to be addressed to facilitate B2C ADR at both national and global levels, as well as incentives and disincentives for businesses, consumers, and governments to participate in and/or encourage the use of ADR. Session 5 will focus on the challenges to online dispute resolution, including identifying important elements for fair and effective online ADR mechanisms. Session 6 will focus on the role of stakeholders in promoting fair and effective ADR, ensuring compliance and enforcement, and educating all stakeholders.

Introductory remarks by Day 2 Chair

Jytte Oelgaard, Chair, OECD Committee on Consumer Policy

Session 5: Challenges to online dispute resolution

Awareness of the potential legal and other barriers arising from resorting to courts in disputes resulting from cross-border online interactions is widely shared: which law applies, which authority has jurisdiction over the dispute, which forum is competent to hear the dispute, is the decision enforceable across borders? Another legitimate concern, though less legal in nature, is related to the cost of court proceedings, which may exceed the value of the goods or services in dispute, or the length of the procedure, which may be far slower than "cyber-time".

This session will explore and discuss the variety of possible challenges to the effective use and implementation of online ADR, either socio-economic (including linguistic and cultural), legal (including last resort principle) and technological (including security). While discussing these challenges, participants may recognise the need for common ground among stakeholders on essential elements that should be in any fair and effective online ADR for B2C disputes, including: *i)* Transparency, *e.g.* information on the ADR procedure, its cost, and other important features should be made readily available to all parties before entering into an ADR process; *ii)* Accessibility; *iii)* Free or low cost to the consumer; and *iv)* quick decisions.

I. Socio-economic issues related to online ADR

"Behind their screens there are people of all nationalities, all ethnic-cultural groups, social classes and professions, of all religions and political convictions, of all ages and life-styles, of both sexes who together, but also among themselves show a rich diversity of preferences and disfavours, expectations for the future and fears, likes and dislikes."[17] This quotation illustrates how challenging the global online environment is in its sociological dimension, in particular when it comes to B2C interactions. Like the legal and technical issues, sociological and economic factors must be explored to better understand how they can affect the use and implementation of online ADR.

This session will discuss some of the socio-economic challenges, including how cultural, linguistic and economic differences might affect the effectiveness of ADR systems; or similarly, how differences in information and expertise might affect the use and implementation of ADR, while considering that online means of communication (digitalised texts, sounds, stationary or moving images) affect methods of work, cultural patterns and life-styles[18].

Moderator: Anna Fielder, Director, Consumers International

Panellists:

Giles Buckenham, Administrator, Directorate General for Health and Consumer Protection, European Commission

Scott Cooper, Manager of Technology Policy, Hewlett-Packard

Carmen Fernandez Neira, Chairman, Internet Working Group, European Advertising Standards Alliance (EASA)

William Marsh, Director, CEDR

Toh See Kiat, Partner, Tan Peng Chin and Partners

Presenters:

Nora Femenia, Professor, and Vice President, OnlineDisputes.org, will discuss how online dispute resolution techniques and the global management of customers' complaints could be responsive to different social and cultural environments. She will focus on culturally different approaches to customer complaints, the impact of community pressure on conflict solving, and what would be the role of computer-assisted negotiation techniques in furthering public education on legitimate ways of solving online transaction problems.

Christopher Drahozal, Professor, University of Kansas School of Law will offer an economic perspective on various questions relating to the fairness of online ADR, including: why do parties use ADR in the first place? Should ADR mechanisms replace access to the courts? How do the incentives of stakeholders and of the neutral affect the use and implementation of ADR? and how differences in resources and information between businesses and consumers may raise concerns about whether online ADR mechanisms will be fair.

Suggested questions:

How do linguistic and cultural differences affect the use and implementation of ADR? Should users and consumers be offered to interact in their own language during ADR? How do economic differences affect the use and implementation of ADR? Are there ways to level the imbalances in information and expertise among the parties? Should training of neutrals include education on socio-economic related issues?

II. Legal issues related to online ADR

Legal issues are related to making the ADR process fair and effective for both consumers and businesses. This session is expected to highlight those procedural and substantive elements considered as essential to ensure a fair and effective ADR process, while recognising that these elements may vary depending on the type of ADR and/or dispute.

During the discussion, participants may recognise the need for common ground on issues such as: i) Whether providers of ADR for online B2C disputes should be independent; ii) Whether ADR intermediaries should be neutral or impartial in their decision making, and have sufficient skills and training to fulfil the dispute resolution role in an appropriate manner; iii) Whether consumers should be permitted to choose between ADR and traditional legal mechanisms. i.e. should recourse to ADR be voluntary or could it be mandatory; iv) Whether parties should have representation or v) Whether the procedure should be adversarial.

Other issues to be discussed include whether current legal systems pose barriers for consumers to use ADR or prevent businesses from implementing outcomes, rendered under ADR, to which consumers have fully agreed. In addition to the more procedural questions, an important issue to be examined is what substantive principles might be applied to resolve an online cross-border dispute. [19]

The issue of whether the outcome of the ADR process should be binding or non-binding may also be discussed. While this is an important issue, participants will be reminded that the focus of the Conference is primarily on the more flexible and informal ADR systems.

Moderator: Mozelle Thompson, Commissioner, US Federal Trade Commission

Panellists:

Matthias Blume, Austrian Ministry of Justice

Eric Ducoulombier, Administrator, Directorate General for Internal Market, European Commission

Marco Gasparinetti, Data Protection Commissioners' Office, Italy

Michael Geist, Professor, University of Ottawa Law School

James Murray, Director, *Bureau Européen des Unions de Consommateurs*

Ron Plesser, Partner, Piper Marbury Rudnick & Wolfe, and Co-ordinator, Electronic Commerce and Consumer Protection Group

Presenters:

Philippe Fouchard, Professor, University Paris II will discuss the fundamental legal elements that are necessary for online ADR to be fair and effective for users and consumers. He will focus on online ADR mechanisms where parties participate voluntarily and agree upon the outcome at the conclusion of the process.

Christopher Kuner, Of Counsel, Morrison & Foerster, LLC will present an overview of the main conclusions of a study on legal obstacles to business-to-consumer ADR in electronic commerce in Europe. The study was commissioned last spring by the Global Business Dialogue in response to the uncertainty and confusion related to the legal framework for B2C ADR in Europe.

Suggested questions:

How might national or international laws and related public policy issues affect the use or implementation of ADR? (e.g. non-waivable rights, differences in substantive law, or procedural rules related to ADR). How do the legal rules affect the availability of out-of-court dispute resolution?

III. Last Resort Principle and Juge d'appui *("support judge")*

This session will focus on the intersection of online ADR with the jurisdictional framework.

It is expected that business internal complaint handling systems and online ADR mechanisms will succeed in resolving most disputes that arise from B2C online interactions. However, in cases where the alternative mechanisms fail, recourse to court might be necessary. Furthermore, as used in arbitration, recourse to a judge (*juge d'appui)*[20] in the course of the ADR may be helpful to solve a difficulty (*e.g.* the service provider disappears during the procedure, or there is a serious violation of the principles of independence and impartiality) and to facilitate a successful and smooth process. The discussion will include an exploration of the applicability of traditional notions of jurisdiction (competent forum), related enforcement issues, and a review of existing solutions and proposals for new ones. It will also explore the practicality and possibility of adapting the concept of the *juge d'appui* to less formal online ADR processes.

Moderator: Catherine Kessedjian, Professor, University of Paris II, and former Deputy Secretary General, Hague Conference on Private International Law

Panellists:

Katharina Boele-Woelki, Professor, University of Utrecht

Giacinto Bisogni, National Expert, Legal Service of the European Commission

Asunción Caparrós, Manager, European Affairs, ABN Amro Bank

Roger Cochetti, Senior Vice President and Chief Policy Officer, Network Solutions

David Goddard, Barrister, New Zealand Law Commission

Pippa Lawson, Counsel, Public Interest Advocacy Centre

IV. Technological issues and trends affecting online ADR

Current developments in technological applications and practices as well as the growing interoperability of systems have an impact on the development of online ADR mechanisms. The continuous technical innovation in the Internet environment is therefore worth discussing in relation to online ADR. This session will highlight technologies already in use or under development with a view to how they can be used to facilitate online B2C dispute resolution. For example technologies used for secure electronic signature and authentication[21], or encryption of content messages may help ensure confidentiality and integrity of the process and the information exchanged. Furthermore, interactive technologies like video-conferencing may bring the parties together, moving them from behind their computer screens to a virtual setting making the experience a face-to-face interaction. Similarly, automatic translation and voice recognition may help bridge some cultural differences.

During the discussion, participants may also examine the need for common ground on issues related to the security of online ADR systems and to the confidentiality and integrity of the process and the information exchanged.

***Moderator*:** Wibo Koole, Head of Consumer Policy, *Consumentenbond*

Panellists:

Sarah Andrews, Policy Analyst, EPIC/Privacy International

Peter Lübkert, Information Technology and Networks, OECD

Marc Wilikens, Joint Research Centre, European Commission

Presenters:

Joseph Alhadeff, Vice President for Global Public Policy, Oracle, will present the policy-side of the technological issues and challenges related to ensuring effective online ADR for B2C dispute resolution.

Chris Lynn, Legal Associate, Microsoft Europe, Middle East and Africa will present the various advances in software technology that will make resolving basic consumer disputes in the B2C sector more effective.

Suggested questions:

How will technological innovation assist to remedy these challenges? How can technological interoperability be ensured? Can technological innovation bridge cultural and other sociological differences between the parties?

Session 6: The roles of stakeholders

Most stakeholders agree that online alternative dispute resolution (ADR) can be very helpful to both parties in electronic interactions or transactions, especially in cross-border disputes. They see incentives for fostering ADR, whether economic (*e.g.* reducing costs), legal (*e.g.* helping obviate the very perplexing issue of competent forum, because with online ADR, the forum will no longer be tied to a geographic location but rather it will be virtual,), or more sociological (*e.g.* improving confidence, and bridging cultural differences). Potential negative impacts have also been highlighted such as lack of consumer choice, disparity between the parties (*e.g.* lack of information, education, and resources) or possible lack of enforceability of decisions.

Based on previous discussions, this final session is expected to highlight common stakeholder views on a number of socio-economic, legal or technological elements that should be in any fair and effective online ADR for B2C disputes, and to focus on how best to foster their implementation through exploration of two main policy areas.

The session will therefore be divided in two discussions. The first will be devoted to the roles of stakeholders in relation to promoting essential elements for online ADR (regulation, self-regulation or integrated approach), and ensuring compliance (public and private sector trustmark programmes). The second discussion will focus on providing effective education about ADR.

This session is expected to highlight the need for complementary approaches among the stakeholders that effectively balance the interests of individuals and business, while exploiting particular stakeholder expertise where available.

Moderator: Arie J.M. van Bellen, Managing Director, Electronic Commerce Platform Nederland

Panellists:

Roger Cochetti, Senior Vice President and Chief Policy Officer, Network Solutions

Susan Grant, Director of National Fraud Information Center, National Consumer League

David Mair, Administrator, Directorate General for Health and Consumer Protection, European Commission

Rebecca Richards, Director of Policy and Compliance, TRUSTe

Yuko Yasunaga, Deputy Director, Commerce Policy Divisions, MITI Japan

*I. Promoting fair and effective online ADR and ensuring compliance (***e.g.** *trustmark programmes)*

As discussed in session 1, a variety of stakeholders have developed principles for B2C ADR systems or expressed views on essential elements of such ADR systems. This session will further discuss the roles of stakeholders in relation to promoting fair and effective B2C online ADR. This will include discussing how the stakeholders should co-operate to identify essential elements for online ADR (*e.g.* who should sit at the table? should there be separate recommendations by different stakeholders, as is the case to date? where should guidance for ADR be identified – *e.g.* in regulation or codes of conduct). It will also include how the stakeholders can work together to ensure compliance with these elements**.**

Among other complementary measures to ADR, online trustmarks and seals programmes are worth exploring as they may have a positive impact on the issue of compliance, and encompass approaches that may be considered both by the private sector and governments. There is ongoing discussion among stakeholders on if and how trustmark/seal programmes could be designed to render fair and effective online ADR systems, how compliance with such programmes could be ensured, and how decisions rendered by ADR systems could be enforced under such programmes.

Presenters:

Naoshi Shima, Vice President, Business Development, NEC will provide background on how the GBDe successfully co-ordinated its recent recommendations on B2C ADR. As the principal organiser for the GBDe's work in the Asia/Oceanian region, on behalf of NEC, Mr. Shima will begin with a closer look at the Asian experience with regards to resolving disputes that arise online among consumers and business.

Barbara Wellbery, Partner, Morrison & Foerster LLC, will explain the US self-regulatory approach as it relates to privacy and consumer protection, with emphasis on online ADR. She will also describe how self-regulation fits within the broader US framework for promoting consumer and business trust in e-commerce, which includes a complementary mix of industry mechanisms, government initiatives and law enforcement efforts.

Martin Bond, Assistant Director, Department of Trade and Industry, United Kingdom will present how government, traders, and consumer organisations in the UK came together to develop the TrustUK program. The presentation will include how the program was developed, how it works, and where ADR fits into the system.

Malcolm Crompton, Data Protection Commissioner, Australia, will focus on online seal programs. He will present the findings of a review of Online Privacy Programs conducted in September 2000 by his Office and the Office of the Information and Privacy Commissioner/Ontario. The project identified three key components for an effective online seal program, including sufficient privacy principles, sound dispute resolution method, and a robust compliance mechanism.

Suggested questions:

Is convergence of stakeholders in defining essential elements for promoting fair and effective online ADR desirable? Who should participate as stakeholders? What are the roles of stakeholders in developing trustmark programmes and codes of conduct, common complaint systems and ensuring enforcement? How can stakeholders co-operate best to develop such programmes and systems for cross-border transaction?

II. Educating business, consumers and government about online ADR

Cross-border ADR is common in the B2B context, but is new in the B2C context. While it is expected that online ADR will be effective in resolving B2C disputes in the online environment, it is important to recognise that users' and consumers' knowledge and understanding of ADR is minimal. Recognising the need for education, this session will focus on the roles of various stakeholders in educating businesses and consumers about online ADR. In particular, the discussion will include effective approaches to educating business about offering ADR and to educating consumers about the nature of and procedures for fair and effective ADR.

Presenters:

Duncan McDonald, American Institute of Contemporary German Studies, will explain how transparency through conspicuous online disclosures in plain language and multiple languages minimises consumer confusion and distrust, adverse media attention, and government scrutiny and enforcement.

Francis Aldhouse, Deputy Data Protection Commissioner, United Kingdom, will explain how the UK Data Protection Commissioner supports good customer care systems, ombudsman schemes, sectoral dispute resolution arrangements and other examples of ADR, and uses formal advertising and PR techniques to alert individuals to their legal rights and encourage them to pursue their own remedies and assert their own privacy.

Suggested questions:

What are the roles of stakeholders in educating business, consumers and government about online ADR? What can stakeholders do to ensure overall participation in ADR? What are the incentives and disincentives for the different stakeholders to promote online ADR?

Conference concludes

The conference will conclude with brief highlights of the conference discussions.

Report on the conference

Main points

Need for strong co-operation between stakeholders, and flexibility in ADR mechanisms

The Internet is global and borderless. Efforts to devise online ADR mechanisms must take into consideration the voices of all stakeholders – be they governments, businesses, or consumer groups. In the same respect, any mechanisms for online ADR must have flexibility as a key principle to allow for differences between nations and cultures and to respond to the variety of disputes that can arise. ADR can provide fair and effective redress for users in the online environment. More generally, effective online ADR can help to foster the sense of trust between Internet businesses and users and consumers, necessary for the continued growth of e-commerce.

Common elements have emerged for ADR principles

Not one size fits all in terms of ADR and differing situations (in value or in complexity, for example) may require differing approaches. At the same time, some common principles have emerged among government, industry, and consumer groups for approaches to fair and effective ADR including: accessibility, low cost for consumers, transparency (*i.e.* providing information that is essential for consumers to make an informed choice about the ADR mechanism), reaching decisions quickly, addressing culture and language differences in the ADR process, and impartial and qualified intermediaries to conduct ADR.

Differences have come into focus

Three areas requiring further debate among stakeholders are particularly clear. First, stakeholders disagree as to whether there are situations where it should be mandatory for consumers to engage in an ADR process before going to litigation. Second, stakeholders disagree as to whether online ADR resolutions should, or even could, be binding on parties. Third, stakeholders need to further explore what are the most effective means to ensure compliance with, and enforcement of, ADR processes and outcomes.

Growing number of users and consumers complaints in relation to e-commerce

The number of privacy and consumer related complaints with regard to the Internet is increasing each year. The most common consumer complaints with regard to e-commerce include the failure of merchants to deliver goods on time, if at all, non-disclosure of charges/costs and insufficient information on product attributes, and inadequate complaint handling. Privacy complaints mainly focus on data collection without consent, use of data different from original purpose of collection, selling data to third parties, unsolicited commercial e-mail, identity theft, providing credit history without consent, and children's privacy online. Complaints by consumers in one country about merchants in another are just beginning.

Consensus that disputes should be settled at the earliest stage

Global business-to-consumer disputes should be resolved as quickly as possible for the benefit of all parties involved. The first step toward resolving disputes online is to avoid them. To this end, businesses should provide effective and efficient customer service and internal complaints handling systems. "Chargebacks" and other consumer refund mechanisms are also positive, even if limited in

scope. In general, online customers have high expectations for response times from online companies. Good handling of customer complaints dramatically increases customer loyalty.

Just as complaints including a fraudulent element may not be conducive to ADR, not all online ADR programs may be suited to resolve all privacy and consumer related disputes

There is a range in online ADR programs from the fully automatic at one end to a formal arbitration setting at the other. It is recognised that each point along that spectrum has both advantages and disadvantages for consumers and businesses alike. While not every mechanism is appropriate for every dispute, the development of a wide variety of mechanisms can help address the breadth of disputes; such variety is enhanced by healthy competition among mechanisms. Practical guidance and sufficient information should be made available so that parties can make appropriate choices about dispute resolution mechanisms.

Socio-economic and cultural barriers persist

ADR providers and related service providers should work to make ADR truly accessible to all. Many socio-economic and cultural barriers exist as challenges to implementing fair and effective systems of online ADR on an international scale. In particular, linguistic barriers are a frequent problem, as are differences in how cultures approach disputes and disagreements. It is important that ADR services be sensitised and responsive to these issues.

Technology can advance online ADR, but also presents a paradox

Advances in such fields as computer languages, enhanced videoconferencing, translation, speech recognition and broadband access technology may facilitate some online ADR mechanisms, and bring the parties to a nearly equivalent face-to-face relation. However, where some users may find synchronous (*e.g.* face-to-face) resolution mechanisms more desirable, asynchronous communication may provide a party the advantage of longer deliberation on a response.

Debate continues over the possible roles for judges during the ADR process as well as of last resort

The conference reviewed four situations related to judicial involvement in the context of ADR: *i)* As enforcement authority since courts have the exclusive exercise of coercive powers; *ii)* As a judge of last resort; *iii)* As a *juge d'appui*, in cases of binding arbitration; and *iv)* In the enforcement of a settlement agreement. There appears to be little support for involving a judge (*juge d'appui*) in the course of a non-arbitration type online ADR process because it could jeopardise the principle of having an informal process and making it economical for both parties.

Now may be the right time for stakeholders to join forces

All stakeholders independently have issued principles, recommendations and guidance on ADR. While areas of divergence still exist, there are many areas of common ground. There is agreement that stakeholders should work together to continue to find more common ground to ensure fair and effective online ADR mechanisms to resolve B2C privacy and consumer-related disputes.

Day 1: Overview of ADR in relation to the online environment

The conference was opened by Peter Ford, Chair of the Working Party on Information Security and Privacy of the OECD and Jytte Oelgaard, Chair of the Committee on Consumer Policy of the OECD.

Welcome and keynote

A.H. Korthals, Minister of Justice, The Netherlands, discussed electronic commerce generally and then recalled the fundamental tension between nationally oriented governments and their related legal systems and the borderless nature of the Internet. Mr. Korthals proposed four questions for the attendees to consider: *i)* At which level and in which form should regulation take place? *ii)* Should the same norms and values apply online and offline?; *iii)* Is it possible to clearly determine what aspects of private international law are involved?; and *iv)* How can laws be enforced in the context of a borderless world? He pointed out the advantages of ADR as a way for speedy, efficient resolution of disputes that helps overcome the issue of jurisdiction, and suggested that a digital form of mediation, a means through which both parties voluntarily commit themselves to the outcome, may be the best option.

Herwig Schlögl, Deputy Secretary-General of the OECD stressed that this broad, international conference was the first of its kind to discuss online ADR issues, and in keeping with OECD practice, to bring all stakeholders to the table. Mr. Schlögl recalled that in terms of micro-economics, the "electronic" economy has, since 1995, fundamentally changed how business is done, and will continue to change how the markets function in the future. He offered some compelling figures to illustrate the growth of online trade.

Mr. Schlögl discussed the OECD's work on electronic commerce policy and referred to the 1998 Ottawa Ministerial conference and the OECD's current programme of work in the areas of privacy and consumer protection. He highlighted that building trust is an important policy issue related to the new economy and global information society. In particular, he stressed that a key element to building trust is ensuring users and consumers effective redress for disputes arising from interactions and transactions in the online environment. However, for online ADR to reach its potential, particularly for settling cross-border B2C disputes, the complex legal issues and equally complex technological ones must be addressed; to this end, he encouraged participants to utilise the range of expertise to find practical solutions in this area.

Maria Livanos Cattaui, Secretary General of the International Chamber of Commerce offered the perspective of the global business community and the ICC, which, for 80 years, has been a pioneer in the field of commercial dispute resolution. She said that all stakeholders have a distinct role to play in establishing effective ADR around the world, and that building partnerships among stakeholders ready to commit time and effort is the most crucial step toward this end.

Mrs. Cattaui outlined the distinct roles of the various stakeholders. She stated that governments can contribute political strength and a common forum, but must not limit the benefits of ADR. Accreditation or approval must neither be mandatory nor exclusive of international self-regulatory principles and rules, and must embrace transparency and openness where offered. Governments should actively promote ADR as an alternative to court-based methods. Governments must not allow obstacles to innovation to appear, especially in terms of online confidentiality and security. Finally, they must give equal consideration to the efforts for all stakeholders.

Mrs. Cattaui suggested that the world business community should provide resources to promote ADR but must remain flexible to the needs of consumers and responsibilities of governments in their approaches. This includes ensuring that consumer complaints are handled thoroughly by the business itself before they are referred to an ADR mechanism. It also means that companies should be prepared to co-operate with consumers from any place on the map, any culture, and in any language.

Civic organisations, including consumer representatives, must be attentive to the needs of their constituents, and must communicate to them that ADR is here for their benefit, that it is cost efficient, and that it is fair. They must recognise that government is there to ensure that both parties ultimately gain from using ADR. Today's ADR providers are pioneers and must therefore remain flexible when recognising consumer choices, and must manage procedures and decisions in such a way that consistently ensures impartiality, accessibility, convenience and transparency. It is also their responsibility to bridge cultural and linguistic gaps. The burden of efficiency ultimately falls on ADR providers, as it is to them that businesses and consumers entrust the resolution of their disputes.

Finally she stated that businesses, governments, ADR providers and civic organisations alike must not succumb to fears about addressing sensitivities of ADR, as this is counterproductive.

Hans van Loon, Secretary General of the Hague Conference on Private International Law stressed the importance of co-operation among interested parties on a topic such as online ADR, which is trans-national and affects both the industrialised world and developing countries.

Mr. van Loon drew a distinction between the technological and economic environment, which is truly global, and the legal environment, which is a patchwork of national, sometimes regional issues. He stressed that against such a background, the challenge is to build bridges to cope with diversity. He stated that it was necessary to provide an ordered system for access to national courts and to facilitate court conclusions, and he described the work of the Hague Conference to these ends. He said that it was also equally important to promote ADR and to provide citizens with precise rules stating exactly what occurs if agreement is not reached. Mr. van Loon commented that there is a future for trans-national ADR, interfaced with rules on appropriate law and uniform policies, but that the major challenge is to find a formula creating room for ADR on the one hand and adjudication on the other.

Session 1: Taking stock – overview of recent discussions about online ADR

Focus: In an effort to provide a forum, at a global level, for exploration of ADR and to foster co-operation among the stakeholders, this session aimed at taking stock of the work undertaken on online ADR by other fora. The session was expected to outline similarities and differences in the various approaches to date in order to identify challenges to be met and gaps to be bridged in terms of essential elements for fair and effective online ADR.

Risaburo Nezu, Director, Directorate for Science, Technology and Industry, OECD, opened the session by stressing that it was important to get a general understanding about common ground and principles for ADR mechanisms as well as an awareness of the remaining issues to be further discussed.

Carina Törnblom, Head of Unit, Directorate General for Health and Consumer Protection, European Commission (EC), gave an update of activities taking place in the European Union to advance effective dispute resolution for B2C transactions. She explained that the EC, in co-operation with business and consumers, has first focused on preventing consumer problems, and encouraging the use of best market practices. The EC has also discussed practical alternatives to going to court, codes of conduct for trustmarks programs and credit card chargeback mechanisms.

Ms. Törnblom highlighted the concern that the rapid proliferation of codes of conduct make it easy for a business to assert that it adheres to a code of conduct, but might leave in question the quality of the code and the issue of compliance. To this end, she stated that European Member States need to establish certain common criteria and a basis for approval of codes of conduct; she gave the example of the 1998 Recommendation on Out-of-Court Dispute Settlement Bodies, produced by the EC. She said that the Recommendation had been quite successful and Member States had already notified the Commission of which bodies meet the criteria prescribed by the Recommendation.

Ms. Törnblom also discussed the European Extra Judicial Network (EEJ Net), a European-wide system of clearinghouses for consumer complaints, which should be established by summer 2001. As to other work on ADR, she explained that the EU is considering adding rules to the regulations governing the functioning of mediators and facilitators. Finally, Ms. Törnblom stressed the importance of allowing consumers to have access to their own legal system while at the same time working to prevent the need to go to court by providing voluntary access to ADR.

James Dorskind, Acting General Counsel of the US Department of Commerce shared some observations from a workshop on ADR for online consumer transactions held in June 2000 by the Department of Commerce and the US Federal Trade Commission. He stressed that what works in a B2B environment may not necessarily work for B2C. For ADR to be useful in the B2C context, it must be practical for consumers to use as well as effective in protecting their information. He also referred to other means of resolving disputes such as credit card chargebacks. Mr. Dorskind explained that different kinds of businesses may approach ADR in different ways; for example, smaller companies may have a greater need to use a third party provider than larger companies. In addition, the best approach for resolving a dispute is likely to vary depending on the value of the transaction, or the complexity of the dispute. He described some general principles for ADR that emerged as a result of the discussions at the US workshop, adding that it is too early to define these in detail. They include: impartiality, accessibility, low or no cost to the consumer (relative to the amount in dispute), transparency (*i.e.* consumers should have information about the mechanism before they are asked to make a decision about entering ADR), timeliness, and speed. He mentioned that there is little consensus among stakeholders about whether or not ADR should be binding.

Mr. Dorskind expressed that in order to promote consumer confidence, global and seamless ADR mechanisms must be achieved. To this end, the Department of Commerce is working with the EU to encourage development of ADR mechanisms by the private sector and in response to market developments. He stressed that all stakeholders should participate in these discussions to ensure fair and effective mechanisms. In addition, Mr. Dorskind explained that the problems of applicable law must be addressed at the international level, as ADR must work well across different national and legal cultures.

Yuko Yasunaga, Deputy Director, Commerce Policy Division, Japan Ministry of International Trade and Industry, followed with an overview of the experience of APEC in relation to consumer protection and ADR. He described the establishment of the E-Commerce Steering Group (ECSG) of APEC and the 1998 APEC Blueprint for Action, which charged business to take a leading role in developing e-commerce, and governments to provide a favourable environment for the growth of e-commerce. He discussed the Consumer Protection Workshop, held by the ECSG in Bangkok in July 2000. The workshop demonstrated the need for greater co-operation and collaboration among stakeholders in the region as a way to overcome the uneven situation that exists among APEC economies regarding laws, rules, practices, information availability, and education in relation to e-commerce. Workshop participants agreed to share information about consumer protection laws and regulations, and to look for ways to increase law enforcement co-operation.

Mr. Yasunaga illustrated several "Best Practice Models" for building consumer confidence online, being undertaken by APEC economies, including Australia's codes of conduct initiatives, Japan's Online Shopping Trustmark program, and Singapore's CaseTrust, a government-led dispute consultation program. He offered an example of joint co-operation in Asia, describing talks between Japan and Korea regarding accreditation and mutual recognition of trustmarks, and the July 2000 APEC/ECSG workshop on consumer protection in Bangkok. Mr. Yasunaga stressed that online ADR is still at the beginning stages in APEC, and that private sector initiatives must be the primary driving force behind the use of such mechanisms; he added, however, that governments also have a role to play. He said that governments should encourage the use of clearinghouses, for example, and other appropriate solutions to foster use of and adequate information about ADR.

Constanze Picking, Senior Manager Trade and E-Business at Daimler Chrysler AG, discussed the views of the Global Business Dialogue on E-Commerce (GBDe). She outlined GBDe's work on ADR during 2000, including efforts by each regional working group (Europe/Africa, the Americas and Asia/Oceania) to conduct an inventory of online ADR mechanisms within the region, as well as numerous workshops and meetings with stakeholders.

Ms. Picking described the GBDe paper on online ADR programs prepared for their annual conference in September 2000. The paper makes recommendations to Internet merchants, ADR service providers and governments on best approaches for developing online ADR. The GBDe recommends that Internet merchants encourage the use of in-house customer satisfaction programs and inform consumers about the possibility and conditions of using ADR. For service providers, the GBDe specifies that ADR mechanisms should be impartial, accessible and convenient, speedy, low cost to the consumer, transparent, allow for an adversarial procedure, and ADR officers should be adequately qualified. Furthermore, ADR mechanisms should allow parties to be represented and should specify applicable rules for the procedure. ADR providers should also promote consumer awareness of online ADR. Finally, GBDe recommends that governments finalise international rules on competent forum and applicable law; encourage the use of customer satisfaction programs; not discriminate between different ADR systems; not establish mandatory criteria or accreditation systems for ADR, and allow the possibility for binding arbitration in B2C disputes in certain cases.

Ms. Picking described several open issues that are still under discussion by GBDe members, such as certification of ADR systems and accreditation of certification bodies. Among GBDe's next steps in this area will be to create a consumer confidence Web site, establish ADR clearinghouses, and hold discussions with consumer representatives.

Louise Sylvan, President of Consumers International said that there were many areas of commonality and agreement between Consumers International principles for online ADR and those provided by GBDe, the EU and the TACD. She presented a summary of the Consumers International study of online ADR providers, released on 11 December 2000. The study rated 30 online ADR programs against eight criteria, including independence/impartiality, transparency, availability, affordability, effectiveness, fairness (due process), legality/liberty, and third party oversight. The results of the study concluded that none of the 30 programs met all the criteria, although most were easy to find, timely, easy to use and described the procedure adequately. Ms. Sylvan cited a number of shortcomings with the mechanisms: many were limited in their ability to resolve disputes in multiple languages, most were disproportionately costly, and few reported the results of ADR transparently. She stated that the study shows that there are problems with enforcement of ADR decisions and that ADR is suffering from a proliferation of programs that will confuse consumers. In addition, consumer interests do not have the same level of representation in the programs' governance structures as business interests.

Ms. Sylvan offered a number of recommendations for online ADR programs, based on the study. Mechanisms need to cater to non-English speakers and should report decisions more transparently. In addition, costs of ADR to consumers can not be higher than most B2C disputes, and inappropriate mandatory ADR and binding arbitration clauses need to be eliminated. She concluded that global standards are needed for online ADR as well as ongoing independent oversight.

Mr. Nezu summarised the discussion by saying that while it is clear that not one size fits all *vis-à-vis* ADR programs, the discussion helped identify some common elements for ADR mechanisms and approaches to developing such mechanisms, including the need for:

- Strong co-operation amongst all stakeholders.
- Transparency (*i.e.* providing information that is essential for consumers to make an informed choice about the ADR mechanism).
- High quality accessibility to permit consumers to use the ADR systems at low cost while striking a balance between the cost of ADR and the benefit to the consumer.
- Addressing culture and language differences in the ADR process.
- Reaching decisions quickly.
- Impartial and qualified intermediary to conduct ADR.

Mr. Nezu added that none of the existing online ADR mechanisms (most of them very recently set up) meet all of the above elements and therefore the systems still need further improvement. Regarding future work in this area, he stressed that several thought that a clearinghouse to facilitate the sharing of information would be beneficial. He also identified two outstanding issues that deserve further discussion: *i)* Whether recourse to ADR should be voluntary or could be mandatory, and whether the outcome of the ADR process ought to be non binding in nature or could be binding; and *ii)* The need to clarify what is ADR and to differentiate between the ADR process and the court process.

Session 2: Illustrating possible B2C complaints in the online environment

Focus: This session was intended to provide information and statistics on the types and volumes of complaints received from users and consumers in relation to their interactions and transactions online in order to educate all stakeholders on where to focus their efforts in exploring redress mechanisms and discussing online ADR mechanisms.

Michelle Childs, Head of Policy Research for Consumers Association, United Kingdom gave an overview of the Web Trader seal program, a European partnership of consumer organisations in seven countries. Currently, 1 500 member companies hold the seal. The scheme is one of adherence to a code of practice that requires traders, for example, to give the consumer clear and inclusive prices, provide refunds within a maximum of 30 days, maintain a secure site, and a have in place a complaint handling procedure. There are strict pre-entry conditions for merchants, and there is ongoing monitoring of compliance with the code.

The Which?Web Trader program also collects consumer complaints. As of November 2000, the two largest areas of complaints were failure to deliver goods on time (226 of more than 740 total complaints) and inadequate complaints handling (107 of more than 740 total complaints). In the event of a consumer dispute, the code requires the consumer to contact the trader first. If the trader does not adequately respond in five days, Which?Web Trader intervenes. Outcomes suggested by Which?Web

Trader are binding on the trader. Which?Web Trader does not presently provide cross-border dispute resolution services, and is seeking EU funding in order to expand this service.

Stephen Lau, Privacy Commissioner for Personal Data, Hong Kong, China, outlined the main threats to data privacy on the Internet against Hong Kong's Personal Data Ordinance. The privacy Ordinance establishes six principles for data protection, covering purpose and manner of personal data collection, accuracy and duration of information retention, use of personal data, security of personal data, information on data held and purpose of use, and access to personal data by data subjects. The main complaints which were received by his office include data collection without consent, identify theft, interception of data during transmission, and use of data different from original purpose of collection.

Mr. Lau then summarised the results of a sample survey of 531 Hong Kong Web sites conducted between July and October 1998 in order to measure compliance with the Ordinance and standards of good and reasonable personal information handling. The study concluded that in 1998 only 6.2% of sites with online personal data collection forms displayed a privacy policy statement. That figure increased, he said, to 25% in 1999. Formal investigations are being conducted against 16 sites with personal data collection forms that are lacking a personal information collection statement. The Privacy Commissioner's office has since published guidelines on protection of privacy and privacy policy statements for individual net users and data users as a way to promote awareness of good online privacy practices, and thus diminish the risk of breaches of privacy.

Maneesha Mithal, Attorney with the Consumer Protection Bureau of the US Federal Trade Commission (FTC) provided an overview of the Consumer Sentinel Database, a joint project of the FTC and Industry Canada. Consumer complaints are fed into the database from both public and private sources and government users can review specific complaints, and general complaint trends. Internet-related complaints have increased dramatically over the past three years, more than doubling each year from 872 in 1997 to 7 955 in 1998 and to 18 622 in 1999. At the same time, the proportion of Internet-related complaints in the database also consistently has grown, from just 3% in 1997 to 11% in 1998 and to 22% in 1999. In the last year, 10% of the complaints involved US consumers and foreign companies while 2% involved foreign consumers and US companies. The FTC has seen a rise in the past three years in the numbers of Internet-related complaints regarding breach of warranty and the mail order rule. Ms. Mithal also described some of the more common privacy-related complaints made by consumers such as unsolicited commercial email, identity theft, harassing phone calls, providing credit history without consent, selling data to third parties, and children's privacy. Finally, she mentioned that complaints including a fraudulent element may not be conducive to ADR.

Marcie Girouard, Assistant Deputy Commissioner of Industry Canada, illustrated the volume and types of e-commerce complaints filed by consumers with the Canadian government, mentioning that consumer trends in Canada lag behind the United States by two years. In the first three-quarters of 2000, complaints about activities on the Internet accounted for 2.2% of overall complaints filed with Industry Canada. Of these Internet complaints, 17.4% were based on e-commerce-related transactions. The most common areas of e-commerce complaints were non-delivery of goods, time for delivery, non-disclosure of charges/costs, product attributes, and retail versus online pricing. An increasing number of complaints were against Web sites established outside Canada.

Ms. Girouard also described Industry Canada's recent review of 292 Web sites, comparing them against selected criteria set forth in the *1999 OECD Guidelines on Consumer Protection in the Context of Electronic Commerce*. Among the results were that 77% of merchants disclosed full purchase cost and 52% described the return/exchange policies; 26% of merchants provided consumer complaint procedures and only 16% described dispute resolution mechanisms. As a result of Industry Canada's

complaint database and the Web site review, she concluded that consumer issues are multi-jurisdictional, that consumers using the Internet report a range of complaints, and the ADR mechanisms are not yet widely available.

Session 3: Dispute resolution at the earliest stage – internal complaints handling and customer refunds

Focus: This session was intended to examine the scope of application and effectiveness of internal customer complaint handling systems and customer refunds (as a result of chargeback systems) to resolve complaints and disputes that arise in the B2C online environment.

Hugh Stevenson, Associate Director, Bureau of Consumer Protection at the US Federal Trade Commission, served as moderator for Session 3.

Charles Underhill, Acting Chief Operating Office at the Council of Better Business Bureaus, provided an overview of the customer complaint handling activities of the BBB and some general observations about internal complaints handling. BBB's AutoLine program, which handles consumer automobile disputes, received nearly 33 000 complaints during 1999. A significant number of these complaints were settled by the merchant before the consumer filed a formal case. BBB handled most of the remaining cases through a process of mediation. Also in 1999, local BBB offices throughout the United States and Canada received more than 3 million requests for complaint assistance from consumers. The BBB resolved 66% of these.

Mr. Underhill described a recent survey conducted by e-Satisfy of customer service by e-commerce site. The study showed that online customers have higher expectations than offline customers for response time from companies. Poor handling of online contacts create at least 30% lower customer loyalty among the two-thirds of online contacts that are not satisfied. He said that BBBOnLine is helping to promote better business practices by online merchants through its new Code of Online Business Practices, approved in May 2000. In addition, BBB has entered into an alliance with Visa USA to educate the US online merchant community about the Code and security and data protection issues, and has just entered into a partnership with PriceWaterhouseCoopers to develop a Web-based B2C problem resolution system.

Alastair Tempest, Director General of the Federation of European Direct Marketing (FEDMA), discussed the need to boost trust in the online marketplace between businesses and consumers. He noted that FEDMA's "ring of confidence" program aims to help achieve this through a code of conduct, a related consumer complaint resolution mechanism, and links to online ADR systems. In addition, he said, FEDMA believes that various mediation systems should be available and that multilingualism should be stressed. But, Mr. Tempest added, the consumer should never be given the impression that she or he is forced to use either a consumer complaints resolution mechanism or ADR; the consumer should not be denied the alternative of legal action.

Helen Bridges of American Express Services, Europe discussed the use of credit card chargeback mechanism as a means of nurturing consumer confidence.

Discussion

The following arose from the discussion with the panellists and the audience:

- Payment mechanism rules do not apply in the same way to all payment card mechanisms; for example, where there are rules, debit cards and credit cards have different rules (Jean Ann Fox, Director of Consumer Protection at the Consumer Federation of America).
- In countries such as France where it is impossible for a card scheme to have chargebacks because of the irrevocability of payments principal, it is however possible to find a way to ensure that consumers have the same rights as in the United States for example. For example, Visa requires as a first step that the cardholder try to resolve the problem directly with the merchant; if the problem is not so resolved, the consumer can then appeal to the card issuer for assistance (Peter Møller Jensen, Manager of EU Relations at Visa International).
- There are no figures available on chargebacks. However, one of the benefits for consumers is that card issuers have extensive negotiating power and can leverage this power to impose best practice requirements on merchants (Eric Mickwitz, Finnish Consumer Ombudsman).
- It is not helpful to think of chargebacks as ADR. They are a form of complaints handling system, even if they go further than normal complaints handling. They do not constitute ADR mechanisms and certainly do not meet the criteria set forth for ADR, such as independence, transparency, etc. (Ms. Fox and Mr. Mickwitz).
- It is worth noting the need to be careful when encouraging consumers to use credit cards online because a merchant's ability to accept a credit card does not reflect in any way on the merchant's credibility.

Session 4: Online alternative dispute resolution mechanisms

Focus: This session was intended to explore through presentations of online ADR mechanisms already existing or under development, the variety of approaches for solving disputes arising online. In an effort to focus on distinctive procedural and other elements that exist in these various mechanisms, the session was divided into three parts. The first discussion was devoted to fully automated mechanisms where outcomes are generated without human intervention. The second and third discussions were expected to examine mechanisms that vary from flexible to formal with regard to procedure and intervention of a neutral. Finally, the fourth discussion, by exploring systems under development, was designed to focus on objectives and methodology necessary for setting up an online ADR mechanism.

Bernard Clements, Head of the ICT Unit at the EC Joint Research Centre's Institute for Prospective Technological Studies (IPTS) in Seville, served as moderator for Session 4. He recalled that the previous sessions had shown that not all types of disputes may be conducive to ADR, citing fraud, non-co-operation of the vendor and privacy matters as examples. He asked the audience to consider, therefore, whether there are particular types of disputes which may be better resolved through given categories of ADR, and whether in fact ADR mechanisms can be tailored to B2C privacy and consumer protection disputes, given the low-value, low level of harm, high-volume nature of transactions in this segment. He added that this session was expected to bring out problems and difficulties in implementing different types of ADR mechanisms and thus help stakeholders identify essential elements for fair and effective B2C online ADR in subsequent sessions of the conference.

Session 4-I: Fully automated online resolution mechanisms

Focus: Most fully automated ADR systems are designed to settle cash-based disputes, such as insurance claims, and require the parties, before entering a negotiation, to be bound by the generated outcome, if the dispute settles. This session was intended to explore whether automated systems could help settle non-financial B2C disputes arising in the area of privacy and consumer protection.

Richard Belczynski, Vice President of the International and Commercial Division at ClickNSettle.com, described one of their forms of ADR, the online blind-bidding process used to resolve insurance and other cash-based disputes. Mr. Belczynski explained that the system is designed for parties who have previously met and have not resolved their dispute. Each party registers on the Web site and is allowed to enter a desired settlement amount. If the parties' bids are within 30% of each other's, the case settles; if not, the parties are notified and can enter another round of bids. Neither party is able to view the bids of the other, but can see if the other party has entered a bid and when. Before entering the process, the parties agree to be legally bound by the outcome. If a settlement does not occur within 60 days, the parties can resubmit to the process or seek a traditional settlement approach, such as offline arbitration.

Discussion

Ethan Katsh, Director of the Center for Information Technologies and Dispute Resolution at the University of Massachusetts, noted that in these early stages of online ADR development, there is a great difference in technological capabilities of systems. Some are much simpler than others, and cost less money, as is the case for such "arbitration-type" automated systems. However, where fraud is suspected or a human intervention is needed, fully automated systems can not offer an adequate solution.

John Borking, Deputy Privacy Commissioner for the Netherlands, questioned whether the technology would allow the system to serve as an intelligent agent whereby it would learn case law and apply it accordingly when reaching decisions.

A discussion ensued about the capacity of such fully automated systems to settle typical consumer disputes.

- The scope of the ClickNSettle model appears to be limited to damage-type claims, and use of such ADR schemes seems to require the assistance of an attorney (John Borking). Mr. Belczysnki confirmed that the system might be limiting when more human issues are at stake. He also indicated that 70% of consumers using the system have attorneys and 30% use the system themselves.
- The ClickNSettle model has a very limited applicability for typical consumer purchase disputes; it appears to cover purely monetary settlements in cases where the consumer is willing to compromise (Pippa Lawson, Counsel for the Public Interest Advocacy Centre).

The topic of disclosure of case outcomes was also discussed.

- ClickNSettle has a reporting mechanism that allows clients to view their own cases. This mechanism creates an imbalance of information from a consumer's perspective: insurance companies that repeatedly use the system can view all of the cases they have been involved in, whereas a consumer will only be able to view the results of his/her individual case. A suggestion to create information symmetry may be to post publicly accessible information on cases (Mr. Underhill).

Finally, Dana Haviland, Partner at Wilson Sonsini Goodrich & Rosati, asked about ClickNSettle's experience in the international context and suggested that in order to ensure enforcement across borders, extra mechanisms like escrow accounts might be needed. Mr. Belczynski replied that the program has existed for 13 months and most cases have been domestic. In the case of international cases, the company has not yet had a challenge to a decision, but is discussing the use of escrow accounts in the future.

Session 4-II: Flexible resolution mechanisms

Online Resolution, Inc.

Colin Rule, CEO of Online Resolution, Inc., offered an overview of the onlineresolution.com dispute resolution system, with particular emphasis on their online collaborative environment tool, Resolution Room. Online Resolution accesses a network of 500 mediators and arbitrators and settles a range of consumer, workplace, business, and family disputes. An online advisor tool helps consumers choose which type of ADR is best suited for their type of dispute. The Resolution Room is a secure Web-based environment that combines chat rooms, caucus rooms, a voting tool, and a calendar function that the neutral can configure to best suit the needs of the parties. No dispute information is sent via email, as this is inherently insecure, according to Mr. Rule. For disputes under USD 500, onlinedisputes.com charges consumers USD 20; for disputes over USD 500, each party is charged per hour of a neutral's time. The company has a tiered fee structure for use of the Resolution Room; for low value transactions, the room is used for only a short time and the fees are relatively low.

SquareTrade

Cara Cherry Lisco, Director, SquareTrade Online Dispute Resolution Network, followed with an overview of Square Trade's model, and focused particularly on how technology can be an effective tool for helping to resolve high volume, low value transactions. Square Trade allows parties to conduct direct negotiations with one another as a first step to resolving disputes. If the parties are not successful through this approach, the dispute is elevated to mediation. The direct negotiation tool is free to consumers. Ms. Lisco explained that when Square Trade started its direct negotiation system, only 30% of cases settled, but with improved technology, the settlement rate has reached 80%. An important part of their technology is the online complaint form that is not static but is rather a "wizard" tool that presents different options depending on the answers to the previous question. This helps parties better define their problems and demands. Ms. Lisco described another helpful resource for users, which is the provision of data on how similar disputes reached solution. At the time of the conference, they had resolved more than 30 000 cases of which 12-15% were cross-border.

Ms. Lisco discussed some of the privacy and confidentiality issues that arise in the context of online ADR. Square Trade maintains a database of complaints against seal holders; it remains questionable who should have access to this information and what information may be subject to disclosure. Additionally, Square Trade continues to consider whether it should make information about case outcomes public or not.

Discussion

Questions ensued from the panellists regarding the ability of average consumers to use the Resolution Room tools and regarding the training of neutrals. Mr. Rule replied that the Resolution Room system has been tested by consumers in a number of different countries and appears to be very

intuitive and easy to understand. They utilise pop-up windows and animation and have conducted demonstrations in many countries. Neutrals are experts in their areas. Each of them receives 60 hours of training to ensure they can move effectively their mediation/arbitration skills online.

Questions were also raised about the types of disputes handled and length of time to resolve them. Mr. Rule explained that their program was developed to resolve disputes that arose online but their market has grown to include offline cases. He also explained that 90% of disputes are resolved in less than two hours of total neutral time.

Odile Nicolas-Etienne, of the *Union Fédérale des Consommateurs*, stressed that consumers need to be given the resources to determine if ADR is the best approach for them. This includes information about the ADR schemes. She expressed disappointment that ADR providers did not provide information about the settlement outcomes.

Pippa Lawson drew attention to the high cost structure of most online ADR providers as found in the Consumers International report. She lauded Mr. Rule for mentioning that they are exploring a new pricing structure. Ms. Lawson also raised the issue that mediation is more appropriate where both sides must compromise. She urged caution that there are some situations where consumers must not be forced to compromise; online dispute resolution may mean more effective redress but that does not mean that avoiding court at all cost is the solution either.

Mr. Borking advised against disclosures, saying it would discourage businesses from entering into mediation. Ms. Lawson observed that between the models of onlinedisputes.com and Square Trade, Square Trade seemed to be more appropriate for the typical consumer dispute since most disputes, if not settled by internal complaints handling mechanisms, can be settled at the first stage through direct negotiation.

The issue of the appropriateness of online ADR to settle privacy disputes was discussed. Some felt that for simple privacy disputes, some of the kinds of systems illustrated in this session might apply. Mr. Borking pointed out that his government (the Netherlands) had received funding from the EC to build an intelligent software agent capable of handling more complex dispute cases, such as those pertaining to consumer privacy.

Finally, Mr. Borking raised the issue of the advisory tool that helps consumers decide which type of ADR to pursue, and if onlinedisputes.com provides a disclaimer. Mr. Rule responded that they do provide a disclaimer, telling consumers the advisory tool is not legal advice and suggesting that they may wish to seek legal counsel during the resolution process.

A question was raised from the audience regarding oversight of the quality of the neutral's activities, and disparities between writing abilities of parties. Mr. Rule highlighted the benefits of online ADR, saying that all the information exchanged between a neutral and the parties is captured, so can easily be reviewed for quality control. In addition, asynchronous communication can be helpful to those with writing difficulties because it allows parties to take time to prepare responses rather than being forced to provide an immediate verbal response. Ms. Lisco responded that their system builds in technological triggers that, for example, notify Square Trade if a mediator has not responded to a client within 24 hours, or if a case has not been settled within one week, etc. Other quality control measures include reviewing satisfaction and settlement rates of neutrals.

Session 4-III: Formal resolution mechanisms

Fabien Gélinas, Vice President and General Counsel of eResolution, described his organisation's activities as a dispute resolution service provider under the ICANN Uniform Dispute Resolution Policy for domain names. eResolution also recently began licensing its technology for B2B disputes and providing dispute resolution for any type of commercial transaction. In the B2C field, eResolution will provide its technology to the ECODIR project, which is presented in Session 4-IV. Since launching on 1 January 2000, eResolution has handled more than 300 cases involving parties from 45 different countries. A new, Web-based case and document management system allowing the parties and the neutral to work on a case from anywhere was recently put into place. It includes fax uploading capability, chat room, and soon, videoconferencing. In addition, eResolution is currently developing a system in which the same neutral may play both the role of mediator, and, if necessary, decision-maker. He said he believes that "soft" enforcement mechanisms are more promising than methods based on a legalistic approach.

Erik Wilbers gave an overview of the World Intellectual Property Organisation (WIPO) resolution system for domain name disputes and the development of their online ADR program. WIPO is developing an online database that will allow parties to access files and other information securely. The system lets parties submit files of all types, provides notifications of submissions, allows parties to pay fees online and will in the future include videoconference capabilities. He outlined the ICANN rules for domain name dispute settlement, and said that in the last year, 1 682 cases were filed with WIPO from parties in 74 countries. More than 1 100 cases have been resolved, and the average case is settled in less than two months. Of the case resolutions, 880 came through panel decisions and 251 came through party settlements.

Discussion

Ms. Haviland noted that regarding ADR for domain name disputes, it is crucial that arbitrators are trained and highly qualified since they are acting as "judges" in a *de facto* international commercial court. While ICANN rules require domain name case outcomes to be made public, she is not convinced that this should be the case with B2C disputes since in the case of domain names, the goal is to develop precedent where the same may not be the purpose in the B2C sphere. Others suggested that perhaps provisions for disclosures could be specified in the pre-dispute conditions.

A discussion ensued about potential problems of bias in the ICANN process; consumer representatives asserted that WIPO arbitrators rule in favour of the domain name trademark holders more often than the registrants, accounting for the relatively larger number of disputes filed with WIPO. ADR providers argued that the issue is one of perception.

Ethan Katsh said that arbitration in the B2C environment is difficult because whilst some parties would prefer to arbitrate it would always be difficult to persuade others to participate. He recommended that recourse to arbitration be non-binding or governed by an arbitration agreement in place between the parties. Mr. Katsh reminded the conference that domain name dispute resolution is still in its early days. He said that there were three main providers of domain name dispute resolution, one of which used mainly IP practitioners and one of which used academics and a final one used retired United States judges. He said that it could be interesting to look at the effect the different classes of neutrals have on the different outcomes.

Session 4-IV: ADR mechanisms under development

Duncan McDonald of the *American Institute for Contemporary German Studies* (AICGS) outlined a proposal by the AICGS to create a joint venture network between German and United States companies to settle online B2C disputes between parties in these countries. The aim of the joint venture is to bypass legal systems and minimise the role of lawyers. The system is being designed to be free to consumers, non-adversarial, voluntary and non-binding. In order to give consumers the freedom to work with a neutral where they live or bought the product, universities would provide neutral services. Important issues to address include educating neutrals on how to handle this kind of work, deal with the consumers who are unfamiliar with the rules in the other country and design a very simple system to accommodate the majority of consumers who do not want to read or write.

Vincent Tilman, Researcher at the *Centre de Recherches Informatique et Droit*, described the ECODIR (Electronic COnsumer DIspute Resolution) project, currently under development and funded by the EC. The objective of the project is to implement an online ADR process for pan-European, cross-border B2C disputes. Due to launch in June 2001, the project takes into account studies of the social, legal and technological aspects of ADR. Stakeholders involved in the project include European and North American universities, mediation centres, private sector partners, and an advisory board including representatives of business and consumer organisations and national out-of-court-bodies. To date, organisers have identified several areas of difficulty in meeting the criteria for online ADR, including:

- Independence: how to finance ADR for small value disputes?
- Transparency: how to strike a balance between the quantity of the information and the simplicity of such information to be provided to consumers?
- Adversarial principle and how to protect confidentiality in the mediation process?
- Effectiveness and legality.

Christopher Kuner, of Counsel, Morrison & Foerster, LLC gave a presentation on the International Chamber of Commerce's strategies in the area of B2C ADR. Mr. Kuner recalled that ICC houses the world's largest B2B arbitration forum and is interested in B2C because it is the world business organisation, because it has wide experience in arbitration and because it can offer the leadership that the business community needs. He mentioned that an expert group had been formed taking into account geographical and professional diversity and had issued a strategy paper on policy matters and concrete steps to be taken. The policy principles highlighted in the paper are aimed at businesses, governments and ADR providers, in an effort to promote principles such as availability (need for access to ADR when doing business), credibility (notice of terms and conditions relating to ADR), competition (variety of ADR offered) and openness.

The concrete steps outlined in the strategy paper include the setting up of a dispute resolution clearinghouse, which would:

- Provide information to business and consumers on ADR world wide.
- Assist parties in search of ADR.
- Provide standard online forms for submission of cases to ADR.
- Provide a translation service of these forms.
- Develop basic standards for ADR provision.

Finally, Mr. Kuner mentioned that ideas for the future included assistance to business in internal consumer services and setting up their own ADR. To this end, he stressed that the ICC intends to work closely with the GBDe and consumer groups.

Discussion

Two areas of difficulty identified for setting up online ADR mechanisms were discussed by the panellists: the issue of mandatory recourse to ADR, and the independence of ADR schemes.

- At this early stage of development of online ADR, the binding nature of arbitration makes it less attractive to consumers (Charles Underhill).
- Non-binding ADR creates an incentive for providers to develop good ADR that meet the minimum standards and thus could engender consumer confidence. Consumers should not be bound, but business should be (Pippa Lawson).
- ADR is just a tool to achieve consumer confidence which, in any case, will mostly be achieved by compliance by business with all aspects of the transaction. Independence of ADR schemes should be secured by using collective funds from e-commerce companies (Odile Nicholas-Etienne).

Day 2: Reaching effective online ADR at a global level

Ms. Jytte Oelgaard opened the second day of the Conference, saying that it was important to discuss how ADR could become an effective tool in establishing peoples' trust in the online B2C marketplace. She outlined the day's focus on legal and technical issues surrounding online ADR. Based on the previous day's discussions, she offered her views on the necessary requirements of online ADR, including impartiality, easy access, low cost, transparency, and reliability. Ms. Oelgaard said it was also important to examine who is competent to have oversight over these ADR.

Session 5: Challenges to online dispute resolution

Session 5-I: Socio-economic issues related to online ADR

Focus: This session was intended to discuss some of the socio-economic challenges, including how cultural, linguistic and economic differences might challenge the effectiveness of ADR systems; or similarly, how differences in information and expertise might affect the use and implementation of ADR, while considering that online means of communication (digitalised texts, sounds, stationary or moving images) affect methods of work, cultural patterns and life-styles.

Anna Fielder, Director of the Office for Developed and Transition Economies at Consumers International, served as moderator for session 5-I. She raised three points discussed during Day 1 that related to the session's focus. First was the idea of synchronicity of communications in online ADR, and the potential benefits of giving parties time to think before responding. Second was the possibility that online ADR helps eliminate bias and preconceived notions of, for instance, race, gender, or age. And finally, she stressed that online ADR may accentuate literary imbalances: those who can write well have an advantage in the online context.

Nora Femenia, Professor and Vice President of OnlineDisputes.org, presented the results of her extensive research on social aspects of ADR, and how cultural differences affect the use and

implementation of ADR systems. She said that some studies have shown that where a mediator is an Anglo-Saxon, invariably any party that is non-Anglo-Saxon will lose. She said that each culture has different ideas about what conflict means, and that, in examining culturally-influenced behaviour in mediation, it is possible to draw a basic distinction between: *i)* individualists (focus on personal gain) and *ii)* collectivists (focus on good of the community). It is important to look at how people act and whether they are orientated towards individualism or collectivism as these two types approach a dispute in different ways, the individualist concentrating on receiving redress, and the collectivist concentrating on the outcome that is best for the community and the relationship with the other party.

She also highlighted that it is very important for customers to perceive that they have experienced justice through a dispute resolution process. She referred to the message delivered the day before by other speakers that customers who complain, and whose complaint is dealt with correctly, actually return and are more loyal and spend more money than before. She also said that in general people want sympathy and understanding and want to feel like a valued customer.

Ms. Femenia also stressed that customers' expectations of a dispute resolution process include an expert complaint handling, an apology from the other party, and a quick and simple mechanism. Customers will accept a decision generated by a computer (*i.e.* automated) because computers are seen as neutral parties.

She discussed that some cultures are not conducive to complaining and business must therefore give support that recognises this difference to those customers. She explained that some elements of customers' desires are however cross-cultural, for example, the offering of an apology; acknowledgement of the customer as a real person; business not denying or excusing its fault; identifying the problem quickly; acting in a respectfully attentive way; and providing opportunities for emotional "venting." Ms. Femenia added that businesses should offer some token of reparation in recognition of the time spent by the consumer in complaining, and that any dispute resolution mechanism should be free of charge and designed from a customer's point of view. Finally, she emphasised that customers should not be overwhelmed with information, rather they should be provided information that is necessary at the appropriate moment.

Discussion

- The ability of a consumer to complain in his/her own language is an integral component for an accessible system. From the experience of the European Advertising Standards Alliance (EASA), which has 28 members in 25 countries and deals with 50 000 complaints per year (national and cross-border) in a variety of languages, ensuring linguistic barriers are properly addressed is a key necessary first step towards effective ADR. (Carmen Fernandez Neira). And language does not just mean literal translation, it must reflect the intended cultural meaning. Online translation sites should therefore have cultural adaptation as well as language translation (Ms. Femenia).
- The issue of community values versus individual values in dispute resolution must be taken into consideration. There are several examples of difficulties in mediation between Asian and American or European parties. The culture of the mediator can also be an issue. It is doubtful that automated dispute resolution systems could take account of these complex human elements (Toh See Kiat, Partner, Tan Peng Chin and Partners).

- There are many different meanings and interpretations of what is ADR. Even within the European Union, the lack of information on ADR available to consumers and linguistic barriers are a serious source of concern (Giles Buckenham, Administrator, Directorate General for Health and Consumer Protection at the European Commission).
- It is important to develop a system that recognises cross-cultural differences. People want to feel they have a fair hearing. Stakeholders should not expect perfect ADR mechanisms at this stage: it is important to be flexible and consider what needs to be done in order to get global or regional ADR programs up and running (Scott Cooper, Manager of Technology Policy at Hewlett-Packard).

Christopher Drahozal, Professor at the University of Kansas School of Law made a presentation on the economics of online ADR. Starting from a basic definition of economics that parties make choices in the face of scarcity he raised a number of issues to consider when looking at the development of online ADR. He stressed that some disputes are too expensive to resolve, even through online ADR. On the other hand, because the online medium can reduce the cost of ADR, it may enable the settlement of disputes that in the offline world would be too expensive to resolve. However, he stressed that without online dispute resolution available at a global level, many disputes will remain unresolved or outcomes un-enforced.

He discussed the issue of fairness related to who bears the cost of ADR: not all consumers have disputes, yet the costs of ADR will be passed on in the price of the product, and all consumers will end up paying for the dispute resolution mechanism.

Mr. Drahozal also raised the point that not all disputes are the same, and because of this, different disputes may require different approaches. For example, low value consumer purchase disputes and disputes involving personal injury are completely different. He commented that, from an economic perspective, there may be certain circumstances where removing access to court by including a pre-dispute, binding arbitration clause might be efficient. However, he also acknowledged that requiring consumers to submit to binding ADR will likely not be conducive to building trust.

Discussion

- The first barrier to achieving consumer confidence in e-commerce is mistrust in the medium itself. ADR is not a complete solution to consumer confidence in e-commerce and consumers need further confidence that nothing will go wrong in the first place (Mr. Buckenham).
- Many consumers are reluctant to use the Internet; however, e-commerce can save consumers a lot of time and money, and they may receive better service in the online environment (Dr. Toh).

Ms. Fielder closed the session by saying that consensus is emerging that ADR must be free or low cost to consumers and accessible. In making dispute resolution fair and more accessible, cultural and language problems must be addressed.

Session 5-II: Legal issues related to online ADR

Focus: This session was expected to highlight those procedural and substantive elements considered as essential to ensure a fair and effective ADR process, while recognising that these elements may vary depending on the type of ADR and/or dispute.

Mozelle Thompson, Commissioner at the US Federal Trade Commission, served as moderator for Session 5-II. He raised, on behalf of Philippe Fouchard, Professor, University of Paris II, four important legal issues to be addressed: *i)* Preserving voluntary recourse to courts; *ii)* Insuring transparency for the status of intermediaries; *iii)* Fostering flexible procedures; *iv)* Ensuring confidentiality unless agreed otherwise by the parties.

Christopher Kuner presented a summary of a study he conducted for the GBDe on legal obstacles to online ADR. He acknowledged that there is no common understanding of the different ADR processes, and that basic terms such as "arbitration" are understood differently, due to cultural differences among people. In looking at the out-of-court dispute resolution systems run by third parties, Mr. Kuner explained that ADR must be based on some sort of agreement between the parties, adding that it is in no-one's interest to force a party into arbitration against his/her will. He then discussed whether the accreditation of ADR schemes should be considered. He raised other legal concerns related to online ADR, such as the difficulty of determining the place of arbitration online, or the fact that national laws on encryption could add further complications. He discussed online security and commented that flaws in the Internet could run afoul of constitutional guarantees for fair procedures in countries such as Germany.

Mr. Kuner discussed embodying the result of ADR settlement agreements. He added that enforcing judgements based on these agreements is too costly. He then discussed binding awards. He stated that he did not think that the New York Convention was useful in the e-commerce context.

Discussion

James Murray, Director of the *Bureau Européen des Unions de Consommateurs (BEUC*), discussed the question of binding or non-binding procedures. He argued in favour of a non-binding arbitration procedure, adding that ADR should be an alternative to court but should not require a strict choice between court and ADR. He emphasised that there was great difficulty in enforcing legal rules. In this regard, he recommended standards for ADR schemes and suggested that trusted third parties could assess whether or not a business meets those standards. He also said that sensible involvement of public authorities should be encouraged.

Ron Plesser, Partner at Piper Marbury Rudnick & Wolfe, discussed the possibility of an exhaustion of remedies concept. He advocated a system that requires consumers to go to ADR first; if after undertaking ADR, the consumer is still not satisfied with the outcome, he/she may then go to court. This approach does not extinguish the rights of consumers. He argued that businesses would be investing a significant amount of money in developing and maintaining ADR systems; therefore, it was only fair that consumers should be required to undertake ADR first. He added that in relation to standards, the difficult issue is whether to accept the law of a particular jurisdiction. He suggested that it may be easier to create codes for different types of procedures, and examine the question of how codes should be enforceable.

Petra Spring-Reiman, Directorate General for Internal Market at the European Commission, commented that, in relation to the question of binding and non-binding ADR, continental lawyers probably agree that the threat of establishing a quasi-judicial system would be problematic. In this respect, she explained that if the system of ADR were binding then its decisions would act as a form of precedent and lawyers would be examining those decisions for consistency and potentially the establishment of new legal principals. She said that if the right to go to court were precluded and the ADR system were binding then there should still be clear appeal possibilities. She also provided that moving online requires systems to be flexible, not burdened by the types of safeguards required in judicial procedures.

Michael Geist, Professor at the University of Ottawa Law School said that a list of elements can be established to make ADR work, but that tradeoffs need to be made on issues such as precedence and cost. He said that there is a need to have precedence and that once a number of decisions will have been made, seeking legal counsel will be important. This is now the case with domain name disputes. As for the issue of who should pay for the ADR, he added that very little money is being invested in ADR systems at the moment as the market is not yet receptive.

Matthias Blume of the Austrian Ministry of Justice commented that there was a thin line between who pays for the ADR and who achieved the standards. He said that it was important to build trust for consumers, and that, in this regard, standards should not be mandatory and the voluntary character of ADR schemes should be upheld. In relation to trustmark systems for ADR, he argued that enforcement measures are needed, and he explained that such measures have been set up in Austria.

Jean Ann Fox said that when consumers are going online to purchase goods, they often do not read the ADR agreement, and therefore, they do not voluntarily agree to be bound by ADR. She commented that she was strongly opposed to Mr. Plesser's proposal to require consumers to go through the ADR system before they seek court remedies. She said that an ADR system ought to be established in such a way that it is more attractive to consumers than court.

Mr. Plesser responded that there is a need to justify the expense of the ADR system. He said that his proposal for an exhaustion requirement was a middle ground solution because he was not preventing recourse to court but only requiring ADR to be tried first.

Mr. Blume said that in his three years' involvement in the area of consumer issues, he had never seen a consumer proceed to court at the first stage. However, he argued that consumers should have the possibility to go to court at any moment during a dispute.

Hubert van Breemen said that in the Dutch system, binding outcomes are possible, but this was a decision reached by both industry and consumer representatives.

Another question came from the floor regarding the role of preserving class action lawsuits in the discussion of ADR. Mr. Plesser described such suits and explained that in some class action cases in the United States, security brokers have opted for mandatory arbitration.

Mozelle Thompson closed the session by stressing the need to foster co-operation between business and consumer representatives on these legal issues.

Session 5-III: Last resort principle and juge d'appui

Focus: This session aimed at focusing on the intersection of online ADR with the jurisdictional framework, during the ADR processes as well as when the alternative mechanisms fail.

Catherine Kessedjian, Professor at University of Paris II, served as moderator for Session 5-III.

She presented the framework for the session, which included first addressing the question of whether, in the course of ADR, to facilitate a successful and smooth ADR process there is a role for the *juge d'appui*, a notion which exists in international trade arbitration; and second, the notion of last resort which preserves recourse to the courts. Ms. Kessedjian recalled that the focus of the session was on methodology and the competency of the judge and did not address issues of the applicable law.

She invited the panellists to discuss what part a *juge d'appui* might play in ADR.

Roger Cochetti, Senior Vice President and Chief Policy Officer at VeriSign, responded that the *juge d'appui* is a useful concept but is based on the presumption that cases involve low volume/high value disputes, a presumption which underlies the practice in the context of international commercial arbitration. In B2C e-commerce, he argued, this presumption is defeated given that it deals, to a large extent, with low value/high volume disputes. He added that it would be difficult to involve the judicial process in ADR without jeopardising the principle that the process should be economical for both parties.

David Goddard, a barrister representing the New Zealand Law Commission, outlined four basic situations in which the judge may still be useful in the context of ADR: *i)* Pure enforcement of consumer rights issues as courts still have the exclusive exercise of coercive powers; *ii)* As a judge of last resort, by having clear rules as to what happens if there is no agreement about ADR; *iii)* As a *juge d'appui*, in cases of binding arbitration (in case of non-binding arbitration if parties cannot agree on a new replacement ADR, there is not much hope that an agreement could be reached on the merits); and *iv)* In the enforcement of a settlement agreement.

Naja Felter of Consumer International, asserted that consumers should always be able to go to court and should never be required to forfeit that right. She agreed that the *juge d'appui* concept is difficult to build into the B2C context given the usual low value nature of the disputes, and added that if there is good oversight of the ADR, there should be no need to resort to a *juge d'appui*.

Asuncion Capparros, Manager of European Affairs at ABN Amro Bank, said that the *juge d'appui* is not *a priori* an attractive new layer in B2C. Furthermore, she raised the issue of the background of a judge in this context and what the qualifications might be. Would a judge come from the court system or a government law enforcement agency? What specialised experience could be required of judges?

Giacinto Bisogni, National Expert in the Legal Services of the European Commission said that, given the voluntary nature of ADR, he did not see a role for a *juge d'appui* in the course of an ADR process. He added that recourse to a judge in the course of an ADR process may introduce far too much rigidity. He suggested that responsibility to ensure a successful and smooth ADR process be given to the ADR provider or to an oversight organisation.

An audience participant pointed out that questions of applicable law and procedure could be solved by the judge since the neutral has no power in this regard. He also suggested that the judge could serve to protect consumer rights in provisional and protective measures as well as in

enforcement issues. In addition, he posed the question of whether it would not be appropriate, instead of having a limited role for a *juge d'appui* in ADR, to make jurisdictions more mediation-oriented.

Ms. Kessedjian then invited the panellists to consider the following questions in relation to a last resort: *i)* What role must a judge play; *ii)* Who should that judge be, what are the required competencies; *iii)* Could it be compulsory for a consumer to make a choice or should there be rules by default; *iv)* What means should be used.

Mr. Goddard presented an overview of the ongoing work by the Hague Conference on Private International Law on a convention on jurisdiction and recognition of foreign judgements. The convention's original proposal to have a special consumer jurisdiction (*i.e.* the place of habitual residence of the consumer) gave rise to a lot of controversy. In view of the difficulty of the issue, some proposed to exclude consumers from the scope of the Convention; others proposed that countries be allowed to let their consumers agree to some other forum than the ones provided in the Convention. Another possibility would be to retain the classical jurisdiction (defendant's habitual residence, place of establishment or branch, place where the tort occurred, or voluntary appearance of the defendant).

Ms. Caparros recalled that whereas under current European legislation consumers have the right to sue in the courts of their country of residence, they may still need to seek enforcement of the judgement in a foreign country.

Mr. Cochetti indicated that the access of consumers to local courts is not practical and that the results are likely to be unenforceable given the low value of the disputes.

Finally, Giacinto Bisogni recalled that the Commission is considering a general consultation on the creation of an extra-judicial European space where ADR outcomes would be recognised.

An audience participant pointed out that it is important in designing rules to be careful not to discourage smaller countries and industries from participating in e-commerce.

Session 5-IV: Technological issues related to online ADR

Focus: This session aimed at highlighting technologies already in use or under development with a view to how they can be used to facilitate online B2C dispute resolution. For example technologies used for secure electronic signature and authentication, or encryption of content messages may help ensure confidentiality and integrity of the process and the information exchanged. Furthermore, interactive technologies like video-conferencing may bring the parties together, moving them from behind their computer screens to a virtual setting making the experience a face-to-face interaction. Similarly, automatic translation and voice recognition may help bridge some cultural differences.

Wibo Koole, Head of Consumer Policy Department at *Consumentenbond NL*, served as moderator for Session 5-IV. He stressed the importance of examining how technologies can support ADR and speed its development.

Chris Lynn, Legal Associate with Microsoft Europe, Middle East and Africa, gave a presentation on technological developments that will be useful for online ADR. He focused on advances in computer languages, enhanced videoconferencing, and translation and speech recognition software. Mr. Lynn stressed that technology is ethically neutral and that users need to think about policy issues before they deploy systems.

He described XML (extensible mark-up language), a language that allows Web-based applications to talk to each other and make "intelligent" decisions from this information. XML connects all the technological components of the supply chain. In the ADR context, he suggested that it could help achieve transparency by overcoming certain person-to-person barriers such as allowing for digital signature "handshakes". He discussed how ultra-fast broadband access technology, such as Mbone, will allow for secure high-quality videoconferencing at a low cost. Finally, Mr. Lynn discussed advances in translation and speech recognition software. Although the current versions of these are far from perfect, "smart" software is being designed that promises to change the user experience.

Joseph Alhadeff, Vice President of Global Public Policy at Oracle, followed with a discussion of some of the policy issues to consider in developing online ADR, including how do ADR providers use technology, and how does technology affect an arbitrator's evaluation of facts. Among some main questions for parties to consider in doing business online are: *i)* Can you authenticate the other party (are they really who they say they are?); *ii)* As a merchant, what are my tax obligations for providing goods or services cross-border?; *iii)* With whom has the consumers information been shared; (are there privacy concerns?).

Mr. Alhadeff also discussed technology-related issues specific to customer service online, such as navigability of a Web site and language capabilities; security and confidentiality of data online; and ability of a merchant to know product availability. For ADR providers, he stressed that systems should be backed up regularly to maintain data integrity. Finally, he identified a number of consumer trust issues involving technology and policy. Among those cited on the technology side were concerns about identity theft, the security of payment card information, and lack of customer-side controls. The list of policy topics included privacy, authentication, and fraud and consumer protection.

Discussion

- Common market technology can be used for online ADR. XML and other new technologies, such as video conferencing, will be used in the future. As XML can be used to formalise a group of applications, it could be an Extended dispute resolution language. First, there may be a need for simple middle ground technology, not a Cadillac, but "a public transport" technology (Peter Lubkert, Head of Division, Information Technology and Networks, OECD).
- Language problems can still occur with videoconferencing, whereas asynchronous communications may give each party time to fully understand the communications they are reading and sending (Pippa Lawson).
- There is a need for generic standards and criteria for ADR, and the challenge is how to translate these standards into technological requirements. It appears that a very high level of automation is needed to handle the first stages of online dispute resolution such as direct negotiation (Marc Wilikens, European Commission's Joint Research Centre).
- Technology has to be guided by principles as on the one hand, technological tools can help consumers maintain their anonymity online, and on the other hand, technology also poses threats to data protection and individual liberties. ADR may not be appropriate for privacy disputes where users need injunctive relief. Because most privacy violations are not single cases, but perpetrated against large numbers of users, the right to class action must be preserved (Sarah Andrews, Policy Analyst, EPIC/Privacy International).

Speaking from the floor, Susan Grant, Director of the National Fraud Information Center at the National Consumers League, raised the issue of interoperability of computer hardware and software between the ADR provider and the consumer. She suggested using an approach similar to the one adopted in the recently-passed United States e-signature law that requires consumers to give consent to receive electronic documents in such a way that it demonstrates they have the capability to receive this information on their systems.

During a brief discussion about "intelligent" software agents, Mr. Alhadeff raised the concern that, although useful, such agents could create legal concerns if they make decisions on the part of the parties.

Session 6: The roles of stakeholders

Focus: Based on previous discussions, this final session was expected to highlight common stakeholder views on a number of socio-economic, legal and technological elements that should be part of any fair and effective online ADR for B2C disputes, and to focus on how best to foster their implementation through exploration of two main policy areas.

Arie van Bellen, Managing Director of Electronic Commerce Platform Nederland, served as moderator for Session 6.

Session 6-I: Promoting fair and effective online ADR and ensuring compliance (e.g. trustmark programmes)

Focus: This session was expected to further discuss the roles of stakeholders in relation to promoting fair and effective B2C online ADR. This included discussing how the stakeholders should co-operate to identify essential elements for online ADR (*e.g.* Who should sit at the table? Should there be separate recommendations by different stakeholders, as is the case to date? Where should guidance for ADR be identified – *e.g.* in regulation or codes of conduct). It was also to include how the stakeholders can work together to ensure compliance with these elements.

Naoshi Shima, Vice President for Internet Business Development at NEC Corporation, offered an overview of dispute resolution in Japan. He stated that while most Japanese consumers trust the good faith of merchants, they are very strict about product/service defects. As a result, standards of quality tend to be high. While recourse to courts is available to consumers, most prefer to negotiate directly with the merchant or to use ADR mechanisms such as consultation and mediation if direct negotiation fails.

Japan's consumer protection law obliges local governments to establish consultation centres for B2C disputes. In addition, NGO's and industry groups operate consultation centres. Almost all disputes brought before the centres are settled. The centres operate offline and lack the requisite knowledge and skills to move to the online environment. Mr. Shima discussed several issues being discussed in Japan related to dispute resolution, including deregulation of the "attorney law," which permitted only attorneys to deal with consumer dispute cases.

Barbara Wellbery, Partner at Morrison & Foerster, LLC, presented her perspective of the roles of stakeholders in identifying criteria for online ADR mechanisms. She stated that thus far stakeholders agree that ADR must be effective, no or low cost to consumers, easily available, and independent/impartial. However, she questioned how long this consensus would last once stakeholders begin to discuss the specific details of these elements. She highlighted a similar situation that arose in

discussions of privacy principles for the recently adopted safe harbour accord between the United States and the European Union. She further identified a number of elements of ADR on which participants did not yet agree, including: who should bear the cost of ADR; possible trade-offs between procedural guarantees and efficiency; whether ADR can be mandatory for consumers; and whether ADR outcomes can be binding on consumers.

She discussed two options for who should set rules for ADR: governments or the private sector. She argued that because governments have national interests and perspectives, it is unlikely that they will adopt globally-compatible guidelines. Rather, she recommended that the private sector take the lead in establishing criteria for online ADR, ensuring that all stakeholders are at the table. She also suggested that if stakeholders define the scope of this exercise to that of making rules for cross-border, online ADR for B2C transactions and simple privacy disputes, the task will become more manageable.

Malcolm Crompton, Federal Privacy Commissioner of Australia, provided an overview of Australia's proposed co-regulatory approach for privacy protection. The Australian privacy law provides for either the establishment of sectorally-based codes of conduct and code complaint bodies for settling disputes, or the ability of the privacy commissioner to handle consumer complaints. The approach is to set minimum standards and benchmarks for privacy protection, and to allow the marketplace to develop solutions to privacy over and above the standards. The Privacy Commissioner will implement the standards and enforce compliance. Mr. Crompton stressed that 50% of the transactions by Australians are abroad where national laws do not apply. This illustrated the importance of privacy commissioners working together globally, and gave the example of the recent joint study conducted by his office and the Information and Privacy Commissioner of Ontario, Canada, on online trustmark programs. He argued that privacy commissioners need to rethink their roles in the Internet age, focusing on co-operation and strategic partnerships.

Martin Bond, Assistant Director, UK Department of Trade and Industry, illustrated the United Kingdom's approach to identifying the roles of stakeholders in establishing rules for e-commerce. He said that there is a demand for official endorsements and governments can help forge global links. He described the United Kingdom's "light touch" approach to regulating the development of codes of practice and best practice programs. He strongly encouraged consumer organisations to participate in this process so that there is "buy in" from all stakeholders.

Mr. Bond outlined the TrustUK program through which the UK Government is encouraging codes of conduct. Rather than imposing a single code for the online environment, TrustUK approves codes of practice that embody their core standards on, for example, privacy, advertising, and provision of contract information. He stressed that ADR should be an integral part of these code systems.

He commented that as a result of this arrangement, the government is well placed to promote links between national codes. For instance, TrustUK is taking part in the EC's stakeholders group effort to develop guidelines for code providers in Europe. He also pointed to fora like the OECD where governments can participate on an international level.

Discussion

- Governments have an important role to play in setting down a general policy framework. In particular, governments should set guidelines for fair and reliable ADR systems and to facilitate international co-operation in this area, for example, in the promotion of mutual recognition of online seal programs (Yuko Yasunaga).

- A proliferation of seal and ADR programs is arising nationally and there is a need to have general guidelines. Such guidelines should be concerned with all types of disputes. In developing these, it is important to include the ADR providers themselves who have practical experience in dealing with disputes (Rebecca Richards, Director of Policy and Compliance at TRUSTe).
- Governments ought to proceed with caution in looking to developing guidelines, because there is a tendency to be too territorial. The Internet is at a very early stage of development, given that more than 50% of current Web sites started just in 2000 and more than half of consumers who spent money on the Internet did so for the first time that year. However, if there is a need for a cautious approach, this does not mean inaction (Roger Cochetti).
- Although there is a need to be realistic about the early stage of Internet development and a need to experiment, some guidance is required at this point. Guidelines should come from a high level like the OECD consumer guidelines. Participants should consider what the role of stakeholders would be. In the case of consumer organisations, they can give input to businesses and rate business services, as they did for the online shopping checklist for consumers developed by the Trans-Atlantic Consumer Dialogue (Susan Grant).
- The adoption of guidelines should not be delayed because the marketplace is developing, because once online models are in place, businesses may argue that it is too costly to modify their processes to account for new standards (Jean Ann Fox).

David Mair described the difficulty of identifying who really speaks for e-commerce in the context of stakeholder discussions; for example, it is not always easy to find the voice of retailers and SMEs. David Mair also stated that it was important to distinguish between the following two key questions: *i)* The role of technology in ADR and *ii)* The role of ADR in e-commerce. He said that we should be extremely careful not to blur the distinction between these two questions and address them separately.

Session 6-II

Focus: Cross-border ADR is common in the B2B context, but is new in the B2C context. Recognising that users' and consumers' knowledge and understanding of ADR is minimal, this session aimed at focusing on the roles of various stakeholders in educating consumers, as well as businesses, about such mechanisms to resolve disputes online. In particular, the discussion was to include effective approaches to educating business about offering ADR and to educating consumers about the nature of and procedures for fair and effective ADR.

Francis Aldhouse, Deputy Data Protection Commissioner in the United Kingdom gave a brief overview of the role of the Data Protection Commission and the Data Protection Act 1998. He explained that enforcement of the Data Protection Act is by criminal prosecution and added that there is a duty to investigate compliance at the request of any individual. However, the primary method of enforcement is by the provision of a notice period and therefore a type of regulatory power. However, Mr. Aldhouse argued that the best way forward was not for the Commission to take on a policing role but rather to promote cultural change by, among other ways, getting organisations to include privacy protection in their business plans, and to promote good practices, including ADR.

The Data Privacy Commission receives between 5 000 and 6 000 complaints a year. He said that last year, two thirds of cases handled by the Commission were based on simple factual disputes. Mr. Aldhouse also discussed efforts by the Commission to educate consumers about their privacy rights by running television advertisements and through poster advertising.

Ms. Grant referred the conference to the Consumers League Web site at www.nclnet.org. She said that there was a guide to shopping online safely available on the Web site and added that effective public education was crucial.

Mr. Mair commented that it was important to look at ADR in a wider context. He said that it is important to educate customers by promoting the message that if something goes wrong with a transaction, a good complaints handling system is available, then they may have recourse to ADR and then finally, if that is not adequate to redress their complaint, they can take the matter to court.

Mr. Yasunaga indicated that consumers who are not educated about seal programs or online issues are more likely to encounter problems. He said that it is important to promote disclosure about ADR and that consumer representatives should play a more active role in this area. He said that education was more effective for the younger generation than for adults.

Mr. Cochetti agreed that education was extremely important. He discussed a privacy leadership initiative that is launching a United States education campaign about protecting privacy on the Internet. He said that his company is developing an education program for SMEs about codes of conduct and other self-regulatory initiatives.

Ms. Richards said that it was important to remember that it necessary to educate stakeholders offline as well as online.

Conference conclusion

Mr. Ford recalled the key themes discussed on day 1:

- The keynote speeches highlighted the need for global partnerships among stakeholders as a key element in developing fair and effective online ADR mechanisms for business-to-consumer disputes. Speakers also acknowledged the complex legal and technological challenges that need to be addressed to reach this end.
- Session 1 provided a summary of efforts taking place to examine the development of online ADR nationally, regionally and internationally. It was clear that stakeholders from government, business and consumer organisations are equally committed to promoting ADR for B2C disputes. The discussion helped identify areas of common ground and differences to be bridged among the various stakeholders with regard to essential elements of online ADR. There was a degree of consensus in a number of areas. All recognised that attention should be paid to finding ways to avoid disputes that arise between businesses and consumers. It is clear at this stage that no one size fits all in ADR, meaning that no single approach is likely to apply best to all types of disputes. Next, given the borderless nature of the Internet, ADR mechanisms must be designed to bridge cultural differences. Finally, while it is crucial that ADR mechanisms are fair and effective, the speed of decision-making should be tailored to Internet time. The presentations in this session also highlighted areas that need further exploration, including issues of consumer choice (voluntary versus mandatory ADR), binding or non-binding outcomes, compliance and enforcement.
- Session 2 featured discussions and statistics on the most common types of online B2C disputes and compliance rates with privacy regulations. The most frequent consumer complaints are non-delivery, followed by late delivery, and lastly problems associated with costs. Some of the most frequent privacy complaints are related to unsolicited commercial e-mail, identity theft, harassing phone calls, providing credit history without consent, selling data to third parties, and children's privacy. An increasing number of consumer e-commerce

complaints involve cross-border transactions. The importance of law enforcement co-operation was also highlighted through the illustration of a United States-Canadian joint database of fraud complaints.

- Session 3 focused on the issues of customer expectations for service and credit card chargeback mechanisms as a way to settle disputes. Recent surveys show that consumers expect faster responses from online merchants and are less likely to remain loyal if their problems are not addressed by internal mechanisms. It is important to educate merchants about the needs of consumers. A key point raised during this session was that chargebacks are not a form of ADR but are an important element in resolving consumer disputes.
- Session 4 included demonstrations and discussion of different types of online ADR mechanisms, including automated systems (where the outcome is generated by a computer); direct negotiation and mediation systems; formal arbitration systems; and cross-border systems under development. While it was not yet clear which ADR systems are best suited to resolve different types of disputes, there was agreement that current automated systems are mainly tailored to resolve monetary disputes. There was recognition that there are limits to what ADR systems can accomplish and development is still in an early stage, but it was agreed that they offer great potential.
- The session also highlighted the need for training of neutrals/intermediaries and awareness building. Participants addressed several consumer-related concerns with online systems, including asymmetry of information, language barriers, the funding of mechanisms and the relationship between funding and impartiality of the ADR system.

Ms. Oelgaard recalled the key themes discussed on day 2:

- Session 5-I explored cultural differences in dispute resolution and economic considerations in examining online ADR. It appeared clearly that not only language barriers in online ADR must be tackled, but also cultural distinctions that have an effect on dispute resolution, such as habits of complaining and what consumers expect from customer service and ADR.
- On the economics of dispute resolution, the point was raised that some disputes may be too expensive to be resolved by online ADR, and that offering ADR at low cost to consumers raises issues of who should bear the cost. Since not all consumers have disputes, should they all bear the cost, or would competition be strong enough to bring the price down overall? Another challenge is that there may be a conflict between the need for economic efficiency and the need to build consumer trust. Further work must be done to strike the right balance.
- Session 5-II focused mainly on the difficult issues of voluntary *vs.* mandatory recourse to ADR, including the idea of a pre-court exhaustion requirement for consumers, and binding *vs.* non-binding outcomes. Although the session did not lead to concrete solutions, the message was clear that work is needed in this area, starting with definitions of terminology. ADR forces stakeholders to look at certain fundamental aspects of the legal system.
- In Session 5-III there was consensus on the fact that recourse to a *juge d'appui*, while good theoretically, may not be feasible at a practical level, except maybe in a limited number of cases. In fact, there was concern that this may add an additionally burdensome layer. Further work is needed on the last resort principle, in particular on how the competent forum would be determined.
- Session 5-IV highlighted that technology is fundamental for online ADR but requires a policy framework to ensure security and confidentiality, but also transparency and simplicity. Advances in new industry technology standards such as XML offer an

opportunity to harmonise and increase interoperability of global ADR. Similarly, technological advances like translation software, intelligent agents, and videoconferencing may improve the efficiency of ADR and the potential to bring parties from around the globe to a face-to-face dialogue.

While there is much promise in the use of technology in online ADR, as in other areas of e-commerce, participants cautioned that privacy issues continue to arise and should continue to be considered as the technology is developed. Similarly, what can be considered to be the advantages of technology may also present some difficult choices. For example, where some users may find face-to-face resolution mechanisms more desirable, asynchronous communication may provide a party the advantage of longer deliberation on a response.

- Participants in Session 6 expressed a number of views about the appropriate roles for stakeholders in developing online ADR. Consumer organisations have a strong vision of what they could do to provide input. Consultation with consumer groups should go beyond simply hearing their views, but should also incorporate them into initiatives. Some expressed the view that governments should be involved to the extent that they can inspire trust and provide for democratically legitimised discussion of various ADR elements. Others asserted that the private sector should lead as e-commerce is borderless and governments are constrained by geographic borders. The private sector calls on all stakeholders around the world to be involved in surpassing e-commerce roadblocks. In addition to the current involvement of business, consumer and government representatives, the importance of the involvement of other stakeholders was stressed. More representation from ADR providers and e-merchants would be beneficial to the discussion.
- Lastly, it was agreed that disseminating information about online ADR and educating individual users and businesses was an extremely important task.

The chairs thanked all participants for their active input in the conference, and invited them to widely disseminate what was learned from this conference.

NOTES

1. ADR refers to mechanisms and processes intended to supplement court adjudication in assisting parties in resolving differences.

2. Within the OECD, the conference was organised by the ICCP Working Party on Information Security and Privacy (WPISP) and the Committee for Consumer Policy (CCP), in co-operation with the OECD Business and Industry Advisory Committee (BIAC).

3. "ADR That Works" by Ernest G Tannis - the quote is taken from the ADR Primer of the American Bar Association (Appendix E).

4. In most situations, a party files a complaint with a third-party ADR provider who then notifies the other party or parties of the complaint. Then, an exchange or series of exchanges occur between the parties with the intervention of the third-party neutral as the parties attempt to settle the dispute. This neutral may be a human mediator/arbitrator or an automated system, as in the case of computer programs that settle insurance claim disputes. The parties may decide on the rules of procedure or the rules may be imposed by the ADR provider; the final outcome of the ADR process can be either an agreement reached by the parties themselves or a judgement imposed by the third-party; outcomes may be non-binding on both parties, binding only on one of the parties, or binding on both parties.

5. Assisted negotiation (or conciliation) is an informal process whereby a neutral third-party guides the parties towards a compromise.

6. Arbitration is a process whereby the parties submit the facts of their dispute and their arguments (oral and/or written) to one or several independent decision-makers who decide the case on the basis of equity or law. Arbitration is legally binding and most often final.

7. See Appendix A.

8. www.oecd.org/dataoecd/39/13/1840065.pdf.

9. DSTI/CP(98)12/FINAL.

10. The *Guidelines for Consumer Protection in the Context of Electronic Commerce,* approved on 9 December 1999 by the OECD's Council, available at: www.oecd.org/document/51/0,2340,en_2649_34267_1824435_1_1_1_1,00.html.

11. DSTI/ICCP/REG/(99)15/FINAL, declassified on 15 September 2000, available at: www.olis.oecd.org/olis/1999doc.nsf/LinkTo/dsti-iccp-reg(99)15-final.

12. Available at www3.ftc.gov/os/2000/02/altdisputeresolutionfrn.htm.

13. Information available at: www.ita.doc.gov/td/industry/otea/ecommerce/apec/.

14. See www.gbde.org/acrobat/miami00.pdf.

15. 123Settle.com, for example, allows parties at the outset either to sign an agreement to be bound by the automatically-generated outcome or to view their settlement figure first (if the case reaches settlement) and then determine whether or not to sign a binding agreement to fulfill the settlement. At least one other system under development, OnlineDisputes.org, does not require parties to be bound by the outcome; furthermore, it allows parties to settle more than cash-based disputes, such as consumer exchange of products.

16. eBay refers customers with disputes to SquareTrade via its Web site.

17. Benshop, Albert, *Peculiarities of Cyberspace "Building Blocks for an Internet Sociology"*.

18. Albert Benshop, ibid.

19. For example the OECD Privacy Guidelines, the OECD Consumer Protection E-commerce Guidelines, or any other international set of rules or guidelines.

20. The parties or the court of arbitration can refer to a *juge d'appui* where there are difficulties in the organisation, the implementation and the enforcement of the arbitration procedure. This particular judge does not have a competitive role, but is complementary to and co-operates in the arbitration procedure. The *juge d'appui* may be asked to intervene in the constitution of the court of arbitration (either *ab initio* or during the course of the arbitration procedure, if the tribunal is truncated and the remaining parties or arbitrators cannot reach agreement to rectify the situation). The *juge d'appui* may also be called upon, in particular, in cases of urgency, (although all national laws do not allow this role), in cases of difficulty in obtaining proof (more rarely), and to compel the enforcement of measures ordered by the court of arbitration. His exact role depends on the law applicable to the arbitration, which may be different to that applicable to the root of the dispute, and to that applicable to the arbitration procedure itself.

21. An electronic signature signifies any action that expresses the intention to sign (agree on, accept), such as a name attached at the end of an e-mail, a click on "I agree" button on screen or the use of a certification authority's e-signature. When an e-signature is certified by some method to assure the identity and/or authenticity of the signed document, it becomes electronic authentication. In other words, electronic authentication can be understood to encompass any method of verifying some piece of information in an electronic environment, whether it is the identity of the author of a text or sender of a message, the authority of a person to enter into a particular kind of transaction, the security attributes of a hardware or software device, or any one of countless other pieces of information that someone may want to be able to confirm in the electronic world.

APPENDIX A: ONLINE ADR MECHANISMS

Online ADR provider	URL	Type(s) of disputes settled	B2B, B2C or C2C disputes	ADR method used	Languages	Geographic origin	Funding source
123Settle	https://ssl-073.imconline.net/123settle/details/ Mediation_Init.asp	all	B2B, B2C, C2C	automated negotiation; mediation; arbitration	English (Spanish to come)	USA	user fees
AllSettle	www.allsettle.com	insurance only	B2C	automated negotiation	English	USA	fees to insurance company
BBBOnline	www.bbbonline.org	all consumer	B2C	conciliation, mediation, arbitration	English	USA/Canada	business membership fees
clickNsettle	www.clicknsettle.com	all financial	B2C	automated negotiation	English and Spanish	USA	user fees
Cyberarbitration	www.cyberarbitration.com	domain name; all other	B2C, B2B, C2C	arbitration	English	India	
Cybercourt	www.cybercourt.org	all online disputes	B2B, B2C, C2C	mediation	English and German	Germany	TBD
Cybersettle	www.cybersettle.com	all financial	B2C	automated negotiation	English and French	USA	user fees
E-Mediation	www.e-mediation.nl	all	B2B, B2C, C2C	mediation	Dutch, English	Netherlands	To Be Determined
Consensus Mediation (e-Mediator)	www.consensusmediation.co.uk/index. html	all online	B2B, B2C, C2C	mediation	English	UK	user Fees
eResolution	www.disputes.org/eresolution	domain name; all other	B2B, B2C, C2C	facilitated negotiation, mediation, arbitration	English and French	Canada	user fees
European Advertising Standards Alliance	www.easa-alliance.org	disputes related to advertising claims	B2B, B2C, C2C	various approaches	English and French	EU	member dues
Fsm	www.fsm.de	complaints against members of Association	B2C	arbitration	English, German and French	Germany	member dues
iCourthouse	www.i-courthouse.com/main.taf?&redir=0	all	B2C, B2B, C2C	non-binding arbitration	English (French and Spanish to come)	USA	user fees
ILevel	www.ilevel.com	all	B2C, B2B, C2C	non-binding arbitration	English (French and Spanish to come)	USA	membership fees for membership
InternetNeutral	www.internetneutral.com	all commercial online	B2B, B2C	mediatio	English	USA	user fees
Internet Ombudsman		all commercial online		mediation, arbitration	German and English	Austria	Government/NGO /private sector

Online ADR provider	URL	Type(s) of disputes settled	B2B, B2C or C2C disputes	ADR method used	Languages	Geographic origin	Funding source
(Austria)							
Internet Ombudsmannen (Sweden)		all commercial online			Swedish	Sweden	Government
IRIS Mediation	www.iris.sgdg.org/mediation	all commercial online	B2B, B2C, C2C	mediation	French	France	
MARS (SuperSettle; Fair□ other)	www.resolvemydispute.com	all (Fair&Square -online only)	B2C, B2B, C2C	automated negotiation; mediation; arbitration	English (Spanish, French, Chinese to come)	USA	user fees
Mediate-Net		family disputes		mediation	English	USA	free during trial
NEWCourtCity .com (Virtual Mediator & Online Mediation)		all financial	B2B, B2C, C2C	automated negotiation, mediation, legal consultation	English, Spanish	USA	user fees
NovaForum	www.novaforum.com/main	all	B2B, B2C, C2C	facilitated negotiation; mediation, arbitration	English, French, German, Portuguese, Polish, Russian, Ukrainian, Cantonese, Mandarin	Canada	business subscriber fees
Online Mediators		all	B2B, B2C, C2C	mediation	English	USA	user fees
Online Ombuds Office	www.ombuds.org/center/index.html	all consumer	B2C	mediation, ombuds services	English	USA	public/private grants
OnlineDisputes	www.robindownes.com/OnLineDisputesWebsite/OnLineHomePg.html	all commercial	B2C, B2B, C2C	automated mediation	English, Spanish	USA	business subscriber fees
Resolution Forum	www.resolutionforum.org	all	B2C, B2B, C2C	facilitated negotation; mediation	English, Spanish	USA	user fees
SettlementNow		insurance only	B2C	automated negotiation	English	USA	user fees
SettleOnline	www.settleonline.com	all financial	B2C, B2B, C2C	automated negotiation	English, Spanish	USA	user fees
SettleSmart		all financial	B2C, B2B, C2C	automated negotation	English,	USA	user Fees
SettleTheCase	www.settlethecase.com/main.html	all	B2B, B2C, C2C	mediation, arbitration, summary jury	English	USA	user fees
SquareTrade	www.squaretrade.com	all online	B2C	facilitated negotiation, mediation	English	USA	business subscribers; user fees
The Virtual Magistrate	http://vmag.org	all consumer online	B2C	non-binding arbitration	English	USA	funded by law school

Online ADR provider	URL	Type(s) of disputes settled	B2B, B2C or C2C disputes	ADR method used	Languages	Geographic origin	Funding source
TRUSTe	www.truste.org	online privacy disputes	B2C	conciliation/negotiation	English	USA	business subscriber fees
USSettle	www.ussettle.com	all financial	B2C, B2B, C2C	automated negotiation	English	USA	user fees
WebAssured	www.Webassured.com	all consumer online	B2C	mediation	English	USA	business membership fees
Web Dispute Resolutions		all online	B2C, B2B,	mediation, arbitration	English	USA	user fees
WEBdispute.com	www.Webdispute.com	all online commercial	B2B, B2C	arbitration	English	USA	user fees
Webmediate	www.Webmediate.com	all	B2C, B2B, C2C	mediation, arbitration	English	USA	business subscriber and user fees
Which WebTrader	www.which.net/Webtrader	all consumer online	B2C	ombuds service	Language of host country	UK, NL, BG, IT, FR, SP, PO	member and subscriber fees; other?
WIPO	http://arbiter.wipo.int/domains/index. html	domain name	B2B, B2C	arbitration	English, French, Spanish	Switzerland	user fees

Source: OECD.

APPENDIX B: POSSIBLE PROCEDURAL, SUBSTANTIVE AND OTHER ELEMENTS THAT MIGHT EXIST IN ADR MECHANISMS

The following list of questions is based on a factual survey of existing ADR mechanisms and is meant to spur conversation and discussion among conference participants in thinking about the variety of procedural and substantive elements that might exist in ADR mechanisms.

1. GENERAL

1.1. To what parties is ADR offered?

B2B
B2C
C2C
G2C (Government to Consumer)

1.2. What type(s) of dispute is ADR offered for?

Auctions
B2C contractual disputes
Copyright
Domain name disputes
Family disputes
Insurance
Intellectual property disputes
Other financial
Personal injury
Other

1.3. What type(s) of ADR are offered?

Automated negotiation
Assisted negotiation (facilitation, conciliation)
Mediation
Med-arb or other combination of traditional ADRs
Arbitration
Non-governmental ombuds-type
Non-governmental tribunals
Other

1.4. What is the background of entity offering ADR?

Business organisation/industry group
Consumer organisation
International governmental organisation
National governmental organisation
Law firm
Local governmental organisation
University
Association of former judges or lawyers (or other similar professional group)
Other

Were other types of organisations consulted when the ADR programme was being developed and implemented?
If so, which organisations (*e.g.* government, consumer group)?
What was the role of this organisation (*e.g.* funding, approval, referral, recommended practice)?
Has the ADR provider sought partnerships with any other organisation providing ADR?
Does the ADR provider represent that it complies with Guidelines governing the procedures of ADR issued by an organisation?
If so, which organisation?

1.5. Has the ADR programme been certified and/or been granted a trustmark/seal?

If yes, by whom?
What does the certification and/or trustmark seal granting process entail?

1.6. Cost of ADR to the Parties:

Is there a fee for the ADR service?
What kind?
Free
Flat fee
Fee contingent on value of dispute
Fee split among parties
Other (*e.g.* fee calculated on value of claim)

1.7. What is the average length of a dispute?

1.8. Statistics:

What is the number of disputes dealt with?
If applicable, how does the number of cases dealt with compare to the overall number of transactions?
What is the number/percentage of disputes successfully resolved?
Where applicable, what is the number/percentage of outcomes appealed to a court or other body?
Was the number/percentage of outcomes in which there were compliance problems reported?

1.9. When was the ADR programme established?

1.10. Socio-economics:

What is the geographical location(s) of entity offering ADR?
In which countries has the service been provided?
In what language has the service been provided?
Are there restrictions on the places or language in which the ADR service can be provided?
Which language are the proceedings held in?
Who chooses the languages to be used in the ADR proceedings and on what basis?
Are cultural differences taken into account?

1.11. Has there been any survey of customer satisfaction with the programme service?

If so, what are the results?

2. SUBSTANTIVE RULES STANDARDS OR GUIDELINES (INCLUDING VOLUNTARY SELF-REGULATORY CODES)

2.1. On which basis is the ADR established

General fairness
International rules, standards or guidelines
National rules, standards or guidelines
Other

3. RULES OF PROCEDURE

3.1. Voluntary vs. mandatory ADR and Binding vs. non binding ADR outcomes:

Do both parties voluntarily agree to ADR?
Is participation in the ADR programme required before a party can take a dispute to court?
Is there a pre-dispute binding ADR clause in the agreement that binds both parties to the outcome of the ADR?
Is there a pre-dispute binding ADR clause in the agreement that binds one party to the outcome of the ADR?
Are the parties permitted to enter into ADR that is binding on both parties after a dispute arises?
Are the parties permitted to enter into ADR that is binding on one party after a dispute arises?

3.2. Content of the rules of procedure:

Does the ADR only require fairness and good faith?
Does the ADR provide for parties agreeing to establish their own rules?
Does the ADR apply any established rules of procedure (e.g. UNCITRAL, ICC, ICANN/WIPO (UDRP) procedure)?
Does the ADR apply its own specific or supplemental rules of procedure in addition to any established rules?

4. PROCEEDINGS

4.1. Are the proceedings conducted:

Totally online?
Both on and offline?
Totally offline?

- By mail?
- Face-to-face?

4.2. Means of communication:

E-mail
Online forms
Tele/video conferencing
Telephone
In person
Other

4.3. Is translation/interpretation provided/available?

4.4. Are there time limits to the proceedings?

4.5. Can the parties be represented or assisted?

4.6. Is there a right/opportunity for a face-to-face hearing?

4.7. Adversarial procedure:

Are parties required to provide details of their arguments to each other?
Are parties able to respond to each other's arguments?

4.8. Accessibility and transparency:

What kinds of advertising/marketing does the ADR programme engage in?
How does the ADR programme make the parties aware of its existence?
At what point in a transaction is the availability of an ADR programme disclosed (*e.g.* home page, user agreement page)?
How is such a disclosure made?
What information about the ADR programme is provided?

5. NEUTRAL (S)

5.1. Who chooses the neutral:

The parties
The ADR provider

5.2. Can the parties choose a three-person or other type of panel? If so, how?

5.3. From where are the neutral(s) chosen?

List offered by the ADR provider?
List offered by another ADR entity, such as a professional association of ADR providers?
Other

5.4. Can the parties challenge the appointment of an intermediary? If so, how?

5.5. What experience is required of an intermediary?

IT
Legal
Experience of ADR techniques
Expertise related to topic of dispute
Professional Organisation Certification
Other

5.6. What is the role of the intermediary:

Assist the parties to reach an agreement
Evaluate the substantive merits of the case
Evaluate the procedural merits of the case
Determine the investigations to be made
Recommend interim orders or emergency relief
Recommend the outcome
Impose the outcome
a) In writing
b) With reasons

5.7. Is impartiality of a neutral required? If so, how is this ensured?

5.8. Does the neutral volunteer his/her services?

6. CONFIDENTIALITY

6.1. Are the neutral and ADR provider required to keep the following information confidential?

The existence of proceedings
Information exchanged during proceedings
The outcome of proceedings

6.2. Are the parties required to keep the following information confidential?

The existence of proceedings
Information exchanged during proceedings
The outcome of proceedings

6.3. How much information regarding individual decisions is made public, such as the factual circumstances of the case, the outcome only, etc.? How is the disclosure decided upon?

6.4. Are the parties, neutrals and ADR providers permitted to refer complaints / disputes / outcomes about fraudulent or deceptive ADR practices to law enforcement?

7. SECURITY

7.1. Are security measures taken to protect the confidentiality and integrity of personal information held by the ADR provider? If yes, how (*e.g.* password/encryption/ authentication)?

7.2. Are security measures taken to protect the confidentiality and integrity of communications during the proceedings? If yes, how (*e.g.* password/encryption/authentication)?

8. OUTCOME OF ADR

8.1. Is the outcome notified to third parties?

8.2. If the parties do not voluntarily perform the decision rendered under the ADR programme, does the ADR programme have any mechanism to enforce the decision (*e.g.* posting a bond, using chargebacks, revoking a seal, etc.)?

8.3. If a party wishes to dispute an outcome:

Are the grounds for the dispute specified by the ADR scheme?
Is the applicable law prescribed in advance?
Is the applicable forum prescribed in advance?

9. DISPUTES WITH ADR PROVIDER

9.1. Does the ADR provider limit its legal liability?

9.2. If a party wishes to dispute that liability:

Is the applicable law prescribed in advance?
Is the applicable forumprescribed in advance?

Chapter 9

LEGAL PROVISIONS RELATED TO BUSINESS-TO-CONSUMER ALTERNATIVE DISPUTE RESOLUTION IN RELATION TO PRIVACY AND CONSUMER PROTECTION

This chapter addresses the extent to which existing national legal provisions may impact recourse to alternative dispute resolution (ADR) in relation to electronic commerce. It presents a synthesis of member country responses to the Questionnaire on Legal Provisions related to Business-to-Consumer Alternative Dispute Resolution (ADR) in relation to Privacy and Consumer Protection (attached as an appendix) and provides a summary of the main points, an introduction to the project, a synthesis of the responses received, and a few concluding remarks.

Chapter 9

LEGAL PROVISIONS RELATED TO BUSINESS-TO-CONSUMER ALTERNATIVE DISPUTE RESOLUTION IN RELATION TO PRIVACY AND CONSUMER PROTECTION

Main points

Although the numerous national instruments related to alternative dispute resolution (ADR) reported by member countries are not specific to the online environment,[1] their collation helps provide a general picture of the nature and scope of application of existing provisions related to ADR in most OECD member countries, and may serve as the basis for further work to facilitate online ADR at the cross-border level.

Member countries recognise the potential benefits of, and encourage informal ADR.

A common theme echoed throughout the responses is the importance member countries attach to informal ADR. In the majority of countries, policy initiatives recognising the potential benefits of ADR have been developed. These initiatives aim at increasing the availability of effective, timely and cheap mechanisms as an alternative to formal court-based dispute resolution.[2]

Offline ADR schemes that are established, funded or run by governments are common in member countries.

Legal provisions that establish particular types of offline ADR schemes, such as court-annexed ADR or ADR for landlord-tenant disputes, are common in member countries. They vary from consumer ombudsmen to arbitration boards to conciliation courts. The scope of their competence is usually limited to either a particular type of dispute or a specific sector. Recourse to these schemes may be mandatory or encouraged.

There is little broad-based regulation addressing ADR in member countries: the general picture is a patchwork.

Member countries have no overarching framework regulating formal and informal ADR. Although many countries regulate arbitration, informal types of ADR remain largely unregulated. However, many countries described provisions that apply to business-to-consumer (B2C) disputes in specific contexts. Rules have been developed for different types of ADR depending on the subject matter of the dispute (*e.g.* privacy); the underlying transaction (*e.g.* insurance, telecommunications); the size, value and complexity of the dispute; whether arbitration or mediation is involved, etc.

In most member countries, parties generally are free to agree to non-binding ADR on a contractual basis.

Recourse to informal B2C ADR is not subject to specific legal limitations. In most countries, parties are free to agree to ADR on a contractual basis, subject to the restrictions that apply generally to contracts such as fraud, duress or public policy concerns (*e.g.* unconscionability, non-waivable rights, clauses unfair to an individual, and concerns of equity and fairness). These considerations appear to be a general limit to recourse to, and implementation of mandatory or binding ADR.

Introduction

In order to gain a better understanding of the role ADR can play in enhancing user and consumer confidence in e-commerce, the OECD, the International Chamber of Commerce and The Hague Conference on Private International Law organised a joint conference on online ADR in relation to privacy and consumer protection, that was held in The Hague in December 2000. The conference explored the use of online ADR systems for disputes involving small values and/or low levels of harm that arise between businesses and consumers online. The primary focus was on informal, flexible systems that allow for the necessary balancing between the type of dispute and the formality of the process for resolution.

At their February 2001 and March 2001 meetings, the Working Party on Information Security and Privacy (WPISP) and the Committee on Consumer Policy (CCP) decided to follow up on The Hague Conference with the aim of raising user and consumer awareness about online ADR and encouraging recourse to fair and effective B2C online ADR. This follow-up work included three elements: an updated inventory of online ADR mechanisms, an educational instrument for potential parties to online ADR, and a questionnaire on legal issues.

The questionnaire on legal issues (see Appendix) was developed by the secretariat with input from WPISP and CCP delegates participating via an electronic discussion group. In June 2001, the questionnaire was finalised and sent to member countries and stakeholders for response.

The secretariat received responses to the questionnaire from 24 member countries, including Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Hungary, Italy, Japan, Korea, Mexico, Netherlands, New Zealand, Poland, Slovak Republic, Spain, Sweden, Switzerland, Turkey, United Kingdom and the United States. Responses were also received from The Research Centre for Computer and Law, University of Namur, Belgium (CRID), *Confcommercio* (The Italian Retail Association), and two online ADR providers, TRUSTe and SquareTrade.

The objective of the questionnaire was to generate an overview of the national legal regimes applicable to B2C ADR in member countries, with a view to understanding if and how existing legal provisions impact recourse to ADR, particularly in relation the online environment. The questions aimed to elicit factual information on the content of legal provisions (both general and specific) applicable to ADR, both in national and cross-border situations.

There are limitations in the conclusions that can be drawn from the answers to the questionnaire. First, it was difficult to respond to the broad range of questions in a completely definitive way. In particular, for countries with legal systems in which competence over ADR is shared by national and regional or local authorities, it was not always possible to describe all relevant regulatory measures. Similarly, the fact that legal provisions related to ADR are not usually grouped together in a unique set of rules made it difficult to provide comprehensive responses. Finally, comparisons between countries were complicated by variations among national definitions of ADR processes (*e.g.* mediation or arbitration).

Despite these limitations, a number of commonalties emerged from the answers given by member countries.

General provisions on ADR

Some member countries have specific provisions that require or encourage parties to have recourse to informal ADR for certain types of disputes. Aside from legal provisions, a majority of countries referred in responses to general policies of encouraging consumers to have recourse to informal ADR, particularly where government schemes have been made available. Other countries have specific provisions prohibiting or limiting recourse to ADR in certain circumstances.

Provisions encouraging or requiring ADR

Australia, Canada, Italy, Japan, New Zealand, the United Kingdom and the United States have provisions that encourage recourse to ADR for certain disputes. In the United Kingdom, pre-trial protocols for defamation, personal injury, clinical disputes, professional negligence and construction and engineering matters encourage recourse to ADR. In Australia, the Fair Trading Tribunal Act 1998 expressly encourages the use of ADR in resolving disputes brought before the tribunal.

Austria, Canada, France, Germany, Italy, Japan, New Zealand, United Kingdom and the United States have provisions that, in certain circumstances, explicitly require parties to exhaust ADR prior to seeking judicial remedies.

Provisions requiring ADR before a complaint is filed

Some countries require parties to exhaust ADR in certain circumstances prior to filing a complaint in court. For instance, Germany has regional legislation requiring parties to attempt conciliation for disputes relating to property law, involving small claims for compensation, neighbourhood law and claims over damage to personal reputation. In Austria and Switzerland tenancy disputes should be taken to a specific ADR administrative body. In France if agreement cannot be reached on rent when a lease is being renewed, the parties must refer the matter to the *Commission Départementale de Conciliation* before applying to the courts.[3]

Provisions requiring ADR after a complaint is filed (court-annexed programmes)

Some countries have legislation that allows courts or tribunals to require parties that have filed complaints before them to go to ADR in appropriate circumstances for matters within their jurisdiction. Countries that referred to such provisions include Australia, Canada, Italy, Japan, New Zealand and the United States. For example, in Australia, the 1994 Tenancy Tribunal Act requires mediation as a first method for dispute resolution between parties seeking the intervention of the tribunal. As a further example, in Canada, state-based legislation requires all parties to civil disputes to attend a mediation session at the close of pleadings before any further step can be taken in the case. In British Columbia, Canada, a mandatory settlement conference conducted informally by a judge is part of a small claims court initiative.

In a similar development, the Netherlands noted that it has recently initiated court-annexed mediation projects on an experimental basis in five different courts throughout the country. As part of the programme, judges can request that parties try to reach a solution with the help of a mediator in specific administrative and civil (including family mediation) cases. Further, in the United States, pursuant to a range of legislation, some state and federal courts require litigants to exhaust ADR first as a matter of course, after a complaint is filed, before the trial can continue. For example, in Maine, in most civil cases, after filing a complaint in court, parties must schedule an ADR conference to try to resolve the dispute.[4]

Provisions prohibiting or limiting recourse to ADR

Some countries have provisions prohibiting or limiting recourse to ADR. France, Germany and Italy noted that parties could not generally seek to resolve disputes involving inalienable or non-disposable rights through ADR (*e.g.* divorce, familial disputes, etc.). Similarly, Mexico referred to legal provisions that prohibit certain matters such as familial conflicts and divorce to be resolved by arbitration.[5] In the United States, while the parties cannot be required to go through court-annexed ADR for certain disputes notably involving constitutional rights,[6] they can voluntarily agree to try to resolve them through private ADR.

Denmark, Finland, Germany, Korea, Netherlands, Poland, Spain, Sweden and Switzerland have set up national ADR schemes to which recourse is not permitted for certain types of cases (*e.g.* below a specified monetary value) and/or to certain parties [*e.g.* exclusion of business-to-government (B2G) disputes]. In the Netherlands certified complaints boards are not able to deal with a range of disputes including those relating to death, physical injury or illness. Further in Switzerland, under the *Concordat* (agreement on arbitration), the parties are not free to use arbitration if the case comes under the exclusive jurisdiction of a state authority.

Exhaustion of ADR

Few member countries report having specific provisions that would affect the validity of a contractual agreement to exhaust recourse through ADR prior to seeking redress through the courts.

Korea, New Zealand, the United States and Spain indicated that contracts to exhaust ADR would, in practice, likely be enforceable. For example, in the United States, such a contract would generally be upheld unless the parties seeking to invalidate it can show that it was procured by fraud, duress, mistake, unconscionability or illegality. Australia, Canada and Japan reported that parties could enter contracts to exhaust ADR. However, they stressed that such contracts may be set aside or declared invalid by the court as an "unfair contract term" or because of some other irregularity such as procurement by undue influence, violation of public policy or restriction on consumer access to ordinary legal remedies.

The majority of European Union countries referenced the EU Directive on Unfair Contract Terms that, *per se*, does not allow consumers to give up their right to go to court. They also mentioned national implementing legislation as further bases on which a contract could be invalidated if its effect were to restrict access to ordinary legal remedies. For instance, Austria noted provisions in its Consumer Protection Act which declare invalid a contract that deprives a consumer of his/her right to bring a matter before court. Similarly, Italy referred to its Civil Code which states that any clauses in B2C contracts that concern or entail exceptions to the competence of judicial authorities are presumed to be abusive. Other countries to reference national legislation on unfair contract terms or the EU Directive in this context included Denmark, Finland, France, Italy, Netherlands, Sweden and the United Kingdom. In a similar but broader approach, Mexico noted that its Federal Consumer Protection Law also invalidates clauses that are generally "against consumers' rights".

Binding ADR

In general there are no specific provisions that prohibit contractual agreements between parties to be bound by ADR after a dispute has arisen, and, *a fortiori,* at the end of the ADR process. For example, Austria, France and Italy noted that in the case of agreements signed at the conclusion of an ADR process, contractual autonomy is recognised and agreements signed by the parties will be binding according to contract law.

However, the general practice appears to be that contractual provisions binding parties to ADR prior to a dispute having arisen may be regarded as an "unfair" contract term or contrary to public policy, notably if it deprives the consumer to the right to go to court. Countries which adopted this approach included Australia, Austria, Canada, Denmark, Finland, Italy, Japan, Netherlands, Spain and Sweden. Legislation in Sweden and France for example mandates that consumer contracts entered prior to a dispute containing an arbitration clause are automatically invalid as unfair. Similarly, in the United Kingdom, an arbitration agreement is automatically void as unfair for consumers specifically if it relates to a claim for a small amount.

New Zealand and the United States noted that, in practice, a consumer is free to consent to be bound by ADR but that contract law will apply to ultimately determine the validity of a contract to engage in and be bound by ADR. For example, in the United States, a contract is not invalid simply because it deprives the consumer of the right to go to court – the validity of a contract in this situation is decided on a case-by-case basis. The general rule is that such contracts are valid, irrevocable, and enforceable, except where they violate general principles of contract law, such as fraud, duress or unconscionability. Legislation in Japan also indicates that an agreement to refer future disputes to arbitration is valid as long as it relates to determined relations of right and disputes arising therefrom.

Implementation and judicial enforcement of ADR outcomes

Many ADR outcomes are implemented by the consent of the parties and thus do not require further third-party intervention. However, when one party refuses to abide by an ADR agreement, many countries indicated that they have mechanisms for enforcement of ADR agreements. It remains unclear, in the B2C cross-border context, how an ADR outcome involving nationals from different countries can be enforced.

Japan, New Zealand, the United Kingdom and the United States indicated that ADR outcomes such as mediation or conciliation can be judicially enforced under basic contract principles. Other countries have specific legislative provisions that provide mechanisms for the enforcement of domestic ADR outcomes. For instance, in the Netherlands, agreements reached after a mediation procedure can generally be brought to court to be confirmed by a judge. Further in France, in cases of non-judicial conciliation, if the parties agree, the court may be asked to give binding force to their agreement.[7]

Some countries also indicated that ADR agreements made during the course of proceedings (for example in the context of court-annexed ADR) can be given the status of judgements on application to the court if both parties consent. Australia, France, Japan, the United States, and the United Kingdom referred to this approach. For instance, in France, the courts have a general conciliatory role such that if the parties reach settlement during a procedure, they may at any time ask the court to record their agreement or the court can itself prepare a conciliation agreement to be signed by the parties. Canada also indicated similarly that an ADR outcome can be enforced with the consent of the parties in which case an ADR agreement forms the basis of a consent order issued with the same status as any other court order.

Austria, Germany, Hungary, Italy, Korea, Mexico, Poland, Spain, Switzerland and Turkey indicated that ADR decisions rendered by bodies operating under national schemes can be enforced in some circumstances. For example in Mexico, under the Federal Consumer Protection Law, outcomes issued or agreements approved by PROFECO (the Consumer Protection Attorney's Office) under its conciliation and arbitration procedures have the nature of final judgements and must be fulfilled by the parties or enforced by the courts. Also in Austria, an outcome delivered by the relevant ADR body concerning Landlord and Tenant Law constitutes an "executory title" and as such is therefore enforceable provided the dispute isn't pursued in court within four weeks of service of the ADR outcome. Conversely, Denmark and Finland indicated that the decisions or recommendations of Consumer Complaints Boards are not enforceable or binding.

Finally, a few countries mentioned specific legislative limits on implementation of ADR outcomes awarded by particular statutory ADR bodies or in the context of arbitration. For example, in Japan, under the Law of Public Summons Procedure and Arbitration Procedure, either disputant can apply for the annulment of an award if one of a number of circumstances exist, including for instance, if the award requires a party to undertake an act prohibited by law. Under UK arbitration legislation, an arbitration agreement can be "set aside" if the court is satisfied that the agreement is "null and void", inoperable or incapable of being performed. Further, in the Netherlands, when the outcome of an arbitration or binding advice procedure is manifestly in conflict with public morals or public policy, its implementation will be

affected.[8] Other specific legislative provisions exist in Czech Republic, France, Mexico, Poland, Switzerland, Turkey and the United States.

Procedural safeguards for ADR

In some member countries there are legal provisions imposing certain procedural safeguards for a broad range of ADR programmes. Other countries have procedural safeguards only for a particular type of ADR or ADR for a particular type of dispute.

Confidentiality

The United States cited specific legislation providing for confidentiality of ADR proceedings or outcomes. The United States noted that there are some state-based regulations which ensure confidentiality. For example, Ohio's mediation confidentiality statute requires mediation communications to be confidential, subject to a number of exceptions.[9]

Confidentiality rules for government-run ADR schemes appear to vary. In Sweden the existing ADR body is a public authority such that all processes are usually public but a decision can be made confidential if it contains delicate personal or business information. A similar approach is taken in Poland where Court of Conciliation cases are public unless disclosure would be against public policy or would reveal state/business secrets. Similarly, in Denmark, Finland, and Korea, legislation aimed at ensuring public access to public processes applies to government run ADR bodies to override any agreement as to confidentiality. For example, in Denmark, the Open Administration Act would apply such that information regarding the proceeding of an ADR or an ADR outcome can be given to a third party on demand.

Conversely, in Switzerland, arbitration procedures in state-run bodies are usually confidential but if a party appeals against a decision, the appellate authority is entitled to all relevant information on the ADR process.

Australia, France and Japan referred to safeguards applicable to ADR in the judicial context (or court-annexed ADR). For example, in France there are safeguards imported in the procedures of conciliation undertaken by judicial conciliators and mediation proceedings conducted by court appointed mediators. These safeguards notably guarantee the confidentiality of the proceedings. Further, in Japan, conciliation cases, under the Law of Conciliation of Civil Affairs, are confidential but the parties and the persons interested in the case can request perusal or copying of the record of the case unless it would obstruct the keeping of the record or the functions of the court. Legislation in some countries actually deems information arising from an ADR process as inadmissible as evidence. For example, in Australia the Federal Court Act provides that evidence of anything said, or of any admission made at a court-annexed mediation session, is inadmissible in any court or proceedings.

However, several member countries indicated that, in practice, parties may be compelled under some circumstances to disclose information in relation to an ADR proceeding, regardless of whether the parties have agreed to keep the proceedings confidential. Australia, Canada, France, Italy, Mexico, Netherlands, New Zealand,[10] Switzerland and the United Kingdom outlined this approach. For example, Mexico noted that, under the Federal Consumer Protection Law, authorities, ADR providers and consumers must provide PROFECO, the Consumer Protection Attorney, with any information needed for legal procedures. Also, Australia and Canada noted that ADR practitioners (mediators, etc.) are ethically obliged to disclose certain information if that were necessary to prevent serious harm. Australia and Canada noted further that courts appear to have a general discretion in this context: they may respect confidentiality on the grounds of public interest but, equally, may decide that public interest considerations override the confidentiality agreement.

Qualifications/neutrality of ADR provider

Most member countries indicated that there are legal provisions that specifically regulate the qualifications and neutrality of ADR practitioners in court-annexed/court-referred ADR. Countries referring to such regulation include Australia, Canada, France, Japan, the Netherlands and the United States. For example, in France, the Code of Civil Procedure lays down requirements for judicial conciliators and mediators, including for example that conciliators must have at least three years' experience in law, but there are no mandatory general conditions for non-judicial services. Further, in the United States, some state courts or legislatures impose training or experience standards on mediators who practice in state or court-funded mediation programmes.

Austria, Denmark, Finland, Germany, Hungary, Italy, Japan, Korea, Mexico, Poland, Slovak Republic, Spain, Sweden, Switzerland and the United Kingdom cited provisions regulating the qualifications and neutrality of ADR practitioners in statutory ADR bodies. For instance, in Denmark, the legislation establishing the Consumer Complaints Board has provisions that detail how the board is to be composed (and therefore who can act as an intermediary).

There also appear to be some rules on qualifications and neutrality of general ADR services in some member countries. Australia referred to state/territory legislation that deals with accreditation of mediators. Japan reported that competent ministers must certify organisations that intend to settle privacy/personal information disputes. Japan also reported that people who engage in ADR "for profit" must be qualified as lawyers in principle. In the United States, ADR providers are largely unregulated. In most states, a person can offer private mediation services without taking a class, passing a test or having a special license or certification. In practice, however, most independent mediation programmes and mediation membership organisations impose their own training or experience standards on mediators.[11] Finally, New Zealand noted that practising lawyers usually provide ADR and are subject to ethical requirements and disciplinary procedures. Czech Republic and Mexico also cited provisions applying in the context of arbitration. For example, in Mexico, the Federal Consumer Protection Law contains regulations for registration of independent arbitrators in consumer disputes.

Other procedural safeguards

Canada, Czech Republic [only business-to-business (B2B)], Japan, Mexico (only B2B), Netherlands, New Zealand, the United Kingdom and the United States stated that certain procedural safeguards applied to arbitration. For example, in New Zealand, the *Arbitration Act* 1996 contains a number of procedural requirements and provides that agreements may be set aside if the party making the application was not given proper notice of the appointment of an arbitrator or of the arbitral proceedings or was otherwise unable to present that party's case.

Australia, Austria, Denmark, Finland, Italy, Korea, Mexico, Netherlands, Poland, Spain, Sweden and Switzerland indicated that public authorities and bodies conducting national or state ADR schemes must observe certain safeguards. For instance, in Korea, legal provisions outline some procedural safeguards that apply to the ADR processes conducted by the Consumer Dispute Settlement Committee, such as composition of the Committee, term of its members, quorum for decisions, and deadlines for reaching a decision.

In terms of general regulation of ADR processes, the United States cited some specific provisions governing procedures for B2C disputes over warranties. The Magnuson Moss Warranty Act requires the US Federal Trade Commission to establish minimum requirements for disputes resolution procedures. As such, any consumer dispute resolution mechanism under the Act must, *inter alia*, be able to settle disputes independently, without influence from the parties involved; follow written procedures; and provide each

party an opportunity to present its side, to submit supporting materials and to rebut points made by the other party. There are also some state-based regulations which uphold the right to representation in mediation negotiations. For example, Alaska and North Dakota statutes prohibit mediators from excluding an attorney from the mediation table.

Aside from legal provisions, some other regulatory initiatives that seek to import safeguards into ADR were noted. Both the EU Commission Recommendation on the Principles Applicable to the Bodies Responsible for Out-of-Court Settlement of Consumer Disputes and Benchmarks for Industry-Based Dispute Resolution (a co-regulatory initiative) in Australia were cited in this context.

New Zealand and the United Kingdom also noted that some procedural safeguards may be introduced into ADR processes in a "*de facto*" sense, given that mediators, conciliators and other third party neutrals are often required to adhere to professional codes of conduct. For instance, in New Zealand most ADR is undertaken by lawyers who are subject to ethical requirements and disciplinary procedures which may serve to introduce some procedural safeguards, particularly around independence, impartiality and transparency.

Finally, the United States mentioned the existence of voluntary guidelines for ADR providers conducting B2C disputes.[12]

The patchwork of existing ADR mechanisms

No member country reported the existence of an overarching regulatory framework for B2C ADR. However, many countries described provisions that apply to B2C disputes in specific contexts. Rules have been developed for different types of ADR depending on the subject matter of the dispute (*e.g.* privacy) or the underlying transaction (*e.g.* insurance, telecommunications); the size, value and complexity of the dispute; whether arbitration or mediation is involved, etc.

Most countries offer some sort of government-established, funded or run programme to resolve certain B2C disputes. These programmes can be split into two categories: mixed public-private ADR and government-established, funded or run ADR.

Mixed public-private ADR

Some countries have developed ADR schemes that result from a mix of public sector-private sector initiatives. For example, Australia has legislation through which industry-developed codes of conduct (which often incorporate ADR provisions) can be made mandatory. For example, an Australian franchising code of conduct provides for the referral of franchising disputes to the Office of the Mediation Adviser. Australia also has a mix of public-private sector initiatives in the privacy area, which provide that if the consumer and business are unable to resolve privacy disputes between themselves, the consumer can request that an independent person investigate the complaint. Where the business concerned is subject to an approved privacy code that includes a mechanism for handling complaints, the independent investigator will be an adjudicator nominated under the code. Where the business is not subject to an approved privacy code, the Federal Privacy Commissioner will handle the complaint. In Austria, in the area of telecommunications, an independent industry body serves, *inter alia*, as a conciliation office, and telecommunication providers are obliged to participate in the procedure.

The Slovak Republic reported legislation that entitles non-governmental consumer associations to mediate disputes arising between consumers and business. There are two umbrella consumer associations operating in the whole of the country as well as several regional organisations. Slovak distance and doorstep selling legislation also entitles consumer associations to mediate disputes in that sector.

Government-established, funded or run ADR

General consumer complaint bodies

Member countries have established a variety of consumer complaint bodies to deal generally with B2C ADR. Denmark and Finland have established consumer complaints boards, and Australia, Germany, Hungary, Japan, Korea, Mexico, New Zealand, Spain, Sweden, Switzerland and Turkey have established a variety of other related mechanisms. In addition, Poland described an ADR scheme which is a more formal or "court-like" ADR body, the Court of Conciliation. This ADR body was established by the Act on Trade Inspection and involves a formal process commenced by filing a motion before the court. The parties submit to the court's processes voluntarily, but once the authority and procedures of the court are accepted, its decisions are binding equally to the verdicts of common courts and there is no right of appeal. In contrast to this formal procedure, the United States reported that many state attorney general's offices or consumer protection agencies offer voluntary informal dispute resolution programmes to resolve B2C disputes.

Complaint mechanisms for specific industry sectors or specific types of disputes

A number of member countries also have established government-run B2C ADR schemes or bodies that deal only with consumer complaints from a particular industry or sector or particular kinds of disputes.

Australia, Austria, Canada, Finland, Germany, Italy, Korea, Mexico, Netherlands, Spain, Sweden, and Switzerland reported such government-run schemes. For example, in Mexico the National Commission for Medical Arbitration has been established to deal with the arbitration of disputes related to the provision of medical services. Mexico also reported legislation that mandates presentation of claims in the financial services area before the National Commission for the Defence of Financial Services Users.[13] In Canada, the Financial Services Commission of Ontario has been established with a mandate to resolve motor vehicle insurance disputes through mediation and arbitration. In Italy, the law[14] provides for arbitration and conciliation committees to be set up to resolve B2B as well as B2C disputes in respect of the provision of tourism services.

Canada, Korea and New Zealand mentioned government-run or funded schemes in the privacy area. In Korea, the law[15] provides that any person who wants a dispute over his/her personal information mediated can file an application with the Dispute Mediation Committee[16] that investigates the case and proposes a draft mediation to the parties within a 60-day period. In Canada, legal provisions provide that the Privacy Commissioner may either encourage complainants to try to settle privacy complaints directly with the organisation, or initiate his/her own investigations. The Commissioner can make recommendations to an organisation, make public any information about the personal privacy practices of an organisation, or take a complaint to the federal court of Canada. In New Zealand, the law[17] requires the Privacy Commissioner[18] to use his best endeavours to secure a settlement. The method of ADR is not prescribed. In practice, the Privacy Commissioner's complaints process mostly utilises assisted negotiation in conjunction with an inquisitorial process. Where appropriate, the Commissioner will use mediation.

In addition, Australia, Austria, France, Netherlands, and Sweden described special requirements for tenancy disputes. In the Netherlands, the Act on Rental of Public Housing gives tenants the option of bringing their complaint before one of the Tenants Complaints Boards. The parties are deemed to have reached an agreement, as laid down in the decision of the Board, if none of them resorts to the court in the same matter within two months.

Court-annexed ADR

As regards court-annexed or court-referred ADR, Australia, Canada, France, Germany, Italy, Japan, the United Kingdom and the United States described programmes through which courts could refer disputes to ADR. As an example, France mentioned a scheme that provides for judicial conciliation under which a judge may designate a conciliator to assist in amicable dispute resolution if the parties agree. The conciliator must hear the submissions of the parties and at the end of the procedure, inform the judge of the outcome of the process. If an agreement is reached, it is submitted to the judge for formal approval; otherwise, the case continues before the court.

Regulation of ADR outside the B2C realm

Although not a key focus of this research, some member countries briefly discussed regulation outside the B2C realm and referred to specific provisions applying to the ADR of B2B, consumer-to-consumer (C2C), B2G, and consumer-to-government (C2G) disputes.

In particular, Australia, France, Italy, Korea, and Switzerland reported government-run ADR schemes for disputes involving government. For example, Australian provisions[19] prescribe conferences (conciliation) and mediation with respect to administrative decisions by the Commonwealth that may involve business, or consumer, to government matters (for example, taxation), or for the conciliation of consumer complaints against government agencies (for example, disability access, racial discrimination). In Switzerland, some Cantons (regional administrations) have established ombudsman systems for resolution of C2G disputes and disputes between government employees and superiors. Further in Korea, the Environment Dispute Resolution Committee and the Administrative Appeals Committee have been established to manage a range of disputes involving B2G and C2G disputes in the environmental area.

Conclusion

The results of the questionnaire highlight that there is not a single set of rules governing ADR. Different rules have developed in different contexts. In a number of areas the existing legal framework provides guidance to potential parties to an ADR procedure at the national level. For example, many countries regulate the provision of arbitration services. However, there are fewer regulations that would generally govern the provision of less formal types of B2C ADR. What regulation there is typically addresses the provision of ADR through mechanisms established, funded or run by governments.

The OECD has focussed on flexible and informal ADR mechanisms designed for the online world. Here, no member country reported the existence of specific legal provisions although most expressed an interest in promoting fair and effective online ADR as a way to resolve small value B2C disputes, particularly cross-border disputes. Looking more specifically at the cross-border context, there do appear to be national differences as to the validity of agreements to submit to ADR, the procedural principles for use during an ADR, confidentiality and security of proceedings, validity of settlement agreements arising out of an ADR, and the availability of enforcement mechanisms.

The OECD *Guidelines for Consumer Protection in the Context of Electronic Commerce* suggest that ADR may provide a means for addressing consumer concerns in the electronic marketplace. National differences in existing legal frameworks on ADR may affect the operability of ADR in the cross-border context. Member countries, businesses and consumers need to be aware of what kinds of ADR programmes are offered in different countries and what rules they operate under. This document provides an important tool to facilitate such awareness.

NOTES

1. The main legal instrument targeting online ADR is the EU Directive (2000/31/EC) on electronic commerce. This instrument encourages online ADR but does not impose any legal requirements on it.
2. In addition, OECD member countries have adopted guidelines related to the protection of consumers online that call for meaningful access to fair and timely ADR without undue cost or burden.
3. Article 17, Act of 6 July 1989 concerning leases of dwelling houses.
4. Maine Rules of Civil Procedure, Rule 16B.
5. Article 615 of the Federal Civil Procedures Code.
6. The Alternative Dispute Resolution Act states that courts cannot refer parties to ADR after litigation has been filed if the dispute is based on constitutional rights, concerns equal rights protection and voting or the relief sought consists of money damages of an amount greater than USD 150 000.
7. Article 9 of the Decree of 20 March 1978.
8. See for arbitration procedures, Code of Civil Procedure art. 1065.1.e and for binding advice procedures, Civil Codebook 7 art. 902.
9. In addition, ADR experts in the United States are working on a Draft Uniform Mediation Act, which sets forth a general requirement for confidentiality of mediations and enumerates several specific exceptions. These exceptions include: waiver; communications relating to the ongoing or future commission of a crime; record of a signed agreement; meeting and records open by law and public policy mediations; evidence of child abuse and neglect; evidence of professional misconduct or malpractice by the mediator; evidence of professional misconduct; or malpractice by a party or representative of a party.
10. In New Zealand, the Arbitration Act 1996 prohibits the disclosure of information revealed during an arbitration unless the parties agree.
11. *cf.* Draft Uniform Mediation Act mentioned above.
12. See for the United States: www.adr.org; www.arb-forum.com.
13. See *Law for the Protection and Defence of the Financial Services User*.
14. Act n° 580 of the 29/12/1993.
15. Act on the promotion of information and communications network utilisation and information protection (last amendment on 16 January 2001).
16. Established under the Ministry of Information and Communication.
17. Privacy Act, 1993.
18. The Privacy Commissioner is government funded, but is structurally an independent Crown entity.
19. The Commonwealth *Administrative Appeals Tribunal Act* 1975 and human rights legislation.

APPENDIX

QUESTIONNAIRE ON LEGAL PROVISIONS RELATED TO BUSINESS-TO-CONSUMER ALTERNATIVE DISPUTE RESOLUTION IN RELATION TO PRIVACY AND CONSUMER PROTECTION

For governments, please answer the questions with regard to any "legal provisions" – any domestic laws or regulations, including court decisions (case law), or conventions, treaties or other international legal instruments to which your country is party.

For non-government stakeholders, please answer with regard to any "legal provisions" – any domestic laws or regulations, including court decisions (case law), or conventions, treaties or other international legal instruments of which you are aware.

Questions

When answering the questions below, please:

- Focus on business-to-consumer (B2C) alternative dispute resolution (ADR). However, where informative for the B2C environment, answers may discuss other forms of ADR, such as business-to-business, consumer-to-consumer, business-to-government or consumer-to-government ADR.

- Focus on any legal provisions, but as they particularly apply to privacy and consumer protection.

- Focus on informal B2C ADR mechanisms (such as assisted negotiation and mediation). However, where appropriate, answers may discuss B2C arbitration.

- Distinguish, where appropriate, among: legal provisions addressing B2C ADR generally; legal provisions addressing B2C ADR on a sectoral basis; and legal provisions that may not mention ADR, but that could nonetheless impact ADR (for privacy and consumer protection disputes, in particular).

- Indicate any differences between use of B2C ADR for disputes arising in a domestic context as opposed to those with a cross-border element.

In addition, please recall that we use the term "legal provisions" in a generic, general and inclusive sense.

A. Specific ADR provisions

1. Are there legal provisions that specifically address B2C ADR (either addressing B2C ADR generally or addressing B2C ADR on a sectoral basis)? If yes, please describe the provisions.

2. Are there legal provisions that specifically address other forms of ADR (either generally or on a sectoral basis), such as business-to-business, consumer-to-consumer, business-to-government or consumer-to-government ADR? If yes, please describe the provisions.

B. Recourse to ADR

3. Are there legal provisions that would prevent or inhibit recourse to ADR for certain types or categories of disputes?[1] If so, please explain the provisions and their application.

4. Are there provisions that would require or encourage recourse to ADR for certain types or categories of disputes? If so, please explain the provisions and their application.

C. Exhaustion of remedies through ADR

5. Would a contractual agreement by the parties (such as a business and a consumer) to exhaust recourse through ADR before they can seek redress through courts be against any legal provisions? If so, please reference the provisions.

6. Are there legal provisions that would require or encourage parties to exhaust recourse to ADR before seeking redress in courts? If so, please reference the provisions.

D. Contractually binding ADR

7. Are there legal provisions that would prevent or inhibit a contractual agreement by parties (such as by a business and a consumer) to be bound by the outcome of ADR, if agreement to the contract came:

a. Prior to a dispute arising?
b. After a dispute arose, but before an ADR process had begun?
c. At the end of the ADR process (transaction)?

8. Are there legal provisions that would encourage or explicitly permit a contractual agreement by parties (such as by a business and a consumer) to be bound by the outcome of ADR, if agreement to the contract came:

a. Prior to a dispute arising?
b. After a dispute arose, but before an ADR process had begun?
c. At the end of the ADR process (transaction)?

9. If the parties can agree to be bound, are there legal provisions that could prevent or inhibit, totally or partially, implementation of the ADR outcome?[2] Please state under which circumstances this could be so.

E. Judicial enforcement

10. Can an ADR outcome be judicially enforced? Under which circumstances?

---

1. For instance, one area to possibly consider are disputes where there has been a high level of harm to a user or consumer, such as a severe privacy infringement, bodily harm to a consumer or user, or the loss of a large amount of money by a consumer or user.

2. For instance: could the terms of Article 5 of the Rome Convention affect a consumer's obligation to implement an outcome?

F. Procedure

11. Are there legal provisions that would require certain procedural safeguards[3] to be in place during an ADR process?

a. In general?
b. Any special, or particular, rights for consumers or users?
c. Any special, or particular, rights for businesses?

G. Confidentiality

12. If the parties and ADR provider agree to keep information on an ADR proceeding and/or outcome confidential, are there legal provisions that would require disclosure under any circumstances? If so, which circumstances?

H. ADR services

13. Are there any legal provisions that address who can offer B2C ADR services?

14. Are there any legal provisions that address who can serve as a neutral in an ADR proceeding?

15. Are there any other legal provisions relating to the activity of ADR providers, including the cost of ADR for either users and consumers or businesses?

I. Other

16. Are there any other legal requirements or restrictions applicable to ADR that have not been addressed above?[4]

---

3. These procedural safeguards might include, for example, transparency, timeliness, accessibility and affordability, the ability to be represented by a lawyer, the guarantee of an adversarial process, and the independence and/or impartiality of the ADR provider.

4. For example, please discuss any government commitments and accords, including administrative recommendations, or other items that could significantly affect an understanding of whether and how existing legal provisions impact recourse to ADR.

Chapter 10

RESOLVING E-COMMERCE DISPUTES ONLINE: ASKING THE RIGHT QUESTIONS ABOUT ALTERNATIVE DISPUTE RESOLUTION

This chapter was originally produced as an educational piece to help individual users determine whether online ADR can help them resolve a dispute, such as what to think about before considering ADR, how to choose a particular form of ADR, where to locate ADR providers, and what to do if ADR cannot help.

Chapter 10

RESOLVING E-COMMERCE DISPUTES ONLINE: ASKING THE RIGHT QUESTIONS ABOUT ALTERNATIVE DISPUTE RESOLUTION

Shopping online opens up a world of opportunity, convenience, choice, competitive prices and information. It may also raise some practical questions and concerns. What will happen if something goes wrong with your purchase? What if you don't get the products you ordered? What if they arrive damaged? What can you do?

Often, when you are browsing online, you can learn how a business will help resolve problems, simply by looking at its Web site. Some businesses provide information about their policies on dispute settlement. Enquire about the company's in-house customer complaint services or money-back guarantees. At the very least, you should make sure the site has a phone number or e-mail address so you can contact the company if something goes wrong. In addition, some online businesses are part of "seal" or "trustmark" programmes that certify that a business meets certain minimum standards. Click on the seal or trustmark for more information. Some companies offer escrow services, through which a third party can hold your money until you get the goods or services you ordered. Other companies offer insurance programmes through which you can get your money back if you don't get the products or services you ordered.

When you have a problem with a purchase you have made online, try to resolve the problem with the company directly, as a first step. If your attempts to fix a problem directly with the business are not successful, you may think that legal action is your only option. Often, however, there is a quicker and cheaper option through which you can try to resolve your dispute: using a neutral third party. This process is called alternative dispute resolution (ADR), and, increasingly, consumers and merchants are using it. Online ADR involves a process through which you can contact an ADR provider, file your complaint online, have the other party respond online, and resolve the entire dispute from the comfort of your own home with no need to travel and at minimal cost. If you have a dispute, be aware that some sites may require you to go through ADR before going to court; others may require you to waive your right to go to court. Check the terms and conditions of the sale first. Then, check with your local consumer protection agency to see if "mandatory" or "binding" ADR clauses are legal in your country. If you do not want to give up your immediate right to go to court, consider whether you want to enter into a transaction on the site. To determine whether online ADR can help you resolve your dispute, consider the following questions:

Key questions
1) What should I think about before considering ADR?
2) What kinds of online ADR are available?
3) How do I choose a particular form of ADR?
4) How do I choose a particular ADR provider?
5) Where can I locate ADR providers that could meet my needs?
6) What if ADR can't help?

1) What should I think about before considering ADR?

TIP 1

Before trying ADR, ask yourself the following questions:

What remedy would satisfy me?

Clearly identify what solution would be acceptable to you. For example: Do you want your money back? Do you want the product to be replaced? Do you want the business to take other action?

Have I tried to resolve the problem directly with the business myself?

Usually, the best first step is to contact the business directly. Businesses often have excellent internal complaint handling systems that will help solve your problem quickly and efficiently.

Can my payment card issuer provide assistance? TIP 2

If you paid for goods or services using a credit or debit card, you may benefit from special protections. Carefully read your payment card statements for information on contesting charges, and check with your local consumer protection agency to see whether any special protections apply in your country.

Do I suspect fraud or some other unlawful conduct? TIP 3

If so, contact your national or local consumer protection or data protection authorities.

2) What kinds of online ADR are available?

TIP 4

Mediation and arbitration are already well known and used in the offline world, and are increasingly available online. Automated negotiation is a new form of ADR that takes special advantage of the online environment.

What is mediation?

In mediation, a neutral third party – a mediator – helps you and the other party try to resolve the problem through facilitated dialogue. However, it's up to you and the other party to reach an agreement. Other names for similar approaches to ADR include "assisted negotiation", "facilitation", and "conciliation".

What is arbitration?

Arbitration involves a neutral third party – an arbitrator – who gathers information from you and the other party and makes a decision. Frequently, the arbitrator's decision is intended to be binding.

What is automated negotiation?

Automated negotiation is a computerised process, mostly designed to settle disputes over monetary amounts. It is often based on a system of blind bidding, through which the parties enter successive bids in an attempt to reach agreement, but without knowing what the other party has offered. The process concludes when the bids become sufficiently close to one another and the computer programme can propose a solution. Read the terms and conditions of an automated negotiation carefully, as the outcome generated by the computer can be a legally binding contract.

3) How do I choose a particular form of ADR?

Some online merchants specify in their terms and conditions that a particular form of ADR will be used if there is a dispute about the transaction. Read those terms and conditions carefully, and ensure that you are comfortable with them before making your purchase. With other merchants, you may be able to initiate the ADR proceeding yourself. In thinking about which form of ADR would be best for your dispute, ask yourself the following questions to help you determine which ADR programme to use.

What role do I want the third party to play?

In arbitration, the third party makes the decision. In mediation the role of the third party may vary, but your own active involvement in proposing compromises and finding solutions is essential. In automated negotiation, a solution is generated by a computer programme.

Should the third party have special qualifications/expertise?

Arbitrators and mediators may have formal qualifications. If your dispute is highly technical, or requires a particular area of expertise, make sure the third party has sufficient and appropriate expertise. If it is a simple dispute where, for example, you and the business disagree on the facts, formal qualifications may be less necessary. In either case, having a third party with experience in the subject matter of your dispute will be helpful.

Do I want to agree to be bound by the outcome? TIP 5

You may be bound to obey the outcome of an arbitration. In other words, you may have exhausted your options – and may not be able to sue the company in court. However, in some countries, consumers are not allowed to give up their right to go to court. Check with your local consumer protection or data protection agency.

4) How do I choose a particular ADR provider?

Consider the following:

Does the provider adhere to a code of conduct or guidelines?

An ADR provider may refer to a set of guidelines or a code of conduct. Usually, this means that the ADR provider has voluntarily agreed to respect certain rules. Check the Web site of the ADR provider for details about these types of measures.

What will it cost to use this ADR programme?

Some programmes are free. Others charge a flat rate or a rate based on your ability to pay. Check the merchant's site and the ADR provider's site to see who will pay the ADR costs.

How long will the process take? TIP 6

It varies. Often, ADR can be much speedier than going to court.

Can I go through the process in my own language?

Inquire whether you can use your own language during the process. Sometimes translation may be available but inquire about the cost and availability of a translator.

How will I present my case? TIP 7

The actual process of communicating may take many different forms, ranging from a simple exchange of e-mails to all parties being "present" via Web cams. Consider:

Timing: If the problem is complex, you may want time to think, before having to respond.

Technology: You can send an e-mail any time from home, but can you videoconference?

Security: Messages sent by ordinary e-mail generally have no special security protections. The level of security needed will depend on the sensitivity of the information sent. Although many small-value disputes will not require confidentiality, you should avoid sending highly sensitive personal information in an e-mail. If the dispute itself involves highly sensitive personal information, consider using ADR programmes that have secure Web pages to transmit information.

Does the provider have a privacy statement?

Consider whether the provider has a privacy statement, or otherwise indicates how your personal information will be used. Some ADR providers may ask your consent to make an anonymised version of the outcome of your dispute public. This information can be useful to other consumers evaluating whether to use a particular ADR provider and inform consumers with similar disputes about possible solutions.

5) Where can I locate ADR providers that could meet my needs? TIP 8

There are a number of ADR inventories you can consult.

6) What if ADR can't help?

If you have tried ADR unsuccessfully, or decided not to try ADR, your last resort may be legal action.

TIPS

1. These questions address the issue of dispute resolution. However, before deciding to interact or do business with a Web site there are many other important factors to consider. Some considerations relate to privacy. For links to online information sources regarding privacy protections, visit the OECD's privacy resource page: http://cs3-hq.oecd.org/scripts/pwv3/privcontacts.htm. Other considerations relate to consumer protection. You can find information about the protections you should expect while shopping online at: www.oecd.org/document/51/0,2340,en_2649_34267_1824435_1_1_1_1,00.html. For additional information about safe shopping online, visit: www.econsumer.gov/english/contentfiles/shoptips_1.html.

2. The OECD has prepared a set of *Frequently Asked Questions* that discuss the safe use of payment cards online and the protections available in case something goes wrong: www.oecd.org/sti/consumer-policy. For links to consumer protection agencies, visit: www.oecd.org/countrylist/0,2578,en_2649_34267_1783507_1_1_1_1,00.html.

3. To file a cross-border e-commerce complaint about consumer protection or privacy issues, visit www.econsumer.gov. For links to online information sources regarding privacy protections, visit the OECD's privacy resource page: http://cs3-hq.oecd.org/scripts/pwv3/ privcontacts.htm.

4. OECD countries differ in the way that they classify and define these ADR forms. In your country, special forms of ADR may be available for you to use.

5. Links to consumer protection authorities can be found at: www.oecd.org/countrylist/0,2578,en_2649_34267_1783507_1_1_1_1,00.html. Links to data protection authorities can be found at: http://cs3-hq.oecd.org/scripts/pwv3/ privcontacts.htm.

6. When you consider timing issues, keep in mind that most OECD countries have laws that limit the amount time that you have to bring a claim to court. Ensure that the ADR proceeding will be concluded within sufficient time for you to go to court, if that should become necessary.

7. To verify that your information is secure, make sure the Web address (URL) for the ADR form begins with "https:" instead of "http:" and look for an icon (for example, a closed padlock or a key) at the bottom of your computer screen to signal that your transmission will be secure.

8. The European Commission provides ADR provider information through its EEJ-Net project, available at: http://europa.eu.int/comm/consumers/redress/out_of_court/eej_net/index_en.htm. Consumers International has assessed of a number of ADR providers. Results are available at: www.consumersinternational.org/document_store/Doc35.pdf.

Chapter 11

COMPLIANCE WITH, AND ENFORCEMENT OF, PRIVACY PROTECTION ONLINE

This chapter presents and analyses enforcement mechanisms that are available in OECD member countries both to address non-compliance with privacy principles and policies and to ensure access to redress. It is intended to form the basis for assessing the practical application of available compliance and enforcement instruments in a networked environment and their ability to meet the objectives of the OECD Privacy Guidelines, including effectiveness and coverage across jurisdictions.

Chapter 11

COMPLIANCE WITH, AND ENFORCEMENT OF, PRIVACY PROTECTION ONLINE

Introduction

Privacy compliance and enforcement are different topics, but are interrelated. They are different, since compliance refers to the level of adherence to legal requirements, while enforcement refers to the mechanisms which can be used to compel such adherence and to protect the rights of data subjects when violations occur. At the same time, the two are closely interrelated, since the higher the level of compliance, the less need there is for enforcement, and a strong level of enforcement may motivate actors to adopt a higher level of compliance. This report recognises the close interrelationship between these two topics, and thus deals with compliance and enforcement together, while still recognising the potential distinctions between them.

Background

On 12 March 2002, a Questionnaire on Compliance with and Enforcement of Privacy Protection in the Context of Business-to-consumer Electronic Commerce was sent to OECD governments and private sector participants (see Appendix). It was developed as part of the work programme of the ICCP Working Party on Information Security and Privacy (WPISP) to fulfil the objectives of the OECD Ministerial Declaration on the Protection of Privacy on Global Networks issued at the OECD Ministerial Conference in Ottawa, Canada, in October 1998. Responses were received from 19 member countries and three private organisations.

In the declaration, Ministers stated that they would take steps to ensure that effective enforcement mechanisms are available both to address non-compliance with privacy principles and policies and to ensure access to redress. Moreover, the declaration called on the OECD "to promote user education and awareness about online privacy issues and the means at their disposal for protecting privacy on global networks".

Since the OECD Ministerial Conference, compliance and enforcement have become central issues in privacy protection. Considering the limitations of purely legal and regulatory approaches, both governments and the private sector have been developing alternative methods of compliance and enforcement which make use of self-regulation, market incentives, technological means and other mechanisms which go beyond traditional regulatory approaches and which can better cope with the borderless and fast-moving nature of electronic commerce. It was thus the appropriate time to take stock of compliance and enforcement mechanisms used in the OECD member countries and analyse whether they cope adequately with the requirements of electronic commerce.

Respondents were requested to provide basic information rather than detailed analysis. Governments were requested to answer the questions with regard to any "legal provisions", meaning any domestic laws or regulations, including court decisions (case law), or conventions, treaties or other international legal instruments. Information was solicited both about governmental agencies (such as a government ministry) and independent privacy regulators (such as a data protection authority); in this report, the term "government agency" refers to both types of entities.

Input was also solicited from the private sector, since the private sector can provide practical experience, highlighting the process it undertakes when implementing privacy safeguards. Thus, private sector participants were requested, in addition to providing information on legal provisions they are familiar with as described above, also to provide information on any self-regulatory solutions which they are aware of, such as trustmarks, seal programmes, the use of corporate privacy officers, private-sector enforcement programmes, and the like, as described further in the questionnaire. This report gives an overview of the subject. It is based on the responses received and is non-judgemental.

I. Summary of responses

Responses were received from the following OECD member countries and private sector entities: Australia, Austria, Belgium, Czech Republic, Finland, France, Germany, Italy, Japan, Korea, Mexico, the Netherlands, Norway, Slovak Republic, Sweden, Switzerland, Turkey, United Kingdom, United States, Internet service providers (ISPs) from the Slovak Republic, the US Council for International Business (USCIB) and the US Direct Marketing Association (DMA).

Norms and instruments

Privacy framework

Among the countries with omnibus privacy legislation are Australia, Austria, Belgium, the Czech Republic, Finland, France, Germany, Italy, Korea, Norway, the Slovak Republic, Sweden, Switzerland and the United Kingdom. Countries without a single omnibus law include Japan, Mexico, Turkey and the United States. Legislation is currently being considered in Japan and Turkey. Some countries have sector-specific laws as well. For instance, many European Union (EU) member states have sectoral legislation regarding telecommunications privacy, and Finland has laws on telecommunications, openness in government activities, privacy protection in relation to employment, police data files and criminal records. The United States has laws that address privacy protection concerning various sectors, such as the privacy of children's information, and financial and medical information. Germany has specific acts relating to online services. Most respondents also have additional forms of legal regulation, such as decrees, ordinances, administrative rules, and case law (for instance, France, Germany, Italy, Sweden, and Switzerland have ordinances or decrees). The role of case law differs: for example, in the United States it is a major source of law, while in France it is not regarded as an independent source of law. In Japan there are various self-regulatory guidelines in place, while in the United Kingdom human rights legislation is of particular relevance. Administrative rules and regulations play an important role in the United States.

International and regional instruments

The member countries of the EU are all bound by the Data Protection Directive,[1] and the various public law agreements and instruments which the European Commission has entered into (such as the Safe Harbour arrangement,[2] and the model contracts for data transfer[3]). Some European countries are also parties to other EU agreements that include data protection provisions, notably in the area of police co-operation.[4] The same countries and others are also members of the Council of Europe (COE) and are bound by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[5] Mexico has signed an Economic Partnership, Political Consensus and Co-operation Agreement with the European Union and its member states which establishes commitments to promote the protection of personal data, among other aspects. The respondents also share a commitment to implement various other international instruments, such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (the OECD Privacy Guidelines), the United Nations Guidelines on Computerised Personal Data Files, and others.

With regard specifically to model contracts for data transfer, the decisions of the European Commission on model contracts are applicable in the EU member states and have been implemented by them. The Czech Republic recommends the use of model contracts. The USCIB has participated in the drafting of the alternative model contracts that the International Chamber of Commerce (ICC) and other business organisations have recently presented to the European Commission for approval.[6] A set of model clauses has also been jointly published by the ICC, the European Commission and the COE.[7]

Codes of conduct, trustmarks, etc.

Most countries do not have government-endorsed codes of conduct. In Australia, some industry codes of practice have been lodged with the Privacy Commissioner for approval. In the Slovak Republic, all technological norms are endorsed by a governmental entity, and in Sweden industry organisations may submit codes of conduct to the Data Inspection Board for an opinion and the Board has, so far, issued opinions on two such codes. Japan has created a model for guidelines to be set up by business organisations, and a number of companies have set up guidelines in conformance with the model. In many countries (such as Austria, France, Mexico and the United States) the use of codes of conduct for privacy protection is encouraged.

The majority of respondents mentioned that they have private sector codes of conduct, best practices or seal or trustmark programmes that are either endorsed by a business federation or widely used by the private sector either generally or in a specific sector. Most of the responses concerned codes of conduct, but some (Germany, Japan and the Unites States, for example) also mentioned that they had seal or trustmark programmes. The Korean Association of Information and Telecommunications mentioned that they award an "ePrivacy Mark" to qualified Internet sites that satisfy stringent data protection criteria.

Security

Nearly every respondent mentioned some form of government regulation applicable to the security of Web sites, although in many countries (*e.g.* Austria, Finland, France, Norway, and Sweden) there is general data protection or security legislation rather than special legislation dealing solely with Web sites. In Japan private-sector guidelines set forth security parameters for business, and guidelines have also been promulgated by governmental entities. In Mexico there are self-regulating measures in the financial sector that guarantee the security of online services. In the United States, a site's misrepresentation to consumers about its privacy and security practices could be a violation of federal consumer protection law. Additionally, there are statutory provisions and administrative rules on security safeguards applicable to the financial sector.

Compliance

Variety of systems

Respondents indicated that a wide variety of entities are consulted in their countries for information and advice on compliance with the norms identified above. Those with a public independent privacy authority (for instance, Australia, Austria, the Czech Republic and Belgium) indicated that this authority could be consulted. A number of respondents also mentioned private-sector lawyers and law firms (*e.g.* Finland). Some mentioned governmental bodies other than privacy commissioners: for instance, in Japan there are "information security advisers" at each Prefectural Police Headquarters (local police department) who give information and advice about "unauthorised computer access law" and computer crime.

Best practices, software tools, etc.

Respondents indicated that governmental authorities responsible for privacy protection can review privacy practices of businesses. This can be based on administrative procedures, reviews based on best practices, software tools or other means of reviewing the privacy practices followed by businesses engaged in online activities, Japan indicated that there are standard practices in place (such as "JIS Q 15001") which provide for regular business audits, as well as a "Privacy Mark System". Switzerland mentioned that there is a private-sector initiative for a labelling and auditing project for e-commerce. In the United Kingdom, the British Standards Institute has published an audit manual for self-audit and has included data protection in its suite of software legal compliance tools. Similar initiatives have been promulgated by industry groups such as the World Wide Web Consortium (W3C); this was mentioned by the United States, which indicated that software tools can help companies translate their privacy policies into a Platform for Privacy Preferences (P3P) machine-readable format and allows a company to inventory all features on its Web site so it can track and control its privacy risks. In the German Omnibus Privacy Act, there is a provision on privacy auditing which is to be implemented by more specific legislation.

Australia and the United States indicated that they encourage companies to voluntarily engage in self-assessment of their privacy practices. It was noted that, in the particular case of the "Safe Harbor" frameworks in the United States, participants must assess their practices, either by a third party or by self-assessment. In the Netherlands, the data protection authority has developed auditing tools in co-operation with private organisations (*e.g.* a self-evaluation method and a framework for privacy audits). Mexico and Sweden, companies voluntarily engage in such self-assessment. Most countries indicated that self-assessments are not usually made publicly available. In the United States, however, some (but not all) companies make them public. Only the Slovak Republic has a legal requirement for self-assessment.

Governmental agencies and private-sector oversight entities

In countries with governmental data protection agencies, such authorities are competent to oversee compliance with norms. Other governmental agencies may also monitor compliance with norms in specific sectors (for instance, the Finnish Communications Regulatory Authority, together with telecommunications operators, the telecommunications equipment industry and user associations, promotes privacy protection and information security in telecommunications). In those countries where private-sector compliance systems are active (such as Japan and the United States), the entities that run such systems also monitor compliance, together with competent governmental agencies.

The organisation and powers of governmental regulatory bodies are determined by appropriate legislation. Private sector oversight entities are usually set up on the basis of agreements entered into by the participants in the system. Governmental bodies have oversight powers as granted to them by law, which typically include carrying out audits, issuing warnings and reporting breaches to the appropriate authorities (as in France). Private sector entities tend to have similar powers, which can include responding to complaints and enquiries and expelling offending organisations from the scheme, without, of course, the full panoply of powers available to governmental entities.

Company privacy officers

Responses indicated that there is an increasing trend on the part of companies to appoint internal data protection officers; in a few countries, there is a legal obligation to do so. The USCIB and US government noted that self-regulatory bodies can offer advice on policy and practices, that over 500 companies now have chief privacy officers who are responsible for ensuring that their companies adhere to existing laws and follow sound privacy practices, and that there now exist umbrella organisations in the private sector to assist companies in developing practices and procedures. The United States also mentioned that entities

covered under the Health Insurance Portability and Accountability Act (health plans, health-care providers, and health-care clearinghouses) will be required by law to appoint a privacy officer when the Act takes effect in April 2003. Also, in Korea, companies must appoint a company privacy officer who will safeguard information and deal with complaints from data subjects. In the Slovak Republic, if a controller of information systems employs more than five persons, he has to appoint a responsible person or several such persons to carry out the supervision of compliance with statutory provisions in personal data processing. Finally, in Germany, public and private entities with more than four employees have to appoint a data protection officer. Almost none of the other respondents indicated the presence of a legal requirement for companies to appoint a privacy officer in charge of compliance. However, in Finland, the Data Protection Ombudsman has recommended that companies appoint a privacy officer, as do various self-regulatory programmes in Japan and the data protection authorities in Norway, Switzerland and the United Kingdom. The law of some member countries (*e.g.* Germany, the Netherlands and Sweden) exempt companies that appoint a company privacy officer from certain legal obligations (such as notification of data processing to the data protection authority).

Notification

Notification of data processing to an oversight entity is mandatory in Austria, Belgium, the Czech Republic, Finland, France, Italy, Norway, the Slovak Republic, Sweden, Switzerland and the United Kingdom. However, even in such countries, certain exceptions apply, or notification may apply only to certain situations. For instance, in Sweden notification is not required if a personal data representative has been appointed or if the processing takes place with the individual's consent. Also, in Japan the TRUSTe Japan seal programme requires the notification of processing to an oversight department. Notification of data processing by banks may be required in Mexico under certain circumstances.

Technological solutions

Most respondents stated that technological solutions to protect privacy are implemented only to a limited extent, although some member countries (such as Japan, the United Kingdom and the United States) indicated that the use of technical standards (such as P3P) to ensure compliance is expanding. The UK Information Commissioner promotes the use of privacy enhancing technologies, while in the United States many such tools are widely available on the Internet (including P3P) but it is unclear how many businesses or consumers take advantage of them. The German Ministry of Economy and Technology has a programme to encourage the anonymous use of online technology. The Netherlands indicated that the Dutch government has committed itself to the use of privacy-enhancing technologies in new public data processing systems. However, these initiatives remain the exception. Otherwise, the use of technology to protect privacy was mentioned in the context of security. In Austria, as in other countries, the use of firewalls, anti-virus software and other safety precautions is standard, and the law requires certain data security measures but does not specify the exact techniques to be used. Finland indicated that the situation in companies varies to a great extent depending mainly on the size and partly on the field of the company. Japan stated that secure socket layer (SSL) and other encryption technologies are used to protect sensitive information such as credit card numbers, as is the case in Turkey.

Enforcement

Governmental authorities

Every member country has at least one governmental authority which can enforce privacy norms (including the courts, the police, consumer protection agencies, data protection authorities, telecommunications regulatory authorities, unfair competition authorities). Italy mentioned that under the law, data subjects can always turn to data controllers to exercise their rights in the event of a dispute. Japan, the United Kingdom and the United States noted that data subjects may also be able to turn to a self-regulatory scheme, in cases where one is applicable.

Most respondents indicated the possibility of obtaining judicial or administrative relief based on a case brought to court or to governmental authorities, such as monetary compensation for damages, injunctive relief, erasure of data or blocking of processing. Austria noted that most privacy claims against private entities must be brought before the courts, but that many claims regarding privacy issues are resolved through other legal instruments (such as media law, unfair competition law, telecom law and laws against libel and slander). The United States noted that the Federal Trade Commission (FTC) can sue companies who misrepresent their privacy policies, through administrative procedures or through the courts, and can obtain injunctions and monetary redress for consumers who are harmed. Most respondents indicated that administrative or penal fines are possible. Among those who may impose such fines are criminal authorities, data protection authorities and consumer protection authorities. Most respondents stated that criminal penalties, including imprisonment and fines, are possible; however, Australia and Belgium stated that this is not the case, and the United States noted that such authority is narrowly prescribed. Most respondents indicated that monetary compensation for damages is possible. Most respondents stated also that either courts or data protection authorities, or both, may impose injunctive relief. In Belgium and France the data protection authorities may themselves not impose injunctive relief, but may apply to a court to do so.

Private-sector entities

With regard to remedies that private-sector entities can use for violations, respondents mentioned withdrawal of seals and trustmarks, expulsion from self-regulatory schemes and blacklists. Several also noted that in their countries (*e.g.* Finland, Norway and the Slovak Republic) a private-sector entity cannot itself impose a fine or take similar punitive action, but can bring a case against the offender to court or before a data protection authority. The USCIB said that loss of goodwill and reputation in the marketplace is important, and that in the United States, many alleged privacy incidents have been handled expeditiously by organisations so as to preserve their reputation. Japan indicated that a self-regulatory entity can direct participating companies to take certain measures, and punishment such as expelling the company from the scheme can be used to compel compliance.

Handling of complaints

There are a wide variety of procedures used for handling privacy complaints. In most member countries, complaints are brought before data protection or consumer protection authorities. These may then investigate the complaint and take appropriate action, which may include imposing penalties or referring the case to the courts or criminal authorities. In some countries (such as Italy) the data subject should first make application to the data controller before applying for relief to the data protection authorities, whereas in others (Sweden, for example) the data subject may turn directly to the authorities or go first to the data controller. As Japan pointed out, self-regulatory bodies have their own procedures for handling complaints.

Online filing and ADR systems

Online filing of complaints is possible in a number of member countries (for example, Australia, Austria, France, Germany, Japan, Sweden, and the United States). Norway indicated that, while online filing was not formally provided for, it was used in practice (*i.e.* data subjects often send complaints or inquiries to data protection authorities by e-mail). The United Kingdom is working on an online filing system. Mexico specifically noted that the Federal Consumer Protection Agency (Profeco) takes part in an international project conducted within the framework of the International Marketing Supervision Network (IMSN) which has resulted in the establishment of a Web site to gather and share complaints about cross-border electronic commerce.[8] In the United States, the FTC administers the IMSN Web site project and also maintains its own agency Web site[9] to allow consumers to report on privacy complaints, including those relating to Internet representations and e-commerce transactions.

Alternative dispute resolution (ADR) mechanisms for privacy-related disputes, such as arbitration and mediation, are in use in only a few countries, such as Austria, Korea and the United States. France indicated that a number of such schemes are now being developed by the European Commission. Italy indicated that ADR schemes are used, but that there are not specifically focused on privacy disputes. Such mechanisms are now being developed in Japan. In Germany some trustmark providers may offer such schemes.

Auditing

Only a few countries indicated that auditing of privacy practices is used as a method of enforcement. In Finland the Data Protection Ombudsman has the right to audit personal data registers and the Finnish Communications Regulatory Authority has the right to audit telecom operators' activities. The French Data Protection Authority (CNIL) has also used online surveys to inventory the practices of Web sites. Auditing by self-regulatory bodies is used in Japan and the United States, and voluntary audits are used in Mexico. Auditing may also be a kind of mandatory enforcement mechanism used by governmental agencies, for example in Sweden and the United States. Some of the local data protection authorities in Germany are presently using software tools to conduct audits of Web sites. Many respondents mentioned that security audits are often used to review the security of information systems and computer networks.

Public awareness

Methods

Most countries stated that the public or private sectors had undertaken campaigns to educate the public as to their privacy rights. Among the methods used are speeches and meetings; media interviews; disseminating copies of publications; information on the Web sites of privacy authorities,[10] the publication of annual reports by privacy authorities; the creation of online "privacy toolboxes" by companies; and self-regulatory schemes which tell users how they can limit disclosure of their personal information, what choices they have about how such information is used and shared, and under what circumstances they can access it.

Privacy policies

No respondents have specific legal requirements to post online privacy policies. However, in many member countries data controllers (including operators of Web sites) have legal obligations to inform the data subject of the processing of his data (including such matters as access rights, etc.), and this obligation can be satisfied through an online privacy policy. Many government and private-sector schemes also encourage companies to post online privacy policies. When a privacy policy is posted, it may need to include certain mandatory information, such as the identity of the data controller and the purpose of the

processing. There is evidence from several respondents that the number of Web sites posting privacy policies is growing rapidly.

Contact persons

Only a couple of countries (*e.g.* Belgium and the Slovak Republic) legally require the appointment of a contact person who can provide information on privacy practices or to whom persons can turn with complaints or questions. However, most countries indicated that they provide incentives for the appointment of such a person. For instance, in France the law encourages companies to appoint a contact person for the purpose of access and rectification rights, since notifications to the CNIL must give the name of the department to which requests for access to and correction of personal data should be addressed.

Publication of violations

Respondents provided a wide variety of answers to the question of whether privacy violations are published, and if so how. Some respondents (*e.g.* Mexico and Turkey) stated unequivocally that violations are not published, while others (*e.g.* Italy) do publish them. Most member countries indicated some possibility for publication, restricted in some way, however. For instance, in Austria decisions are published online, but in anonymous form; in Belgium only decisions with particularly serious implications for the public are published by means of press releases; in the Czech Republic the data protection authorities publish only general reports on cases in its annual reports but not the text of individual decisions; and in the Slovak Republic only serious violations are published. In the United States, FTC investigations of alleged privacy violations are not made public, but administrative or court actions are made public on the FTC's Web site. The US Direct Marketing Association also mentioned that their "Safe Harbor Enforcement Program Contract" contains language empowering the DMA to issue public press releases about an enforcement decision. Several respondents indicated that publication of violations, whether by the government or in the scope of self-regulatory compliance schemes, could be a very effective means of privacy enforcement; indeed, France stated that courts may use publication as an additional punitive measure. However, France also indicated that the publication of privacy violations could have legal implications for libel and other types of civil liability, and so had to be carefully considered in each individual case. The UK Information Commissioner has recently conducted a study of web-site compliance, which is published on the Commissioner's Office Web site.[11]

II. Analysis

The OECD Privacy Guidelines

The 1980 OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data contain two types of provisions relevant to compliance and enforcement: *i)* provisions setting forth general principles of data processing (such as collection limitation, data quality, use limitation, etc., and *ii)* provisions dealing with the interests of individuals concerning their personal information (such as individual participation, accountability, and national implementation). The first set of provisions, although formulated in the nature of conditions for the processing of personal data, are relevant to compliance and enforcement, since they set forth the practices which entities processing personal data should observe. The second set of provisions deals more directly with the recommendations for rights which individuals should have with regard to their personal data (Part 2. Basic Principles for National Application, paragraph 13), and the recommendations to member countries to provide mechanisms for accountability (Part 2. Basic Principles for National Application, paragraph 14) and to implement such principles by endeavouring to adopt appropriate domestic legislation, encouraging and supporting self-regulation, in the form of codes of conduct or otherwise, provide for reasonable means for individuals to exercise their rights, provide

adequate sanctions and remedies in the case of failures to comply with measures that implement the principles, and ensure that there is no unfair discrimination against data subject. (Part 4. National Implementation, paragraph 19).

The 1980 Guidelines thus provide that individuals should be given certain rights in regard to personal data relating to them; that the data controller should be accountable for complying with measures which give effect to such rights; and that member countries should implement certain legal, administrative or other procedures to protect privacy and individual liberties in respect of personal data. At the same time, the Guidelines do not set forth in detail the mechanisms by which such protections are to be effected, and only provide certain suggestions for member countries to implement the OECD principles relating to privacy compliance and enforcement (see Paragraph 19 mentioned above). The Guidelines contemplate a flexible mixture between government regulation and private-sector self-regulation as the best way to ensure effect compliance and enforcement.

Shift in national frameworks for privacy protection

The legal frameworks for privacy compliance and enforcement which were initially created in most member countries concentrated on ensuring a good level of compliance and the rights of data subjects by creating a basic legal framework within which data subjects could exercise their rights, and focused on "traditional" enforcement mechanisms such as making complaints to data protection authorities and other governmental bodies, bringing suits in court, and ensuring that adequate penalties existed for punishing infractions of the law.

However, several significant developments since the passage of initial privacy legislation and regulation have complicated compliance with and enforcement of privacy rules:

- The world's economy is now much more globalised than was the case 20 or 30 years ago, and it has become routine for data subjects in one country to enter into transactions via electronic communications networks with entities in other countries.
- The use of computer equipment to process personal data has increased exponentially in a way that would have been unimaginable just a few years ago.
- Online systems such as portals, marketplaces and communities have sprung up, which, while still subject to privacy law, function mainly according to self-imposed rules and terms and conditions agreed upon with users.
- The concept of privacy-enhancing technologies (PETs) has been developed, to provide for before-the-fact compliance with privacy laws.
- The number of cross-border jurisdictional disputes based on online interactions has been continually increasing.[12]

These trends have fundamentally changed the legal landscape for privacy compliance and enforcement as borne out by the results of the questionnaire. While the principle that the government must enforce violations of the law remains the foundation upon which individual user trust in the area of privacy is based, traditional compliance and enforcement mechanisms (such as fines, investigations by data protection authorities, and court actions) are increasingly supplemented by alternative and complementary means of ensuring compliance with and enforcement of privacy protection.

As the responses to the questionnaire demonstrate, OECD member countries and private-sector entities have developed and continue to develop alternative means to ensure compliance with and enforcement of privacy law which go beyond traditional governmental regulations and sanctions. Such alternative methods demonstrate a number of characteristics:

- They tend to make use of market-based incentives and punishments to ensure compliance with norms. For instance, many trustmark and privacy seal programmes have been developed which require participating Web sites to adhere to certain privacy practices. If they do not, then the seal or trustmark may be taken away from them, and the fact may be made public, thus exerting pressure on participants to comply with the scheme.
- They tend to use technical means as a way of ensuring compliance. Both member countries and private-sector entities have been encouraging the use of privacy-enhancing technologies, technical standards for privacy protection (such as P3P), audits and other compliance mechanisms to ensure that computer and online systems process personal data in compliance with applicable privacy principles. By encouraging compliance before the fact, the need for enforcement after the fact can be reduced.
- Businesses have come to see the commercial benefits which can accrue from offering privacy protection to customers, and have thus been offering many tools, mechanisms and systems for privacy protection. These self-regulatory systems include trustmark programmes, seals, PETs, company privacy officers, online privacy policies and others.
- There is considerable potential for taking existing mechanisms for privacy compliance and enforcement and adapting them to the online environment. For instance, some member countries and commercial entities have made it possible to file privacy-related complaints online, and there are also a number of ADR mechanisms for privacy disputes under development.
- Ensuring security is seen more and more as an essential element of privacy protection. It is therefore not surprising that both governments and private entities have been promoting technical standards, audits, security policies and other mechanisms for ensuring the security of data processing online.

These developments demonstrate the changing face of privacy compliance and enforcement. Whereas these topics previously had a legal or regulatory focus, attention has shifted to viewing them more holistically, so that government regulation is part of ensuring compliance and enforcement, but must be combined with technical, organisational and self-regulatory mechanisms in order to attain maximum effectiveness in a cross-border online environment. Moreover, it is critical to view privacy protection in a global perspective, rather than in a purely national one, in order to better facilitate redress for privacy violations that cross national borders. Ensuring compliance before the fact is less expensive and imposes less burden on data subjects than having to pursue enforcement actions in court or otherwise. Many such initiatives are now under way, and there is every sign that their use will grow rapidly in the coming years.

Further steps

At the same time, more needs to be done in member countries to encourage use of alternative mechanisms for privacy compliance and enforcement at the cross-border level. Progress needs to be made in particular in the following areas:

- The international and cross-border co-ordination of compliance and enforcement mechanisms is critical, both to protect the privacy of data subjects and to avoid putting data controllers in the position of being subject to varying requirements for the same conduct. Member countries should thus do everything possible to co-ordinate their compliance and enforcement activity to protect data subjects while minimising excessive burdens on data controllers, and providing for

sufficiently flexible solutions to ensure effective privacy protection and continued transborder data flows, as recommended in the OECD Guidelines (see, for example, paragraph 7 of the Explanatory Memorandum to the Guidelines). At present, too many mechanisms seem to operate on a national or regional, rather than at a global, level; member countries should work together to promote effective worldwide co-operation with regard to privacy compliance and enforcement. In particular, member countries could take steps such as further sharing resources for handling complaints, educating individual users and businesses about privacy regulations and best practices, and fostering the development and use of online ADR and PETs. As a further step, member countries could strengthen enforcement against companies misrepresenting compliance with privacy policies or promises, particularly when those misrepresentations have adverse consequences that could cause harm to consumers.

- It seems that not enough is being done to encourage the implementation of technical solutions for privacy compliance and enforcement (such as P3P), since only a few member countries mentioned this as an area with much activity. Member countries should educate and raise awareness about such technical solutions and encourage their development and use. In particular, the use of PETs should be encouraged in order to provide data subjects with increased privacy protection.
- At present use of some self-regulatory mechanisms which hold particular promise for the protection of privacy online seems somewhat haphazard and is concentrated in a few member countries. For instance, from responses it seems that, in some countries, mechanisms such as encouraging companies to engage in voluntary self-assessment of privacy practices are not used as often as they could be.
- More member countries should encourage the appointment of company privacy officers. For example, member countries could consider providing a legal basis for them and/or giving companies legal incentives for their use. At present, in some countries the appointment by companies of a privacy compliance officer to oversee data processing is foreseen in the law, while in others it is implemented by companies on a purely voluntary or self-regulatory basis.
- While much thought is currently being devoted to the development of online ADR mechanisms for privacy disputes, few member countries have such mechanisms actually in operation. The development of ADR systems could be crucial for improving the legal situation for data subjects regarding enforcement, and more needs to be done in this regard. It is particularly important that such systems be constructed to take into account the global nature of electronic commerce (*e.g.* they should function in multiple languages), and that they are able to cope with transborder disputes.
- Given the likely increase in privacy complaints and the limitations on government resources to address them, member countries should focus on areas where individual users suffer the most harm as a consequence of misuse of their personal data.

Member countries are currently making good progress toward providing an effective regime for privacy compliance and enforcement for the online environment, but continued work remains to be done. The key for the coming years will be to make traditional means of regulatory enforcement even more efficient, while at the same time encouraging the growth of self-regulatory mechanisms, since a mixture of these two systems is likely to best protect the interests of both data subjects and data controllers. Moreover, any mechanisms developed must be able to operate on a transborder basis.

NOTES

1. 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: (1995) OJ L281 31.

2. Safe harbor is a self-regulatory privacy protection system in the United States which was the subject of a positive adequacy decision by the European Commission on 26 July 2000 regarding data transfers from the European Union to the United States. Full documentation concerning safe harbor is available at www.export.gov/safeharbor/sh_overview.html.

3. The European Commission has approved model contracts for data transfer both for controller-to-controller transfers [Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, (2001) OJ L181/19] and for controller to processor transfers [Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC, (2002) OJ L6/52].

4. Such agreements include, *inter alia*, the Convention on the Establishment of a European Police Office (Europol Convention), the Convention on the Use of Information Technology for Customs Purposes and the Convention implementing the Schengen Agreement on the gradual abolition of checks at the common borders (Schengen Convention). Furthermore, the EEA agreement (European Economic Area) between the EU and three EFTA countries (European Free Trade Association) stipulates full implementation of the relevant EU data protection instruments in the EFTA countries that are party to the agreement. The EFTA countries are Iceland, Liechtenstein, Norway and Switzerland.

5. A full list of member states of the COE and the list of those member states who ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data is available at http://conventions.coe.int/Treaty/EN/cadreprincipal.htm. The Convention was opened to signature on 28 January 1981 and the full text is available at www.coe.int/T/E/Legal%5Faffairs/Legal%5Fco%2Doperation/Data%5Fprotection/.

6. The final version of the clauses was submitted to the European Commission on 9 August 2002 and is available at www.iccwbo.org/home/electronic_commerce/word_documents/Final%20version%20July%202002%20Model%20contract%20clauses.pdf.

7. Council of Europe/European Commission/ICC, Model Contract to Ensure Equivalent Data Protection in the Context of Transborder Data Flows of 2 November 1992, with Explanatory Memorandum.

8. Seventeen member countries take part in this project. See: www.econsumer.gov.

9. www.ftc.gov.

10. For the United Kingdom, see: www.dataprotection.gov.uk/dpr/dpdoc.nsf.

11. The report is available under Guidance and Other Publications: Codes of Practice our Responses and Other Papers: Related Papers: UMIST UK Web site Compliance Study at www.dataprotection.gov.uk/dpr/dpdoc.nsf.

12. This is indicated by government reporting on numbers of complaints received through the use of www.econsumer.gov.

APPENDIX

QUESTIONNAIRE ON COMPLIANCE WITH AND ENFORCEMENT OF PRIVACY PROTECTION IN THE CONTEXT OF BUSINESS-TO-CONSUMER ELECTRONIC COMMERCE

1. When answering the questions below, please:

- Focus on their application to online activities. You may give information that is not specifically targeted to online activities, but if so, please indicate how such information is applied to the online world.
- Focus on the business-to-consumer (B2C) realm. At the discretion of member countries, information related to the public sector may also be included.
- Provide broad coverage regarding the information requested. In particular, your responses should cover not only regulatory approaches, but also self-regulatory schemes such as corporate privacy officers, privacy seals, auditing procedures, industry bodies, technologies (such as privacy-enhancing technologies), and the like.
- Distinguish, where appropriate, among regulatory and non-regulatory approaches addressing privacy compliance and enforcement generally, and on a sectoral basis. You should also mention legal provisions and self-regulatory schemes that may not be specifically designed for privacy protection, but which could nonetheless impact it.
- Indicate any differences between mechanisms used in a domestic context, as opposed to those with a cross-border element. Provide information on domestic schemes, but focus on their application at the cross-border level.
- Indicate any co-operative mechanisms or efforts for ensuring compliance with and enforcement of privacy protection at the global level (whether bilateral or multilateral formal or informal cross-border co-operation).

In addition, please recall from the introduction section of this document that we use the terms "legal provisions", "non-regulatory", and "self-regulatory" in a generic, general and inclusive sense.

2. Norms and instruments

These questions are designed to determine the standards and reference points for online privacy compliance and enforcement at the domestic level. Please provide references of these norms and instruments, and also indicate which provisions are directed at cross-border and international issues.

Do you have any of the following that may be the basis for legal rights and obligations in the area of privacy:

2.1 Do you have a law or laws on the protection of privacy and personal data? If so, please indicate if it is a single omnibus law, or a collection of sectoral laws, or both.

2.2 Do you have other forms of relevant legal regulation (such as decrees, ordinances, administrative rules, case law (*jurisprudence*), or the like?

2.3 Is your country a party to public law agreements or instruments in the privacy sphere (for example, the Safe Harbour)?

2.4 Has your country implemented other private law agreements or instruments which may be the basis for data protection (*e.g.* model contracts for data transfer)?

2.5* Do you have any industry codes of conduct endorsed by a government entity?

2.6* Do you have any private sector codes of conduct, best practices, seal or trustmark programs which are either endorsed by a business federation, or widely used by the private sector either generally or in a specific sector?

2.7* Do you have any government regulation or applicable private sector practices requiring Web sites to have security policies, rules or technical measures in place to protect the personal data of visitors from unauthorised access, improper use or disclosure, and the like?

3. Compliance

Keeping in mind the norms identified above, please explain how compliance with these is ensured at both the national and cross-border levels with regard to online activities.

3.1* Where do companies obtain information and advice on compliance with the norms identified above? For instance, do they consult with a lawyer (either external or internal), make use of internal privacy compliance officers (whether because of legal requirements or business practice), use consultants, or consult with data protection or consumer regulators?

3.2* Are there administrative procedures, reviews based on best practices, software tools (whether used for privacy protection or privacy auditing), or other means for reviewing the privacy practices followed by businesses engaged in online activities?

3.3* Do oversight entities exist which are competent to review compliance with the norms mentioned above? For instance, are such entities government agencies, independent data protection authorities, or private sector bodies?

3.4* How are such oversight entities set up, and what powers do they have?

3.5* Do companies voluntarily engage in self-assessment of their privacy practices? Are such self-assessments made publicly available?

3.6* Are companies encouraged or required to appoint a company privacy officer in charge of privacy compliance?

3.7 Are companies required to notify their data processing to an oversight entity?

3.8* To what extent are technological solutions for privacy protection used in your country?

3.9* Are there any other compliance procedures or processes used which are not mentioned above?

4. Enforcement

Please explain how the norms identified above are enforced.

4.1* To which organisations, entities, or persons may parties or data subjects turn to obtain enforcement of the norms?

4.2 What remedies are available to injured parties, and how can infringing data controllers be forced to comply with the applicable privacy norms?

4.3* What kind of remedies can private sector entities impose for violations? For example, withdrawing a seal or trustmark, blacklisting a company, or bringing the case to court?

4.4 Are administrative or penal fines available to deter or punish violations, and who is authorised to request such fines (*amendes*)?

4.5 Can a court order other criminal penalties, such as imprisonment?

4.6 Can injured parties obtain monetary compensation for damage caused to them by violations (*dommages-intérêts*)?

4.7* Can an oversight entity (whether in the public or private sector), authority or court impose injunctive relief (*exécution d'un droit*), such as ordering that access be granted to personal data, or prohibiting a data transfer?

4.8* What sorts of procedures exist for handling complaints?

4.9* Is it possible to file complaints online, or are there other possibilities for making use of Internet or online technologies for the resolution of disputes?

4.10* Are third party dispute resolution mechanisms, such as alternative dispute resolution (ADR) proceedings (whether in the public or private sector), used for the resolution of privacy-related disputes?

4.11* Is auditing of privacy practices used as a method of enforcement? If so, is auditing voluntary, or is there an obligation to be audited? Note that "auditing" in this sense is to be understood widely, and includes, for example, not only auditing of practices by professionals, but also auditing of online practices using software tools (such as software robots to evaluate Web site compliance or to find out where a seal or trustmark is being displayed).

4.12* Are technical standards used to ensure compliance (for example, P3P)? Are there any legal incentives for using such standards?

5. Public awareness

Please explain how members of the public are made aware of their privacy rights and of privacy violations in the online environment.

5.1* Are companies required or encouraged to post privacy policies or to make any reference to notification to an oversight entity, or both?

5.2* Are companies encouraged to appoint a contact person who can provide information on privacy practices or to whom persons can turn with complaints or questions?

5.3* Are violations of privacy norms publicised, and if so how (for example, by posting information on the Internet, or publicity to the press)? Who publicises such violations?

5.4* Does the public or the private sector undertake campaigns to educate the public as to their privacy rights, and if so, how is this done? Is this done through special campaigns or by continual and regular activities?

Chapter 12

INVENTORY OF PRIVACY-ENHANCING TECHNOLOGIES

This chapter sets out an inventory of privacy-enhancing technologies (PETs), discusses methods of data collection, analyses different types of PETs and makes recommendations to the private sector for encouraging increased development and use of such technologies.

Chapter 12

INVENTORY OF PRIVACY-ENHANCING TECHNOLOGIES

Introduction

Technology can play an important role in enhancing the protection of personal privacy online. Using the 1980 OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data as a guide, this paper aims to analyse the availability and variety of privacy-enhancing technologies (PETs), consider the factors affecting adoption of PETs, analyse the relationship between technology and privacy, and form a basis for policy makers to discuss the use and deployment of such technologies.

Privacy enhancing technologies (PETs) commonly refer to a wide range of technologies that help protect personal privacy. Ranging from tools that provide anonymity to those that allow a user to choose if, when and under what circumstances personal information is disclosed, the use of privacy enhancing technologies helps users make informed choices about privacy protection.

PETs can empower users and consumers seeking to control the disclosure, use and distribution of personal information online. PETs can also aid businesses and organisations in enforcing their own privacy policies and practices. In an era of consumer concerns about online privacy, PETs are crucial tools in managing the flow of personal information on global public networks.

This paper discusses methods of data collection, analyses different types of privacy-enhancing technologies and makes recommendations for encouraging increased use of these tools. It also briefly touches on security technologies, many of which were initially designed to protect the confidentiality of information but can also enhance privacy. In addition, many technologies that can enhance security – such as digital signatures or authentication technologies – can enhance the privacy of or ensure the integrity of communications or online transactions, but because they are designed to ensure the identity of the individual, may limit the potential of anonymous online activity.

As a result, because so many technologies can be used in many different ways, it is crucial to recognise the context in which any given technology is used. Different products, different technologies and various functions can serve different purposes depending on the preferences of the user and the implementation of the particular technology. As a result, it is important to keep in mind that consumers and policy makers will need to be educated about and understand the different ways in which various technologies can be used to achieve different goals.

The 1980 OECD Guidelines for the Protection of Privacy and Transborder Data Flows

The rapid rise of interconnected, global networks and the increasing flow of personal data across national borders have raised awareness among policy makers, consumers and companies about privacy concerns. The *Guidelines for the Protection of Privacy and Transborder Data Flows of Personal Data*, while adopted by the Organisation for Economic Co-operation and Development in 1980, were adopted in an earlier era of technological development and expansion, and remain relevant and topical today. In 1980, the OECD was primarily concerned with the rise of processing of personal data transported across national borders by large corporations and data processing firms; today, the OECD addresses the sharing and distribution of personal data across borders through Internet-based technologies and sites. The eight core principles established by the OECD in the 1980 Guidelines 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.
    - 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.

Despite differing national approaches, varied consumer preferences and a wide variety of self-regulatory approaches developed by business, the OECD Guidelines continue to represent a consensus viewpoint on data protection. The OECD reaffirmed that the Guidelines provide an international foundation for privacy at the 1998 Ottawa Ministerial Conference, *A Borderless World: Realising the Potential of Global Electronic Commerce*.

The OECD has long recognised the role that technology can play in enhancing privacy in the online environment. In 1997, the OECD issued a report, *Implementing the OECD Privacy Guidelines in the Electronic Environment: Focus on the Internet,* which encouraged the development of policies and technologies that would guarantee the protection of privacy of individuals on global networks. Ministers affirmed the important role that technology can play in protecting privacy in the 1998 Ottawa Ministerial Declaration, noting that they would "encourage the use of privacy-enhancing technologies" in OECD

member countries. The challenge for industry, consumers and governments is to effectively implement the principles embodied in the 1980 OECD Guidelines in the face of rapid technological change.

The demand for privacy-enhancing technologies

Use of the Internet has skyrocketed since 1993 with the introduction of the graphical user interface and the 1995 movement of Internet administration to the private sector. Once a predominantly North American phenomenon, today the Internet is international in nature and use. With telecommunications deregulation, reduced prices for computer hardware, software and Internet access, and increasingly robust services and products available online, Internet usage is expected to continue to grow at brisk rates for the foreseeable future.

Internet usage varies widely, from simple information presented online to complex systems that may host thousands of simultaneous Web sites. For individuals, primary Internet access may be through their workplace, a school account or a personal account through an Internet Service Provider (ISP).[1]

As usage grows, so does the commercial viability of the Internet. Companies have been flocking to the Internet for several years, representing businesses in every industry, from small entities to multinational corporations, from every region of the world. The international nature of the Internet makes the global network an attractive, and often lucrative, new alternative for increased market penetration which supports a diverse and expanding set of business models that make categorical or "one size fits all" solutions impractical and in a worst-case scenario, counterproductive.

At the same time, concern over the collection of personal data has grown for a number of reasons.

First, advanced technologies make it possible for data to be collected about individuals that visit Web sites, participate in chat rooms or newsgroups, send e-mail or otherwise use Internet services without their knowledge or consent. All the data that is collected is not *directly identifiable personal data*; rather in many cases, it is essential information to support system maintenance and network viability. Nonetheless, consumers are often surprised to learn that such information may be collected.

As discussions about privacy continue in the media, among consumer groups and in a wide range of fora, individuals are often surprised by the amount of information collected about them both online and offline. For instance, they often do not realise how often they are filmed on security cameras in public places, that "electric eyes" may be triggered with automatic doors or that turnstiles on public transportation count and, especially in the cases of pre-purchased long-term passes, that their travels are recorded at turnstiles or tool booths.

Second, much more can and should be done to enable individuals who are concerned about online privacy to utilise the empowering tools that protect them from the unwanted disclosure of personal data (PD). While the majority of the most heavily trafficked Web sites have posted privacy policies, industry sectors have developed and implemented self-regulatory initiatives, and some national governments have passed data collection laws, surveys show that many individuals remain concerned. An October 2000 study by the National Consumers League and conducted by Harris International found that 56% of individuals are concerned about the loss of personal privacy (National Consumers League, 2000). While the Internet has become increasingly user-friendly in recent years, the technical nature is often intimidating for many users who believe that there is little, if anything, that they can do to prevent unwanted data collection, use or distribution.[2]

Third, while recognising that different approaches to privacy among nations is a norm, this landscape complicates the privacy issue for policy makers, businesses and individuals. Europe and the United States, for example, have very different approaches to the issue of privacy (as demonstrated by the recent US-EU

safe harbour agreement), creating a significant challenge for companies that serve both European and US customers.

For consumers and individuals, the differing approaches to privacy in different jurisdictions present a special challenge. A consumer using the Internet may not realise that he or she is visiting sites that may or may not be located in their home country, and, as a result, may not understand that the data protection environment to which they may be accustomed may not apply to the site with which he or she is sharing information. This situation may become particularly worrisome when the consumer is sharing sensitive data.

Of course, no technology can address the myriad of privacy laws in every country, region or jurisdiction. It would simply be impossible given the differing approaches and the limitations of technologies. For example, it is often difficult to identify where a Web site visitor is coming from, where the country of origin for a given consumer might be or for a Web site to keep up with the often rapidly changing regulatory and consumer preferences in every country around the world. As a result, privacy-enhancing technologies installed on an individual consumer's computer, configured to respect perhaps both the consumer's personal preferences and national law, may be an effective means for addressing privacy concerns, particularly if combined with a wider respect and recognition of internationally-accepted privacy principles.

I. Methods of data collection

Data can be collected in a variety of ways. With continuing advances in technology, there can be no doubt that new techniques will emerge that facilitate data collection. As such, this list considers only some of the most widely used techniques and should not be considered exhaustive.

In addition, it is important to recognise that in terms of transparency, significant progress has been made to date. With growing concern from individuals, many Web sites – and certainly most of the most popular Web sites – now prominently display links to their privacy policies, clearly disclose their data collection practices and provide information regarding the use of collected data. There has been, in recent years, a growing awareness by online sites that individuals not only look for, but also make decisions based upon, the existence and content of posted privacy policies.

Data collection and analysis technologies and methods can be highly useful in enhancing the online consumer experience, improving services and developing more customised content, products and services.

Commercial Web sites collect information through both voluntary and passive means. Voluntary measures include registration pages, surveys and other online forms. With voluntary means, some action on behalf of the user is generally required and the user is aware that data is being provided and/or collected. Passive measures typically include aggregate data collection and site usage selection; the user may not be aware that this generally non-personal information is being collected. The use of cookies is often characterised as passive, but because all commercial browsers allow users to reject all cookies or accept certain cookies only after the user has approved the acceptance of the cookie, the use of cookies can also be active.

Passive collection of transactional data

Non-personal data revealed just by surfing a site tell a good deal about online activities. Web servers can collect information about what pages a user looked at, how long a particular page was displayed on a screen, the URL of the most recently visited site and the URL of the next site requested.[3]

None of this information is inherently personally identifiable. In fact, much of this anonymous information is aggregated and used for marketing and site analysis. For example, it may be very helpful for a Web site operator to know that their home page received 100 000 hits one month from 54 000 unique visitors, but that a page highlighting last-minute sales or news on a particular topic received only 2 000 hits.

Much of this information is collected to allow those responsible for maintaining the site to perform necessary system maintenance, auditing, and optimise performance to an individual's computer and connection speed and other system functions. This information is needed to ensure that a Web site is performing properly and providing timely access to visitors. Some information may be collected as part of the normal functioning of the Web server software itself and stored in maintenance logs used for ensuring system reliability.

Personal collection of personal information

Some personally identifiable information can be collected through passive means, especially if a user has configured his or her Web browser in certain ways. Some Web sites collect information from individuals who store their email address or name, for example, in their browser. Users may not know or be aware that this information is being collected. It should be noted, however, that most sites with privacy policies that do collect this information do disclose those practices, and that users can avoid having their information disclosed by simply not including this information in their Web browsers, as it is not required for the proper functioning of any browser application.

Active collection of transactional or personal information

Many sites actively collect transactional or personal information by deploying specific technologies or business processes on their Web sites. Several approaches are quite explicit and require user participation in order to collect information, such as through online forms or user accounts. Others may be less obvious to a Web site visitor, such as cookies, "Web bugs" or clear .gifs.

User accounts

Some Web sites allow users to establish an online account. Generally, account information is stored at the Web site itself, including a username and password. User accounts often are used when a user will likely need to access historical information or data collected offline, such as for an airline frequent flyer programme or a retail e-commerce site. When the user visits a site, he or she is generally prompted to log in, usually by providing a password and username. Upon successful login, the user is granted access to the information stored in his or her account.

To establish an account, a user may have to provide basic contact information, preferences and credit information, if the site charges for its services. Many of these sites often collect and maintain user usage and order history, clickstream and personal information necessary to complete the user's transaction or requests. Preference information also aids a Web site in determining which offerings are most attractive and useful for its visitors, as well as which offerings are not. By determining consumer preferences based on clickstream data – both what the consumer is interested in and what he or she is not interested in – the consumer experience can be greatly enhanced. Such data collection is legal and often desirable for consumers, and sites with privacy policies often disclose that such data is collected. In any case, a site that provides notice about its data collection procedures, whether voluntarily or as prescribed by law, should disclose its clickstream data collection procedures.

Because of the significant overhead investment, maintenance and security requirements for large-scale systems, generally only companies that need to maintain this information on their own server for operational reasons implement user accounts.

Online forms

Online forms are a common method for collecting information from consumers. Forms can be used in almost countless ways – from collecting data from a user who has requested more information about a company's products or services to participating in an online survey. The use of forms is widespread and their utility limited only by the imagination of a Web site designer.

In some cases, a site may request that a visitor register even if the service, product or content offered is free. Generally, registration brings additional benefits not available to unregistered users. A site that provides online electronic greeting cards, for example, may allow its registered users to create personal address books or establish a calendar of important events, enhancing the site's utility to the user and creating a reason for the user to return to the site in the future.

In many cases, registration is not required to use a site, but the additional services are not available to non-registered users. The choice is up to the consumer. Many e-commerce sites, for example, will allow an individual to place an order without creating an account. However, the user may not be able to return to the site and take advantage of advanced customer services, such as checking delivery status, using gift certificates or storing shipping addresses online for future use. Users that do not register may have to re-enter vital information multiple times, be unable to take advantage of loyalty programmes, be unable to resume a previous transaction, browsing or shopping experience or be able to modify their online preferences.

The benefits for companies in collecting this information is clear. By asking the visitor to fill out a registration form with personal information such as name, address, how the user learned about a Web site or preferred topics, companies can develop valuable customer profiles and analysis. This data can in turn be used to improve Web site content and refine the services or products provided.

Cookies

Many Web sites use "cookies" to deliver client-side information and enhance the user experience. Cookies are text files that allow a Web server to store and retrieve information on the client side of the server-browser (client) connection.

In most cases, data stored in cookies is not detrimental to the protection of personal data. Rather, it is essential to providing an enhanced customer experience. A cookie may, for example, track whether a specific user has visited the site previously. Depending on the information in the cookie, the Web site may offer "first-time" visitor information, or, alternatively, thank the visitor for returning. This information is not necessarily personally identifiable, especially if the browser has been used by others or if the computer is shared, as in an office environment.

Cookies also greatly enhance online functionality, as many common e-commerce functions would be impossible without the use of cookies. An example is helpful. When a user visits an e-commerce site and adds products to his or her virtual shopping cart, the information regarding what products the customer has identified while he or she continues shopping, fills out shipping information.[4] The information about which products may be in the shopping cart is stored on the server itself, not on the user's computer. The server then retains control over the information about the individual and his preferences, while the user's computer only contains information that will allow the server to link the session information stored at the site with the individual user. These techniques, known as state management, are necessary to keep track of

which users are selecting which options. Without state management, it would be impossible to conduct online commerce or provide a seamless user experience.

Cookies may also be used to ensure that a Web page is properly delivered to a user. Web pages can be complex, comprised of text, graphics, images, frames and other elements. Delivering each Web page may represent a number of separate requests from the client computer. For example, the client computer may request the initial delivery of the page, of separate graphics or images, or embedded frames that comprise a single page. Cookies, stored on the user's machine, help a Web server recognise when a page has been properly served to the individual.

Cookies used to control the user environment are generally temporary. These cookies are often not permanently stored on a user's computer and are only used to control the user's session. They do not typically contain any personal information.

Persistent cookies are stored on a user's computer until their expiration date. A persistent cookie typically stores more complex information, such as user login information, account identification or other unique data. The data stored in a persistent cookie may or may not be personally identifiable.

Cookies facilitate consumer Web site use (as opposed to online user accounts or storing the temporary information on the Web server itself) because they allow the site to utilise the resources of the client computer, rather than the Web server. For a site that may be hosting thousands of simultaneous users, the ability to share computing resources with the individual improves performance for all users.

However, it is recognised that cookies are the target of criticism. One issue that is often highlighted is that cookies can be written to the user's computer without the user's knowledge if the browser is so configured. Cookies have received negative coverage in the press and from privacy advocates, and significant misinformation about cookies circulates widely on the Internet. Some see cookies as an invasion of privacy, some fear having a remote computer store data on their computer, some believe (incorrectly) that cookies can pass along viruses or otherwise do damage to their machines.

Generally, cookies can only provide information to the Web site that stored the cookie originally. In other words, a cookie created by Web site A cannot be read by Web site B. This practice, defined in several Internet RFCs,[5] virtually eliminates the danger of one Web site reading information stored by another.[6]

Like many technology features, though, cookies can be implemented both to enhance and improve the consumer experience as well as for more problematic uses. The fact that a site uses cookies is neither "good" nor "bad" as technology itself is neutral. However, cookies can store a good deal of information about individual browsing habits, and because they can be deployed in so many different ways, can raise concerns among consumers.

Users have many tools available to control cookies and the information collected through the use of technology. Users that fail to manage their cookies, to at least occasionally review the cookies stored on their systems or use cookie management tools may find that some sites collect more information than they are comfortable with.

All popular browsers have some form of cookie management tools built in, allowing a user to reject all cookies, accept all cookies or decide to accept cookies on a case-by-case basis. Users concerned about cookies should be encouraged to use these features, which are available to all Web users. In addition, all browsers allow users to review the cookies stored on their systems, and to delete those that they no longer wish to keep or find offensive. Sites like the OECD Privacy Policy Generator that ask specific, detailed questions about cookie usage also help increase transparency about the use of cookies. For those seeking

more robust features, cookie management tools are more fully explored in the following section on specific PETs .

Web bugs (Clear .gifs, 1x1 .gifs, Invisible .gifs or Beacon .gifs)

Web bugs are small images, generally one pixel, that are placed on HTML pages[7] that are often used to track usage and provide information to the party that places the image.

Generally, these images are used to determine how many hits a page receives. Web bugs are most often used to gauge Web traffic, how many times a page has been viewed, and other administrative or site monitoring requirements. A Web usage monitor will report how many times the image was accessed – a standard piece of non-personal data used in system maintenance. They may also, however, be used to solicit additional information, including the URL of the page on which the image is stored, the type of browser being used, the time of viewing, the client IP address, or to retrieve information stored in cookies. Such images may be used in any HTML code, whether on a Web page or in HTML email.

Because these images typically cannot be seen nor blocked by traditional cookie blockers[8] or other similar technologies they have raised concerns among privacy advocates. The increasing use of HTML e-mail has added to the concern.

Web browsers

The advent of Web browsers was a crucial step in making the Internet and global networks accessible to individuals and the general public. Before the development of Web browsers and HTML, the Internet was largely limited to academics, engineers and computer aficionados. Without Web browsers, the Internet would never have developed into the valuable information medium that it has.

Web browsers have become increasingly complex and robust since their introduction in the early 1990s. Web browsers now integrate e-mail client software, include FTP capabilities and support a wide variety of plug-ins.[9] In using the features of the Web browsers, some users choose to store personal information, such as e-mail addresses or a name, in their preferences settings. This information may be accessible to a Web server; the browser will provide this information to the Web server when requested.

Users of more advanced e-mail clients such as Microsoft Outlook, Web-based e-mail, AOL or other proprietary online services need not enter this information into their Web browser customisation features. Some users that rely on e-mail clients bundled with Internet browsers must enter at least their e-mail address in order to have their reply-to addresses properly appear or the sender's identity be properly represented to recipients of their e-mail messages. While designed as a convenience feature, the ability to request and receive information stored in a preferences or setting file may be the source of the disclosure of one's e-mail address or other information that the user chooses to provide.

Benefits of data collection

Ministers gathered in Ottawa in 1998 noted the benefits of electronic commerce to all stakeholders, recognising that for electronic commerce to flourish on a global basis users must work together to achieve practical solutions to the challenge of a borderless world.

When considering the privacy issue, policy makers, advocates and industry often point to a conflict between businesses' need for information about their consumers and the desires of individuals to control their personal information. This distinction is perhaps too limiting and unfairly characterises business and consumers as opposed on the issue of privacy. In fact, the private sector has, along with the development of

PETs, championed the widespread adoption of privacy policies and promoted effective self-regulatory efforts.

The following section highlights some of the key benefits of data collection.

User convenience

Collecting information about an individual user creates the opportunity to provide customised, personalised service to each Web site visitor. As examples of the variety of ways the Internet meets consumer demands, many portals, online shopping and news sites offer visitors the opportunity to create accounts or use other technologies to customise their online experiences.

Amazon.com, for example, can be set to remember a customer's name and previous purchasing history. This ability to welcome returning customers and provide a custom home page with suggestions for products allows Amazon.com to build customer loyalty and address critical inventory control operations through tailored messages that promote a product that an individual might like or special offers based on a user's preferences. CNN.com allows users to prioritise the issues and news topics in which they are most interested. And many e-commerce sites allow a user to create accounts and store credit card numbers, shipping addresses and billing preferences, simplifying the use of the site's functionality in the future. Many of these features have analogues in the offline world. For example, a consumer is far more likely to frequent a neighbourhood book store where the owner is familiar with his or her literary preferences, or the corner coffee shop where the counter clerk always remembers his or her name and how he or she takes their coffee. In many ways, the ability to personalise and customise the online experience provides a "neighbourhood" or friendly feel to what might otherwise be a cold and purely businesslike transaction for the consumer. Of course, consumers who prefer more anonymous or less familiar experiences certainly have that option, too.

All of these features enhance the online experience for individual users by making the use of these sites more convenient and timely.

Enhanced marketing and business development

The online environment is an extremely competitive one, as many e-commerce retailers have learned in the past several months. Gaining market share by building customer loyalty, expanding the customer base and increasing the number of transactions per customers (in other words, creating repeat sales) is crucial. Because customer retention is far less expensive than customer recruitment, creating an ongoing relationship with a customer is often a deciding factor in online commercial success.

Providing customised services, responding quickly to consumer concerns and respecting customer preferences are all important elements for a business seeking to develop a relationship with its customers. To do so, companies need to fully understand their market and consumers. That knowledge can only be obtained through the collection of data from existing customers.

Customers benefit from these marketing techniques. A frequent traveller, for example, may benefit from an airline that offers discounts or other benefits to its most loyal customers. A site may be able to offer personal customer service online or store user preferences. These tools encourage customer loyalty and enhance the potential success for online commerce.

User experience enhancement/consumer protection

The collection of data not only enhances the browsing experience for individual users through personalization, customisation and provision of enhanced services from a given Web site, it may also play a crucial role in protecting consumers or enhancing their online experiences.

An example may be illustrative.

Consider an online travel agency where a user has recently purchased an airline ticket for a trip to Paris, France. If the same user then mistakenly books a hotel room in Paris, *Texas* for the same dates that the user is presumably travelling to Paris, *France*, the system could ask the individual to confirm that the hotel reservations in Paris, Texas are accurate. Such a proactive intervention could prevent a user from being unexpectedly charged for hotel reservations that he or she did not need, or from arriving in Paris with incorrect lodging arrangements.

II. Privacy-enhancing technologies

Despite the recognised role that personal data plays in promoting key technical and commercial operations, individual users remain concerned about the risks associated with the sharing of their personal data. As noted in the 1998 OECD Ministerial Declaration, privacy-enhancing technologies (PETs) are an important element in promoting the protection of personal data; moreover, they enable users to make informed choices about privacy. PETs that provide users more control over their personal information can help alleviate many of the concerns that consumers have identified as barriers to the growth of electronic commerce. PETs are also able to allow consumers to exercise the broadest possible choices. PETs allow users to make more subjective and detailed decisions concerning their information.

PETs vary widely in their functionality, capabilities, technical structure and usability. However, all PETs aim to give the individual user or technology manager the capability of controlling if, how much or under what circumstances information is disclosed.

At the same time, it is important to realise that PETs cannot, and are not designed to, address every consumer or policy maker's concern about data collection. PETs are simply one of many tools available to consumers in the online environment, and as this paper discussed, one that consumers should be encouraged to use if they have concerns about data collection.

The biggest limitation of PETs is simply lack of consumer awareness. PETs have recently gone through a significant shakeout. As a result of increasingly difficult market conditions for all start ups and low awareness and uptake by consumers, a number of PETs have either gone out of business or have significantly revised their operations. In short, consumers must be aware of the availability and capabilities of PETs in order to benefit from their features, just as a consumer must use his or her seatbelt in order to be better protected in the event of a car accident.

In addition, even consumers that choose to use PETs must be encouraged to use them consistently. Many users in search of simple, efficient online experiences give up using PETs after a short period, negating the benefits that a PET can have.

Finally, consumers must choose the right PET or other technology to address their particular concern. For different consumers, the primary concern could be anonymity, conducting trustworthy transactions, control over personal data or transaction security. As illustrated in this paper, there are a wide variety of PETs and security enhancing tools, and consumers must understand that not every PET will address all of their concerns. For example, while an e-mail encryption program may work well at keeping electronic correspondence confidential, it will do little to help the consumer manage cookies or keep clear .gifs from

displaying on a Web page. Governments, industry, consumer groups and privacy protection authorities and experts all have a role in helping consumers make the right decisions about which PETs are best suited to address their individual concerns.

Consumer concerns about data collection

Consumer concerns can be generally categorised into several areas.

Sharing of data with third parties

Consumers who have provided personal information to a particular site, organisation or business should not have that information shared with a third party (*i.e.* one not involved in or associated with the site, organisation or business in question) without their permission or knowledge.

Security fears

Users often are concerned that the data collector may not adequately protect personal information from accidental or malicious disclosure. Lack of security or misinformation about available security may deter consumers from providing information across the Internet. Well-publicised disclosures of consumer information, including credit card information, from a few popular Web sites has increased public fears. While the fear has increased, awareness of the need for security or how to evaluate security has not increased dramatically.

Lack of knowledge about data usage

The rapid growth of electronic commerce demonstrates that consumers are willing to provide information, even personal data, in exchange for services, personalization features or customised content. However, many consumers are concerned about how information that they provided will be used by the receiving organisation. A consumer, for example, may be very comfortable knowing that personal information is used to create customised news updates, but less willing to provide the same data if used for unrelated marketing purposes.

Consumer "profiling"

Businesses often use consumer information to create customer profiles. Profiles may be personal (*i.e.* related to a specific individual consumer) or aggregated (*i.e.* where common characteristics are used to identify a specific demographic). Profiles can be beneficial to consumers and greatly simplify their online experiences, but the concept of "profiling" has received extremely negative coverage in the media. Some consumers are uncomfortable being categorised, having their order history stored, or having a Web site maintain personal information. In addition, some consumers seem particularly concerned with the practice of data collected at one site being combined with offline information or data collected from other online sites or stores.

Identity theft

The sharing of particularly sensitive information, such as credit or financial data, is of particular concern to many consumers and policy makers. The abuse of personal information may, in some circumstances, result in identity theft. While identify theft can occur online or offline, there has been a rise in identity theft in recent years. It is unclear to what extent this rise is attributed to poor data security, increased information theft or abuse, or if it is simply easier for criminals to share the information necessary to steal an individual's identity on global networks. Whatever the case, increased awareness

about the crime of identify theft has undoubtedly made some consumers more hesitant to share personal information.

Security and privacy

There is, of course, a close relationship between security technologies and privacy technologies. That the concepts of privacy and security are so closely related is a common source of confusion for many. The two are not separate, and for the purposes of protecting individual information cannot be separated, but at the same time they are not interchangeable technological concepts.

The OECD recognised in the 1980 Guidelines that security was a crucial element in protecting privacy. Without strong security, personal information cannot be properly secured from misuse or abuse.

It is important to note that when the technology community[10] refers to security, it is generally referring to the protection of the data from accidental disclosure, misuse or abuse, and destruction or corruption of data, whether personally identifiable or otherwise. Security may apply to the storage, transmission, backup or other transactions involving data. Security solutions, products and services typically seek to prevent the introduction of viruses, eliminate network vulnerabilities, limit access by unauthorised users and authenticate data, messages, or users.

These are critical tools in protecting stored or transmitted personal information. Without the ability to secure personal data, an individual cannot be assured that his or her data is being properly protected once shared with an online site, business or organisation. Without security technologies, it would be difficult – if not impossible – to protect data and provide privacy tools to individuals, corporations and other organisations. The ability to provide consumer choices about data collection and to secure collected or stored data relies on the widespread availability of strong security technologies.

Beyond the requirement that personal data be protected by reasonable or adequate security safeguards, privacy protection includes limits of a "legal" nature to the collection, handling, storage or transmission of personally identifiable or aggregates data collected from individual users. Whether personal information is collected, how it is used or shared, what options a user may have, whether a user may access stored information, and who has access to that stored data are all issues addressed in the discussion of privacy.

Personal privacy-enhancing technologies

It is important to recognise that privacy preferences often differ significantly, as individuals have different concerns or prerogatives regarding the treatment of personal information. It is also important to note that in the following inventory of technologies and consumer options, some are software tools that are stored on the individual's hard drive, some are deployed on a user's network or some are online services. As such, even when using privacy-enhancing services that are provided online or downloading PET software, consumers should take care to carefully review the privacy policies of the hosting or providing site.

Cookie managers or blockers

Cookie managers or blockers are applications that allow the user to know when cookies are being written to his or her hard drive, to manage the acceptance of cookies, and to view what information is stored in an individual cookie. Cookie managers or blockers vary widely in their usability and features, but all give the individual more control over cookies stored on their personal computers.

Cookie managers or blockers can help users determine which sites have placed cookies on their computers, when the cookies were placed and the expiration dates of the cookies. They also allow users to

delete or retain a particular cookie. However, because the data in many cookies is indecipherable to the average user, cookie managers may be limited in their effectiveness or usability to users who wish to know exactly what information is being stored on their computers in cookie files.

It is important to note that all commercial browsers allow an individual to determine whether he or she wishes to receive cookies. No additional applications are necessary as this functionality is inherent to the browser. In addition, because cookies are simply text files, any user can view any cookie stored on his or her hard drive. However, the data stored in cookies is generally difficult, if not impossible, to understand for the common user as the data may be encoded to simplify communications with the Web site that originally placed the cookie.[11]

Cookie managers are widely available commercially, and several products are available as freeware or shareware.

Ad blockers

For users who do not like and appreciate the targeted advertisements that many sites provide, software to block the delivery of online advertising is available. These applications keep ads from being delivered to the end user and thus, from tracking a client. However, because ads can take many different forms, these applications vary in their ability to completely block advertisements from being delivered to the user.

Ad blocking software may be appropriate for users who have slow connections and do not wish to use valuable bandwidth downloading advertisements. The blocking software also benefits those who are fundamentally opposed to Internet advertising or individuals who wish to prevent their children or other users from viewing online advertisements. However, while several commercial products are available, ad blocking software has seen somewhat limited adoption. Significantly, relatively little personal information can be collected simply from viewing an advertisement.

Encryption software

Encryption software allows the user to encrypt – or scramble – digital data. Users may opt to use encryption to protect the contents of their e-mail messages, stored files and online communications. Once encrypted, only users that have the appropriate digital keys may "unlock" the encrypted information. The digital keys most often take the form of a token which may be incorporated into browsers, biometric identifiers, smart cards and other storage devices depending on the complexity or sophistication of the particular application. Encryption software varies widely, both in terms of available strength[12] and functionality.

Encryption products that combine hardware and software solutions are popular, especially in complex or advanced communications solutions, telecommunication equipment, copyright protection schemes, biometric authentication, smart cards and some firewall products. Hardware-software solutions for individual use, however, are relatively uncommon at this time.

Encryption software can be very useful for the individual user. Not only can encryption protect individual stored files, it can also be used for authentication purposes and to ensure private communications. A powerful tool, encryption can be used in a wide variety of circumstances to provide privacy and security for an individual user.

At the same time, users unfamiliar with sophisticated technology may find encryption products difficult to use. Even relatively advanced, user-friendly encryption products designed for retail distribution may be confusing for those unfamiliar with the technical capabilities afforded by encryption technologies.

Software publishers have developed widely varying products. Effective use of encryption generally requires some effort on behalf of the individual user.

Even so, encryption products and the integration of encryption into standard consumer applications creates an effective and efficient tool that can significantly enhance consumer privacy and the security of an individual's data. Empowering users with robust PETs requires the availability and usability of strong encryption.

Encryption software is widely available and comes in many forms, including hard disk or file encryption, e-mail encryption, personal firewalls, authentication tools and communications utilities.

Web-based technologies

Anonymizers

Anonymizers are Web-based services that offer anonymous Web surfing by acting as an intermediary between the client and the Web site. Generally, an anonymizer service prevents a Web site from being able to identify the IP address of the visitor or planting cookies on an individual's computer. However, for that very reason, anonymizers may also prevent a user from accessing personalised services or taking advantage of certain functionality that requires persistent cookies in order to function properly, such as online account access or using purchase histories.

Anonymizers can be extremely useful for consumers browsing the Web or for sending anonymous e-mail. Simple and easy to use, anonymizers are widely available on the Web and, in many cases, may offer some version of their services for free. For those seeking to keep their Web surfing habits confidential, anonymizers can be an excellent choice.

It is worth noting, however, that anonymizers do not necessarily guarantee that personal information will not be disclosed. Just because a transaction is anonymous does not mean that it is private. Because the anonymizer acts as a go-between an individual Internet user and the Web sites or other Internet services he or she is using, data in a server log could be used to recreate a user's surfing habits. While anonymizer services implement business practices that prohibit such practices – such as regularly deleting their Web logs and not keeping backups of system files that may disclose personal information or be used to help identify an individual – anonymizer services are not inherently foolproof.

In addition, anonymizers create certain concerns for law enforcement officials or others charged with ensuring responsible online usage. Because anonymizers can hide the identity of an individual – or at least make it very difficult to determine an individual's identity – anonymizers raise concerns about accountability or the enforceability of online usage policies.

Anonymous e-mail services are also widely used, allowing users to send e-mail without disclosing their own e-mail address or the originating e-mail address. A resource page can be found at www.publius.net/rlist.html.

Platform for Privacy Preferences Project (P3P)

The Platform for Privacy Preferences Project (P3P) is a proposed standard developed by the World Wide Web Consortium (W3C) that is designed to give users more control over their personal information by allowing P3P-enabled browsers and servers to analyse privacy policies. The proposed P3P standard is based on XML[13], allowing the creation of common vocabulary for identifying privacy practices.

Because P3P is a technology built upon the XML platform, it allows browsers and servers to "negotiate" before completing a request for data delivery. Once a Web page is requested by a given browser, for example, the browser will only deliver the page back to the user if the P3P preferences set in the browser are matched by the Web site. Because a consumer's preferences are set by the individual and the policies of the site are defined by P3P, users are not required to analyse the privacy policies of every site that they visit.

A company defines its privacy policy in the terms established by the P3P standard. Elements include POLICY, ENTITY, DISCLOSURE, REMEDIES, DISPUTES, STATEMENT, CONSEQUENCE, PURPOSE, RECIPIENT, RETENTION, DATA-GROUP and DATA elements. Each element has required attributes that further define the privacy policy of the covered site. The combination of core elements and different attributes creates significant flexibility for both Web sites and consumers. With a wide range of possible choices and combinations of elements and attributes, consumers can develop privacy preferences that accurately reflect their own personal choices and communicate those preferences to P3P-enabled Web sites.

To assist companies in developing P3P compliant products, several companies have created P3P policy editors or development tools that greatly simplify the development of compliant products.

A user must have software that allows the browser to translate and understand the P3P specification. Once configured to an individual user's preferences, the interaction of P3P between servers and the individual can be largely invisible to the user, greatly simplifying consumer usage. Here, too, many companies are developing client-side P3P tools that are increasingly available.

P3P is a rapidly advancing standard that is being utilised in a growing number of settings. The growing use of P3P is due to a number of factors.

First, P3P allows a company to define its privacy policy through technology. Doing so directly addresses one of the most fundamental concerns of many privacy advocates, namely that many privacy policies are difficult for users to understand or that users may not comprehend the full implication of the legal or complex language often found in privacy policies. P3P eliminates a great deal of confusion as the terms are fixed.

P3P also allows a user to define his or her privacy preferences technologically. The user can configure his or her software to reflect what information, if any, he or she wishes to disclose and how the data can be used. Such flexibility allows a user to establish the boundaries of PD collection based on what he or she feels is appropriate. The ability of a consumer using P3P to create a privacy profile that reflects his or her personal, national or cultural preferences greatly empowers an individual in his or her online activities.

Second, P3P requires little ongoing user intervention. Once a user configures his or her own computer, the analysis of privacy policies at P3P-enabled Web sites is relatively seamless. While a user may, depending on the functionality of the P3P client software, on occasion override his or her established preferences in order to access a non-P3P site, the user can be confident that his or her configured preferences will be respected on an ongoing basis.

Third, P3P respects the ability of both companies and individuals to establish different privacy practices. P3P is quite flexible, and allows a company to define its practices and the user to define his or her data collection preferences. P3P empowers individual users to create a unique set of privacy preferences while at the same time using technological safeguards to ensure that those choices are respected.

P3P is still emerging as a viable technology in a rapidly evolving market. Many companies have committed to the integration of P3P into their respective product lines, but P3P implementation remains relatively limited.

The limited adoption of P3P by the marketplace to date is attributable to the still evolving nature of the private sector standards process, the need to respect the fact that a diversity of business models operate globally on the Internet and the traditional pace of technologies that are heavily influenced by network effects. At this time, the only browser that is P3P compliant is Internet Explorer 6 by Microsoft. Consumers with P3P client tools will find that for now, relatively few sites have implemented P3P privacy policies. If a user limits his or her preferences to only visit P3P-enabled sites, he or she may find that their online browsing options are limited. At the same time, companies considering P3P may determine that because of the lack of widespread P3P client tools the investment in retooling their own Web sites and privacy practices may not be justified at this time.

Network effects in the technology market are well-documented and well-understood. Inevitably, it will take some time before P3P usage becomes widespread. At the same time, given the support of P3P by a key Internet standards body (W3C) and the broad support and interest in P3P in technology, privacy and consumer communities, many believe that P3P will achieve critical mass in the near future.

A listing of participating sites can be found at www.w3.org/P3P/compliant_sites.

Privacy networks

Privacy networks, like anonymizers and proxy servers, prevent a Web site from seeing the identity of the Web site visitor. However, many of these services have added features that distinguish them from relatively simple anonymizers.

Privacy networks generally rely on the use of pseudonyms or alternative identities. A user generally has an account with the service provider that contains his or her true identity. The service provides the user with a pseudonym that may or may not include accurate demographic information. The user then uses the subscriber network to host its home page, Internet service provider or Web surfing starting point for any Internet session. The privacy network reveals only the pseudonym identity to any Web site that the user visits.

Typically, privacy networks provide users with significant choice about what information is revealed about them. Some users may choose to include, for example, basic demographic information, allowing Web sites that they visit to know their age, gender or geographic location; other users may choose to block this information from being shared.

A privacy network will typically store cookies served to the user on the privacy network, preventing the delivery of cookies to the individual's computer. The privacy network thus enables users to utilise customisation, personalised services and other convenience benefits without having to have such information stored on their personal computer hardware.

Privacy networks may be Internet-based services, where the individual user subscribes to the service and accesses the services through his or her own Internet service provider. Alternatively, some privacy networks are making their technologies available to large corporate customers, including privacy corporations that wish to limit the disclosure of private information about their employees to third parties, or to Internet service providers who wish to incorporate such services into their own offerings.

For many users, privacy networks offer significant promise because they allow an individual to reap the benefits of personalization and customised services without compromising personal privacy.

Consumers inherently understand that companies need data about their markets and appreciate corporate interest in using that data to improve and enhance their products and services. The ability to create an alternative identity that reflects an individual's choices, preferences and demographic information without having to disclose more personal details to an online site – such as home address or phone number – is an attractive solution for many. Many see privacy networks as an effective tool in balancing these competing interests.

In the corporate market, many network and Internet service providers consider the use of privacy network technologies as a benefit that they can provide to their individual consumers. For many, implementing such tools is considered as a competitive advantage that will enhance their own offerings. While integrating these technologies into a corporate or ISP network is technically complex and generally requires a significant investment, many companies believe the investment to be a cost-effective approach to addressing consumer concerns and helping their consumers make informed choices about privacy and data protection.

Information brokers

Information brokers – often referred to as infomediaries, account aggregators or other terms – are companies that act as a broker for personal information. Because this market segment is evolving, there are several different approaches encompassed within the concept of an information broker or infomediary. This description attempts to provide a broad overview of the various approaches.

The information broker or infomediary approach has been both sharply criticised and widely praised as a viable alternative for individuals seeking to protect their own privacy. This paper does not make a value judgement on the business models of these companies. In light of the fact that some industry observers view this approach as a positive addition to the protection of personal data, it is noted that these tools do meet the basic definition of a PET in that these services attempt to ensure that consumers have greater control over the disclosure of their personal information.

Brokers or infomediaries are typically subscription-based or fee-based services. An individual creates an account with the company, which then tracks through software an individual's online actions, including surfing habits, purchasing history and other data. The services serve as the primary repository of this information.

The individual, however, remains in control of the information, and may direct the company to share information with a particular site and deny information sharing with another. The broker acts on behalf of the individual, not the vendor, and can provide significant consumer benefits and conveniences because of the wealth of information collected. In addition, these companies are significant sources of demographic data for corporate marketers who may be interested in analysing non-personal information about a particular market segment. Through data analysis, the company can provide demographic information without having to disclose PD of individual clients.

If an individual determines that he or she no longer wishes to have the company act as a broker on his or her behalf, the user can cancel the service or subscription. Once the service is cancelled, the information is generally removed from the company's database.

Intelligent agents or software "bots," applications that can act on behalf of a consumer based on his or her expressed preferences, are similar, but not covered in detail in this paper.

Some privacy advocates argue that while the broker concept may empower users, significant risks remain because these companies are largely unregulated (except to the extent that they collect sensitive or legally regulated information) and that consumers must rely on the stated policies of a private company for

reassurance that their data will be protected. Those that believe they offer a viable alternative for consumers note that the business model of a broker is entirely dependent on the company creating a trusting relationship with individual consumers. The market, they argue, will ultimately ensure that these companies do not violate the privacy of their customers. The powerful forces of a competitive market create a strong incentive for these companies to rigorously respect the preferences of the individuals they represent.

This remains a relatively small market at this time, and it is unclear whether consumers that are unwilling to trust a company with a posted privacy policy will be any more willing to allow the broker to collect their personal data.

Network-based technologies

Many privacy-enhancing technologies can be deployed on corporate networks, private LANs or WANs. These technologies allow corporate or large-scale network managers to limit the information disclosed from individuals on a given network.

Proxies and firewalls

Proxy servers and firewalls are technologies that typically are located between the individual consumer and the Internet. In a corporate environment, they may be located on the local area network (LAN) at the point where the LAN is connected to the Internet, at the ISP, or somewhere in between. Proxies and firewalls can also greatly enhance security in a network environment.

Firewalls and proxies are quite similar in terms of their functionality, though firewalls typically include additional security features not found in proxy servers.[14] Generally, however, both can prevent the disclosure of an individual's IP address or other personal information by acting as an intermediary between a Web site and an individual computer.

The key difference between firewalls and proxy servers is how they deliver information to an individual browser. Information requested through a firewall – whether it be a Web page or streaming video – is delivered directly back to the individual user. The firewall may scan for viruses, restrict certain types of content or implement additional security features, but the information is sent back to the individual computer that initially requested the data.

In a proxy environment, the proxy server acts on behalf of the individual user and hides the identity of the client computer from the Web site. When an individual requests a given Web page – www.oecd.org, for example – he or she is actually passing the request to the proxy, which in turns makes the request to the actual OECD Web server. The OECD Web server, in this example, would deliver the page and information back to the proxy, which in turn delivers the page to the individual user.

These technologies are widely deployed on corporate networks. They are readily available, often bundled with network, Web site and other Internet products and services. Firewalls for individual PCs are also widely available on the retail computer software market. Because these products were originally developed for security purposes, their functionality and flexibility are often not as robust as other products developed specifically to address privacy issues. However, their widespread usage and deployment ensure that they will remain at a minimum a crucial element of any privacy-enhancing technology solution.

Proxies and firewalls are widely available from computer security firms, and are often bundled with network or Web software.

Privacy networks

Privacy networks are described in detail above. Of note, however, is the fact that many privacy network companies are working with Internet service providers, corporations and popular Web sites to incorporate privacy network technologies to provide these types of services to their own employees, customers or subscribers. Privacy networks, then, need not only be Internet-based services for individual consumers, but may be integrated into the closed networks of various organisations or businesses.

In addition, many companies that offer online services are providing new capabilities for their consumers that provide additional control over personal data. Microsoft's Passport services and AOL's Magic Carpet – both of which give consumers new options in how each service uses their PD – greatly simplify the online experience by remembering consumer preferences, eliminating the need to re-enter repetitive information and increasing the opportunities to provide the consumer with a friendly, familiar and seamless online experience. While some concerns have been raised about the comprehensive nature of these services – Passport, for example, is being widely deployed on both Microsoft and non-Microsoft owned Web sites – the convenience afforded to an individual user at all of his or her favourite sites is compelling for many users. But as with any online service, the user should carefully check, review and evaluate the options available to him or her in the service's respective privacy policy to ensure that he or she is comfortable with the uses, choices and options available to him or her.

III. Recommendations

The 1998 OECD Ministerial Declaration established that PETs can play a crucial role in giving users greater and more flexible control over personal information. The OECD has consistently recognised since then the importance of PETs in numerous declarations, papers and conference documents, as outlined throughout this paper. In encouraging the use of PETs, both governments and the private sector have important roles to play.

The use of PETs in implementing national law

Policy makers have long questioned whether PETs can play a role in implementing data protection laws and if so, to what extent technology can address the issues raised in such regulation. To some extent, the answer to this important question is yes, PETs can serve an important purpose. However, it is important to realise that PETs cannot alone address the requirements of data protection laws.

PETs can significantly empower consumers concerned about data collection. Privacy is an inherently personal issue, and each individual consumer may have very different privacy preferences. And while national laws may establish baseline data protection rules, consumers will inevitably have unique preferences about data that may or may not be collected about them. Here, PETs can serve as an important complement to national data protection laws for those consumers with specific concerns or who prefer more privacy than the general law allows.

At the same time, however, PETs cannot implement every national data protection law or even broad international guidelines. There are simply too many differences in national laws, exceptions in certain circumstances, nuances or differing treatment for disparate types of data for any single technology (or even combination of different technologies) to address the myriad of rules and regulations that inevitably accompany data protection laws. Generally, software applications and technologies address very singular and/or specific concerns, while data protection laws cover a wide variety of PD in a wide variety of circumstances. As a result, PETs are ill-suited to be utilised to implement what are often very broad, comprehensive national laws.

However, PETs can play some role. CEN (Committee for European Standardization) has undertaken a comprehensive review of whether technology standards can be used to implement the EU Data Directive. As work here continues, there may be the opportunity to use PETs to support the implementation of the EU Data Directive (though it may not address US or other national laws), and may encourage the development of other standards to address different regulatory initiatives.

PETs should be seen, then, by both governments and consumers, as a secondary tool for privacy protection. Consumer engagement – namely checking privacy policies and establishing one's own privacy preferences – are crucial elements without which PETs are largely ineffective. In addition to national law (where consumer and governments determine such an approach is appropriate) and proactive consumers, PETs can be beneficial.

In addition, there are constructive ways that governments can support the development and use of PETs, including:

- Ensuring consumers that users of PETs are not discriminated against in criminal or civil investigations. There is a natural tendency to believe that a consumer who uses robust encryption or anonymizing technologies, for example, on his or her computer must be "hiding something." Data protection laws should recognise that consumers who opt to use such tools may simply be protecting the accidental disclosure of their personal information and not hiding activities of concern. While this may create difficulties for law enforcement or investigating personnel, the ability of individuals to use PETs should be protected.

- Recognise the important role that PETs can play in assisting individual consumers to implement their personal privacy choices in any data protection or privacy related legislation. Such efforts will help raise awareness about the availability of PETs for consumers who may not be aware of their existence.

- Data protection policies should look favourably on Web sites that utilise or make available PETs to their consumers. Whether a site provides robust choices for a consumer or incorporates privacy tools into its own infrastructure, companies that take these additional steps to help empower consumers should be given favourable consideration in consumer complaints or other similar situations.

- Web sites should not be allowed to discriminate against consumers who deploy PETs, except in cases where the PET prohibits the site from meeting consumer requests. For example, a site should not refuse to display for a consumer simply because he or she chooses not to accept cookies. However, the site should be free to deploy whatever technologies or tools it chooses to be most appropriate. For example, just as a hotel that requires a credit card or other deposit for advance reservations should not be required to hold a room for a consumer who refuses to provide such information, a Web site should not be required to provide customised information or facilitate online purchases in the same situation if cookies are the technology deployed by the site and the user chooses not to accept cookies except where the use of cookies provides functions beyond personalization or marketing – such as maintenance of a shopping cart or enhanced security.

Private sector initiatives

The private sector has also long recognised the important role that PETs can play. The wide variety of PETs available demonstrates that companies are responding to consumers seeking such empowering tools. Companies using the Internet understand that privacy concerns pose a barrier to the future growth of electronic commerce. As the private sector seeks to address consumer's concerns and eliminate barriers to

future growth, a wide variety of robust PETs for individual, Internet and network use are increasingly being deployed to enable consumers to make informed choices about the collection and use of personal information.

The private sector can evaluate the feasibility of more widespread use of PETs to support the objectives of policy makers interested in exploring the viability of PETs to protect personal privacy. In particular:

- Businesses should evaluate whether incorporating PETs into their corporate networks will help protect the privacy of their users (*i.e.* providing privacy to corporate users). Similarly, Internet service providers should consider whether making PETs available will help alleviate many of the privacy concerns expressed by subscribers.

- Consumer and business organisations should work, in conjunction with governments and public sector organisations, to educate consumers about the availability and use of PETs.

- e-Commerce and other online sites that collect personal information should evaluate whether integrating PETs such as P3P into their own sites is feasible and useful to their consumers.

- Technology companies should consider how privacy-enhancing technologies can be better incorporated into standard online tools, such as browsers, FTP clients and other access-oriented software, hardware and handheld devices.

Conclusion

The private sector and policy makers have long recognised the importance of PETs in aiding consumers in making informed choices about privacy. The OECD has reaffirmed this in several declarations, conference papers and studies in recent years. The consistent recognition of the role of PETs by policy makers has encouraged both consumers and companies to focus attention on PETs and their continued development.

As the market continues to develop a wide variety of robust tools, consumers must be made aware of the utility of PETs. Industry, private sector organisation and governments can help consumers learn about PETs, understand their role in aiding individuals in protecting personal information, and encourage their use. Such efforts can only serve to enhance consumer confidence and support the continued growth of electronic commerce and ensure that the attendant benefits are widely shared among all online users.

NOTES

1. According to the UK-based research firm Arc Group, www.the-arc-group.com, the fixed wireless market will expand rapidly beyond Europe and the United States over the next few years. By 2005, Europe will account for USD 11 billion of the market, the United States for USD 9 billion, and the rest of the world for USD 22 billion.

2. However, it should be noted that at least some consumers believe that they have more control today over their personal information than they might have had in the past. The 1999-2000 Annual Report from the Canadian Privacy Commissioner's Office found that "In general, Canadians appear to be less concerned about privacy than they were in the 1992 study. By 1999, 47% of Canadians agreed with the statement, 'I feel that I have less personal privacy in my daily life than I did ten years ago,' compared with 60% in 1992. The number of Canadians who agreed with the statement, 'There is no real privacy because government can learn anything it wants about you,' dropped to 63% from 81%. The number of Canadians who agreed with a similar statement about business dropped to 57% from 71%. The 1999 study suggests that Canadians are also becoming more sophisticated in their attitudes towards privacy. Fifty per cent said that they now 'feel confident that they have enough information to know how new technology might affect their personal privacy', up from 43% in 1992. A majority of Canadians (54%) don't mind companies using personal information as long as they know about it and can stop it. Canadians may be willing to provide personal information in certain circumstances, and may even be willing to sacrifice some of their privacy, but they want to know what they are getting in return. One thing they want is control." Available at www.privcom.gc.ca/information/ar/02_04_08_e.asp.

3. This is commonly referred to as "clickstream" data.

4. Generally, the cookie contains the session ID. The session ID is a identifier created by the server that identifies the session. In some cases, the use of a cookie may protect privacy. Consider a situation where a user logs into an online account. A cookie set with a "time out" after a pre-set period of time helps prevent the accidental disclosure of data if the user forgets to log out of a site or is using a shared computer.

5. Internet "RFCs" are technical protocols and standards drafted and written by the Internet Engineering Task Force, the IETF. RFC stands for Request for Comment.

6. This functionality is determined by the Web browser settings, which limits which Web sites can read cookie information based on these common, standard implementation practices.

7. HTML stands for the HyperText MarkUp Language. HTML is the standard language used to develop Web pages.

8. Cookie blockers are one form of PETs that give users greater control over the placement of cookies on a user's PC. They are described in greater detail in the section on PETs below.

9. FTP stands for File Transfer Protocol. FTP was one of the early services available on the Internet, used for sharing files among computers across public networks. Plug-ins are applications that support additional Web services, such as sound or video.

10. The concept of a "technology community" is a broad one and has no generally accepted definition. However, for the purposes of this paper, the term refers to software developers, information technology professionals, and others involved in the creation, implementation and deployment of technology solutions.

11. Data in cookies is typically coded, encrypted or stored in a format that is not easily recognisable to the user. Some have asked why information stored in cookies is not readily decipherable. The reasons are numerous. First, such data is generally coded in a way to minimise the amount of data that is stored in a cookie, minimising data transfers and speeding the user experience on what are often relatively slow data connections. Second, data that is coded is not accessible to other Web sites, and helps protect to some extent the operational nature of a given site from competitive sites. Third, coded data is less likely to be stolen or intercepted by a third party who, like the user, would be unlikely to understand the encoded data.

A cookie that includes "USER=8023" is far less likely to identify an individual than "USER=JaneSmith". In this way, the coded data actually may enhance privacy in those situations where personal data may be stored in a cookie as it creates a disincentive for a third party to try and collect data stored on a user's computer. Finally, coded data may prevent a user from altering the settings stored in a cookie, ensuring that its intended use – such as storing account login information or personalization preferences – is not accidentally lost.

12. The longer the bit length of the key, the stronger the encryption. Most security experts agree that at a minimum, 128-bit encryption is necessary to protect data. Commercial encryption routinely uses stronger key lengths, and personal encryption tools with 1024-bit length keys are available.

13. XML, or Extensible Markup Language, is a standard defined by the W3C that provides context to Web site data. HTML, HyperText Markup Language is the language used for creating Web pages, but is relatively primitive in that it can only control how information is displayed. XML can define what data means in the context of the Web page or how it relates to other data, greatly increasing the functionality of a given Web page and its data interoperability with other sites, databases and online applications.

14. Firewalls, for example, may incorporate the ability to disable certain services such as FTP, close specific ports, or provide advanced intrusion-detection technologies.

REFERENCES

National Consumers League (2000), "Online Americans More Concerned about Privacy than Health Care, Crime, and Taxes, New Survey Reveals", 4 October, www.nclnet.org/pressessentials.htm.

Chapter 13

PRIVACY-ENHANCING TECHNOLOGIES: REPORT ON THE OECD FORUM SESSION

This chapter summarises an OECD Forum Session on Privacy-Enhancing Technologies (PETs) held on 8 October 2001. The objective of the forum was to demonstrate a number of PETs, so delegates could experience using them first-hand, and to facilitate discussion on: *(i)* the policy implications of PETs and the future of PETs in the wider context of online privacy protection; and *(ii)* the challenges of, and methods for educating business about the importance of privacy by design and the use of PETs and educating individuals about the benefits and limitations of PETs. The summary of the meeting is preceded by the orientation document which provided forum participants with background information to assist in their preparation for the meeting. This document also includes two studies:

- A synthesis of a survey of PETs available on the Web, and a table of the surveyed technologies. This study was provided to participants in advance of the meeting to help them gain a better sense of what types of products are available on the market and what their impact could be on safeguarding users' privacy online.

- A research paper by Perri 6 which discusses the question of when, for whom, and under what circumstances, "communication" about PETs might work, in the sense of encouraging businesses to supply such tools, and individuals to use them.

Chapter 13

PRIVACY-ENHANCING TECHNOLOGIES: REPORT ON THE OECD FORUM SESSION

Main points

The Forum was successful in providing participants with a more practical level of understanding of Privacy-Enhancing Technologies (PETs), their functionalities, and the extent to which they can help protect privacy. In this respect, the presentation of the survey of 135 Web sites offering PETs gave a clearer picture of what PETs are available today. The Forum also provided an opportunity to generate discussion and establish common understanding on the range of emergent policy issues surrounding the use of these technologies, including those related to education. The main points that emerged from the Forum are highlighted below.

PETs have the potential to help protect privacy online within the framework of either legal regulation or industry-led self-regulation.

PETs are technological tools that offer a range of functionalities. They can filter "cookies" and other tracking technologies; allow for "anonymous" Web-browsing and e-mail; provide protection by encrypting data or allow for the advanced, automated management of users' individual data on their behalf. Most of the PETs available today are designed to be used by consumers, fewer are designed to be used by organisations, and even fewer are designed to be used simultaneously by both individual users and business.

PETs can be employed to determine, for example, if a site was in violation of a particular privacy principle (thereby reinforcing transparency/notice) or to block a site from taking a particular action without the user's consent (thereby reinforcing choice). Therefore, in either a self-regulatory environment or one in which there are laws governing privacy, PETs have the potential to ensure that at least some of the fundamental privacy principles that form the standards of privacy practices in either setting are in place.

PETs have benefits and limits: they are part of a wider package of solutions for privacy protection online.

As measured against the OECD Privacy Principles, most of the current PETs designed for individual users provide for collection limitation/choice (45%), collection avoidance (40%), and security (27%). However, none of the PETs available provides total privacy protection in line with the OECD Guidelines: more than half surveyed implement only one principle, and only one tool implements as many as five principles.

PETs designed for businesses can automatically monitor and analyse their information collection, use and potential sharing practices. In this way, PETs can help businesses to secure and maintain compliance with their privacy policy. However, to be most helpful to businesses, PETs should be part of a privacy risk management programme.

PETs are therefore necessarily part of the wider package of privacy protection online that includes regulation and self-regulation and other initiatives such as the development and notification of privacy policies, the use of contractual solutions and also the increasing availability of online redress mechanisms as a further option for recourse.

Increasing transparency and wider usability of PETs may strengthen user and consumer confidence.

Current statistics still indicate that users and consumers are uneasy when engaging in e-commerce transactions or other activities online that require the entering of personal data. PETs offer a partial solution to this issue, but individual users must also have strong confidence in the ability of PETs to safeguard their privacy if these technologies are to participate in enhancing trust.

One limit of some PETs is that they do not provide extensive information on the organisation behind the technology or other identifying features. Another limit of some PETs is that they are technical and sometimes not simple enough to be used by average consumers. Therefore, to be more effective and more widely used, and to participate in building trust online, PETs need to be more transparent and to offer wider usability.

Educating business and individual users — the first stepping stone.

There is an important need for raising awareness about the existence of PETs and facilitating the education of both business and individual users about their benefits/limits and their complementary role in the framework of privacy protection. A broad spectrum of education strategies will be required to tailor these efforts to different target groups in order to effectively promote their use for a maximum benefit.

For business, enterprises need to be reminded of the importance of managing privacy/security risks and given incentives to balance cost so privacy protection starts with business and the burden does not rest as heavily with the consumer. Business may be encouraged through targeted education strategies to recognise the importance of privacy protection in enhancing client trust and developing mutually profitable relationships, and thereby have the necessary incentives to better provide notice to consumers of business privacy practices, and maintain privacy during online interactions and transactions. Businesses also need to be reminded of the importance of building in privacy technologies when designing new products.

For individual users, there is a clear need for more and better education to further encourage them to take advantage of PETs when exploring the Web, sending and receiving email, or engaging in other online activities. Given the technical nature of these products, a particular challenge is explaining these technologies in simple language given their complexity relative to the general level of understanding in the community. However, users and consumers will only have trust in technologies if they understand how they operate, how they are implemented and their benefits and limits in addressing privacy needs.

I. Presentation of the forum: orientation document and agenda overview

Introduction

In the 1998 Ministerial Declaration on the Protection of Privacy on Global Networks, issued in Ottawa, the governments of OECD member countries delivered a wide-ranging commitment to ensure that the 1980 OECD Privacy Guidelines "are effectively implemented in relation to global networks" (OECD, 1980). In particular, they focused on five steps. One of them included encouraging the use of privacy-enhancing technologies.

In the three years since the Ottawa Conference and the Ministerial Declaration, the Working Party on Information Security and Privacy (WPISP) has focused on the implementation of other elements of this five-step programme, including work on contractual solutions, alternative dispute resolution (ADR), the launch of the OECD Privacy Policy Statement Generator (to encourage the adoption of privacy policies and their notification to users), and other efforts to educate users, businesses and governments about online privacy. Over the same time period, there have been significant advances in the development and use of privacy-enhancing technologies (or PETs) as a means of promoting online privacy. Many policy makers

see great promise in the ability of PETs to help implement privacy principles, such as those contained in the OECD Privacy Guidelines, within the framework of either industry-led self-regulation or legal regulation.

At the February 2001 meeting of the WPISP, Delegates heard presentations on a US government workshop on PETs[1] from Wendy Lader of the Department of Commerce and on an inventory of PETs prepared for the WPISP by Lauren Hall of the Software and Information Industry Association, who also was serving as a consultant to the OECD secretariat on PETs.[2] The Working Party discussed PETs and decided to address the policy issues associated with these new technologies in greater detail. Delegates agreed that there is a need for raising public awareness about the existence of PETs and facilitating education about their use and agreed that the use of PETs can complement privacy policies by, for example, empowering users to match their privacy preferences with business privacy practices.

Agreement also was reached at the meeting to hold a special Forum session to focus on PETs in which a number of technologies would be demonstrated. Delegates of the OECD Committee on Consumer Policy (CCP) and consumer representatives would also be invited to attend. Forum participants would experience using PETs and discussion would take place on:

- The policy implications of PETs and the future of both PETs and online privacy protection in general.
- The challenges of, and methods for, educating business about the importance of privacy by design and the use of PETs; and
- The challenges of, and methods for, educating individuals about the benefits and limitations of PETs.

The following overview of policy issues related to PETs was intended to provide information and "food for thought" to Delegates prior to the Forum Session. For a more comprehensive discussion of particular PETs themselves and how the technologies function, Forum participants were encouraged to refer to the materials referenced in the section below entitled "Further background material".

Overview of privacy-enhancing technologies

Various definitions have been written for privacy-enhancing technologies and their aims:

- Lauren Hall, in her inventory, states their purpose as giving "the individual user or technology manager the capability of controlling if, how much or under what circumstances" information is disclosed and/or processed.[3]
- The European Commission's Article 29 Data Protection Working Party notes that the concept of PETs "refers to a variety of technologies that safeguard personal privacy, notably by minimising or eliminating the collection or further processing of identifiable data" (EU, 2000).
- Herbert Burkert from the German Institute for Media Communication says the term "refers to technical and organisational concepts that aim at protecting identity" (Burkert, 1997).[4]
- The Ontario Information and Privacy Commissioner and *Registratiekamer* of the Netherlands focuses on the role of PETs as being an "identity protector" in their joint study (Ontario Information and Privacy Commissioner and *Registratiekamer*, 1995).

In other words, PETs are technological tools that assist in safeguarding the privacy of users and consumers. They most often are viewed in the policy context as operating as part of a wider package of privacy initiatives. Given their broad purpose, it is not surprising that PETs, as currently available or envisioned, take on a range of characteristics. Some filter "cookies" and other tracking technologies; some

allow for "anonymous" Web-browsing and e-mail; some provide protection by encrypting data; some focus on allowing privacy and security in e-commerce purchases; some allow for the advanced, automated management of users' individual data on their behalf.

Indeed, the list could be far longer. Accompanying the rapid rise in Internet use and e-commerce sales has been a similar explosion in the privacy and security technologies known as PETs. This "privacy space" of the economy is now a competitive arena, with many companies hoping to attract the interest of users, businesses, and governments. The influx of privacy and security companies comes as surveys continue to demonstrate that users are uneasy about their privacy when venturing online and, especially, when engaging in online purchases where personal information is often revealed.[5] There are also indications that individuals want more information about the privacy practices of the businesses and organisations with which they transact.[6]

Benefits of PETs

Advocates of the development of PETs come from industry, privacy organisations and many government agencies in OECD countries. In offering their support, these advocates often point to two strong benefits that PETs offer international policy makers: *(i)* the technologies can be employed to help achieve some of the internationally recognised privacy principles; and *(ii)* they can be employed in countries that have chosen either a self-regulatory or legal approach to privacy.

Table 13.1. **PETs and privacy principles**

Examples of common types of PETs	Examples of some principal policy effects *(based on the OECD Privacy Guidelines)*
Anonymity/pseudonymity tools	Collection limitation (or avoidance)
Personal data management tools (such as information brokers and infomediaries)	Collection limitation; security
Notice/choice tools (such as the Platform for Privacy Preferences)	Openness/notice; collection limitation/consent and choice
Marketing/advertising control tools (such as cookie and spyware filters and marketing consent management tools)	Collection limitation; choice and/or consent; security
Security tools	Security
E-commerce privacy/security tools	Collection limitation; Security
Access control tools	Notice, security, use limitation, access by data subjects
Children's privacy tools	Collection limitation/consent
Privacy auditing/compliance tools	Accountability

Source: OECD.

Advocates of PETs note that the technologies can function in either a self-regulatory environment or one in which there are laws governing privacy. In either case, PETs can help to ensure that at least some of the fundamental privacy principles that form the standards of privacy practices in either setting are in place. PETs users could employ them to determine, for example, if a site was in violation of a particular privacy principle (thereby reinforcing transparency/notice) or could block a site from taking a particular action without the consent of the user (thereby reinforcing choice).

Concerns and limitations

But it is clear that not all PETs receive unanimous endorsement by all stakeholders in the international privacy community. Some technologies have been criticised by some privacy advocates as too weak, or even as deceptive tools to erode privacy instead of enhancing it, or as distractions getting in the way of potential regulation of privacy. P3P, very popular in industry and supported by many privacy groups, has come under fire from some privacy advocates. Consumers International, for instance, said in its 2001 Privacy@net study that some technologies, including P3P, "are designed more to facilitate data sharing than to protect users."[7]

Defenders of PETs would object to many of the charges. For example, the Independent Centre for Privacy Protection of Schleswig-Holstein in Germany issued a strong endorsement of P3P, noting its ability to give users "increased control of what happens to their personal data."[8] However, most defenders of PETs (including the Independent Centre for Privacy Protection) agree that they would not today label PETs as the complete solution for online privacy concerns.

A few examples of the limitations of PETs show why: First, many PETs help protect individuals' privacy when online or help provide notice and consent to users, but cannot guarantee the privacy of information once it is given to an organisation or business. One important concern, therefore, stems from the need to ensure that collected information is treated in accordance with the privacy principles (such as the Use Limitation Principle of the OECD Privacy Guidelines). At the same time, on the other side of the debate, the potential for the complete avoidance of data collection through anonymity tools also raises concerns about a lack of accountability in cyberspace and may worry law enforcement authorities.

Debates also continue over the proper "default" settings for PETs. With the assumption that many (if not most) consumers will not alter or customise pre-set product settings, the default setting gains significance, especially in a discussion of privacy. If a user makes no changes to settings on such products as cookie filters, for example, how many cookies are blocked, what types of cookies are blocked, and what type of information is given to the user about the cookies that are served to his or her computer would all depend on the default position of the filter. Therefore, concerns are raised that some technologies have default settings that are not privacy-protective enough to count as truly enhancing the privacy of their users. (Conversely, some may also argue that user performance in such activities as surfing the Web would be unduly burdened if the default settings were made too privacy protective, such as by blocking all types of cookies.)

In addition, there are practical concerns about PETs. These concerns include whether the technologies are simple enough to be used by average consumers and whether average consumers are willing to purchase, install and operate PETs as client-side tools on their computers. There are also related questions regarding whether a critical mass of PETs users will grow so as to force changes in privacy practices by Web-site operators, or whether PETs users will be the ones forced to sacrifice performance on the Web for privacy protection. On the business side, firms also might well be concerned about the complexity of integrating privacy tools into their operations and/or products.

Role as a tool

Even given these limitations and concerns, the benefits of PETs ensure that the technologies will be part of the policy mixture that addresses online privacy in the future — as recognised in the 1998 Ministerial Declaration. However, it is important to note that PETs are simply tools, to be used by individual users, businesses or governments. Whether they are implemented in ways that are positive or negative, constructive or obstructive, depends to a great extent on the decisions of those who employ them, not on the tools themselves. (As Burkert writes, "We should not forget that PETs . . . essentially remain

technical: They *follow* the normative decision", Burkert, 1997.) At the same time, it is also important to note that there is a multitude of technologies available under the PETs label. Not all PETs may be as good or as privacy-protective as one would want, and not all may be as bad or as privacy-invasive as one might fear. Not all PETs may spark public-policy arguments against their use, and not all may lead to arguments in their favour.

Need for education

Given that PETs are tools, with both significant benefits and limitations for users and businesses, the need for education becomes clear. Sociology Professor Gary Marx makes this case with regard to the privacy implications of information technology in general, noting: "It is . . . important that the technology be demystified and that citizens not attribute to it powers that it doesn't have. There is a chilling danger in the 'myth of surveillance' when the power of information technology is oversold. On the other hand, when technologies are revealed to be less powerful than authorities claim, legitimacy declines. ... The potentials and limits of technology must be understood." (Marx, 1990).

In terms of demystifying PETs and promoting their use for a maximum benefit, there are at least three target audiences for education. First, individual users might want to take advantage of these technologies on a personal basis when exploring the Web, sending and receiving e-mail, or engaging in other online activities. Second, businesses might be encouraged to use technologies that could, for example, help maintain privacy during online sales, better provide notice to consumers of their business privacy practices, and/or improve the access control mechanisms surrounding a business' databases. Third, businesses might be encouraged to build in privacy technologies when designing new products.

As a result, a spectrum of education efforts would be needed to raise awareness of PETs in all target audiences. All would likely need to include attempts to raise awareness and to ensure that there is an understanding of what privacy solutions PETs can provide, as well as an understanding of their limitations in fully addressing all privacy needs.

According to a recent survey by Harris Interactive for the Privacy Leadership Initiative, few Internet users are currently taking advantage of PETs.[9] Just 15% report having put software on their computer to shield their personal information, while only 10% have used software that allows them to surf online anonymously and 5% have used software designed to allow anonymous purchases. (The numbers are somewhat higher for heavy online users and lower for light users.)

Further background material

Recent workshops and reports

- US Department of Commerce Workshop (September 2000): www.ntia.doc.gov/ntiahome/privacy/.
- EC Joint Research Centre Workshop (May 2000).
- EU Article 29 Data Protection Working Party Working Document, "Privacy on the Internet: An Integrated EU Approach to Online Data Protection" (November 2000) includes discussion of PETs: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2000/wp37en.pdf.

Overview of PETs

- Overview of privacy tools by Lorrie Faith Cranor of AT&T Labs (September 2000): www.research.att.com/
- "The Reinvention of Privacy" by Toby Lester in *The Atlantic Monthly* (March 2001): www.theatlantic.com/issues/2001/03/lester-p1.htm
- "Networking Health: Prescriptions for the Internet" by the National Research Council (2000) includes analysis of PETs in relation to health issues (pages 167-174, in particular).

P3P (with some mention of other PETs)

- Assorted papers discussing P3P technology: www.w3.org/P3P/.
- Analysis of P3P by the Center for Democracy and Technology and the Ontario Information and Privacy Commissioner (March 2000): www.cdt.org/ privacy/pet/p3pprivacy.shtml.
- "Pretty Poor Privacy" report by the Electronic Privacy Information Center and Junkbusters (June 2000): www.epic.org/Reports/prettypoorprivacy.html.

Advocacy group guides to PETs

- Center for Democracy and Technology: www.cdt.org/privacy/pet/.
- Electronic Privacy Information Center: www.epic.org/privacy/tools.html.

Recent international Internet privacy study

- Consumers International, "Privacy@net: An International Comparative Study of Consumer Privacy on the Internet", containing an appendix with a discussion of PETs (January 2001): www.consumersinternational.org/document_store/Doc30.pdf.

Forum session agenda overview

WELCOME AND INTRODUCTION

Welcome and introductory remarks, *WPISP Chair and secretariat*

MORNING SESSION: OVERVIEW OF THE TECHNOLOGY

PETs products: overview demonstrations

Overview presentation of PETs available on the Web, *Laurent Bernat, Director, Projetweb; Consultant*

Demonstration of PETs products designed for individual users:
Policy effect of collection limitation/avoidance

Laurent Bernat, Director, Projetweb; Consultant
@nonymouse (@nonymouse.com) — (anonymity/pseudonymity tool)
The Cloak (the-cloak.com) — (anonymity/pseudonymity tool)
Privacy Companion (idcide.com) — (cookie filter)
Netscape 6.1 (AOL-Netscape) — (cookie filter and password manager)

Demonstration of a PETs product designed for both individual users and businesses:
Policy effect of openness/notice, collection limitation/consent, choice

P3P (World Wide Web Consortium) — (server side)
Helena Lindskog, System Manager, Ericcson Infotech
Internet Explorer 6 (Microsoft) — (client side)
Isabelle Valet-Harper, European Standards Manager, Microsoft Europe

Demonstration of a PETs product designed for businesses: Policy effect of accountability
WebCPO (w*atchfire.com)* - (privacy auditing/compliance tool)
Norman McConkey, Director, Watchfire Ltd.

Exploring the technology hands-on

During this agenda item, participants were invited to use those demonstrated PETs designed for individual users. They were invited to split into small groups on computers that were provided by the OECD. Assistance was provided by representatives of the organisations whose technologies would be used, and by the OECD. Questions, as well as discussion among participants, were encouraged.

General discussion, questions and answers

AFTERNOON SESSION: EDUCATING USERS/CONSUMERS AND BUSINESSES

Privacy risk perception and education about PETs
Perri 6, Director of the Policy Programme of the Institute for Applied Health and Social Policy
King's College London

Privacy-by-design
Stephanie Perrin, Chief Privacy Officer, Zeroknowledge

Educating consumers about PETs
Naja Felter, Policy Officer, E-Commerce and Trade, Consumers International

General discussion and concluding remarks
Concluding remarks and preview of WPISP policy discussion, *WPISP Chair and secretariat*

II. Report on the forum

Welcome and introduction

The Forum Session was opened by Peter Ford, Chair of the OECD Working Party on Information Security and Privacy (WPISP). Mr. Ford welcomed the participants to the Forum. He recalled that technology, and in particular PETs, were perceived in the 1998 OECD Ministerial Declaration as an important element of the policy mixture needed to ensure online privacy protection and have been examined thus far by the WPISP in this regard.

Introductory remarks were made by Anne Carblanc of the OECD secretariat. Ms. Carblanc gave a brief overview of each of the presentations to be provided and the running of the Forum. She then broadly described PETs as 'tools to assist in safeguarding privacy' and stressed that, in the policy context, they appear to be part of a necessary package of solutions aimed at securing effective online privacy protection for users. She then spoke of the wider objectives of the Forum and the WPISP's work on PETs generally — that is:

- On the one hand, to identify the benefits and limits of PETs and under what circumstances their development and use should be further supported at the policy level; and
- On the other hand, to examine how to best raise consumer and business awareness of PETs and their role in the broad spectrum of privacy protection, in order to foster the supply and demand of such tools in the interest of privacy protection online.

Session I: Overview of the technology

This Session focussed on allowing participants to gain a better practical-level understanding of PETs as they exist today. Overview demonstrations of selected representative technologies designed for use either by individual users or businesses were given. Participants were then invited to use, in small groups, those technologies designed for individual users, on computers that were provided by the OECD. Assistance was provided both by representatives of the organisations whose technologies were used and the OECD.

PETs products: overview demonstrations

Overview presentation of PETs available on the Web

Laurent Bernat, Director, Projetweb, provided an overview of a *Study of Privacy-Enhancing Technologies* (see Appendix I) which he undertook in the capacity of consultant to the OECD. Mr. Bernat explained that the aim of the study was to identify the PETs used on the Internet and to show their impact on privacy protection in light of the *OECD Guidelines for the Protection of Privacy and Transborder Dataflows of Personal Data*.

Mr. Bernat explained that over 130 sites were visited during the study and 83 sites selected for further analysis. He emphasised that the PETs analysed were selected according to their functionality and noted that the study was not exhaustive — it did not include examination of pure cryptography tools, tools for protecting children, deletion tools, tools designed to protect the PC network or anonymous security tools.

The results of the survey indicated that the PETs available today offer a range of functionalities with a number offering more than one functionality. Most of them are cookie filters (about half); anonymizers occupy 36%; and encryption, ad filters, and mail privacy are just under 20% each. Further, the study revealed that 80% of the PETs surveyed targeted individual users, 20% targeted organisations and 3% targeted both individual users and business.

As measured against the OECD Privacy Principles, the study showed that the PETs available today provide, in most cases, for collection limitation/choice (45%); collection avoidance (40%) and security (27%). Further, of the 83 sites examined, 58 PETs related to only one of the eight principles; 22 to two principles; two to three principles and only one to five principles.

A number of general conclusions and other observations were drawn from these results and summarised by Mr. Bernat as follows:

- From a technical standpoint, none of the tools identified uses a full range of functionalities that would make it possible to provide total privacy protection. Users must therefore combine several tools to optimise and ensure their level of privacy protection.
- 51% of the tools examined in the study must be installed on the user's computer which may be an obstacle to uptake and raise issues of compatibility.
- Some sites provide very little information on the organisation behind the PET product and other identifying features which may constitute a psychological barrier to uptake by users; and
- Many sites do make a serious effort to educate users. However, some of the sites focus more on commercial information rather than on technical educational information.

Mr. Bernat concluded that PETs can be of value in helping users to protect their privacy but are complementary to other tools or instruments. He emphasised that in order for users to have confidence in PETs, they need to understand the technology, the way it is implemented and to know who makes the technology available. He noted that consumer education will therefore be of paramount importance if

consumer confidence and ultimately use of these technologies is to increase. Finally, he mentioned that a number of areas for possible future analysis were also identified in the study.

Demonstration of PETs products designed for individual users

Mr. Bernat gave a live demonstration of a number of the technologies designed for individual users. These included two anonymizers — *@nonymouse* and *The Cloak,* and two cookie filters — *The Privacy Companion*, and *Netscape 6.1.* While doing so, he explained their basic functionality to participants.

- *@nonymouse* is an interface that permits users to anonymously navigate the Web, send e-mails, and participate in newsgroups.
- *The Cloak* serves as an interface for anonymous navigation of the Web. Furthermore, thanks to an optional encoding function (https), it offers users connected to the Internet through a local area network a higher degree of anonymity with respect to the administrator of that network.
- *The Privacy Companion* is a tool which is installed on individual users' desktops to filter cookies. It is effective and user-friendly. The Privacy Companion distinguishes between cookies from the site visited and cookies from third-party sites (tracking network).
- *Netscape Navigator 6.1* allows the user to select his/her default preferences concerning cookie management on a site by site basis. It also makes it possible to filter cookies from third-party sites.

Demonstration of PETs products designed for both individual users and businesses

Helena Lindskog provided a presentation on the Platform for Privacy Preferences (P3P) protocol developed by the World Wide Web Consortium, from the server-side perspective. Ms. Lindskog is a System Manager for Ericcson Infotech, a Lecturer of Karstad University and Ericsson representative in the W3C P3P Initiative Working Group.

Ms. Lindskog first discussed the general concept of 'privacy' and noted that privacy can be enhanced in a number of ways — through anonymity; pseudonymity; unlinkability; unobservability; user consent; or legislation.

Ms. Lindskog then described the P3P protocol. She explained that P3P, at its most basic, is a technology that translates a Web site's privacy policy into machine readable format so P3P enabled browsers, and other devices, can read the policy and compare it to the consumer's own privacy preferences. She also briefly presented the steps a service provider must follow in order to implement the P3P protocol. These include: *(i)* developing a written privacy policy (the P3P Guiding Principles document can be used to assist in this); *(ii)* deciding which policies apply to which parts of their Web site; *(iii)* selecting a generator; *(iv)* entering information into the P3P generator; *(v)* creating a policy reference file and storing it in a specific place; and *(vi)* using the P3P validator to check if any errors have been made.

In outlining the benefits and drawbacks of the protocol, Ms. Lindskog expressed the view that the protocol does what it is meant to do well — that is, it provides a way for users to consent/not consent to the use of their data by a Web site.

Isabelle Valet-Harper, European Standards Manager, Microsoft Europe, provided an overview of the operation of P3P from the client-side perspective through the use of Internet Explorer 6.

Ms. Valet-Harper first broadly described the privacy context and the place of P3P from the user's perspective. She noted that P3P enables users to have their user agents (*e.g.* browsers) act directly on their

behalf, or facilitate decision-making regarding their privacy preferences. She noted, however, that P3P is only part of the solution — it helps users to understand privacy policies but other aspects including seal programs and regulations; anonymity tools; encryption tools; laws and codes of practice also play an important role.

Ms. Valet-Harper then spoke in detail about Internet Explorer 6 and its implementation of P3P. She noted that Microsoft's goal for end-users in implementing the technology is to help the user communicate their privacy preferences in an unobtrusive way. She stressed that the focus had been on providing more information about cookies and user choices in relation to cookies, creating smarter automated behaviour and providing the ability to discriminate cookies according to purpose.

Ms. Valet-Harper then provided a demonstration of Internet Explorer 6. She explained that a status icon appears every time a cookie is restricted based on the user's privacy settings — that is when the site being visited uses cookies and the privacy policy of that site does not match the user's settings, cookies are restricted and the user is notified. A user can set his/her individual privacy settings on a 'privacy tab slider' (and elect one of six levels of protection — *i.e.* Accept all cookies; Low; Medium; Medium-high; High; Block all cookies) or he/she can allow the default settings to apply. When the icon appears, the user can also double click the icon to access a detailed privacy report.

Demonstration of a PETs product designed for businesses

Norman McConkey, Director, Watchfire Ltd, provided an overview of the operation of 'WebCPO' a privacy auditing tool for business developed by Watchfire Ltd.

In setting the context, Mr. McConkey noted that because the Internet information and commerce market is global and the Internet's characteristics have accelerated the trend toward increased information collection, use and sharing, organisations must now consider how the laws regulating business and issues arising from privacy breaches around the world will affect them. He further noted that issues relating to privacy on the Web are resulting in widespread market backlash for business such as lost revenue and business opportunities or brand and reputation erosion. All these factors combined emphasise that Web site privacy management is critical for businesses which must act to maintain their users' trust if they are to maximise the opportunities afforded by the Internet and have good profitable relationships with users.

Mr. McConkey then discussed the key Web privacy risks for business. He noted that Web sites capture a significant amount of sensitive or unnecessary personal information and that privacy leaks can occur through inadequate and un-enforced privacy statements; lack of adequate security protections at point of collecting sensitive personal information; use of cookies and 'invisible' Web bugs for tracking purposes or third party links and integrated third party content.

In order to secure and maintain compliance, Mr. McConkey spoke of the importance that business create and maintain a privacy risk management program as a first step. He then provided a demonstration of his company's software — 'WebCPO', which is a privacy management software for Web sites that automatically monitors and analyses all Web properties (Internet, intranet, and extranet) so organisations can understand their information collection, use, and potential sharing practices to help avoid privacy glitches. It is designed for large, multi-user environments and works by analysing a Web site and storing the results of this analysis in a central database — users can then query the database to automatically generate comprehensive reports that identify areas where there may be privacy problems. In addition, privacy officials and auditors are automatically notified when changes are made to high-risk areas of the Web site (such as unauthorised altering of a privacy statement). Mr. McConkey demonstrated the software live by using it to analyse a purpose built 'broken' Web site and showed how the various reports can be generated.

Mr. McConkey concluded by noting that most privacy rules are not intentionally broken but companies need to take compliance with these rules and compliance testing more seriously if consumers are to have confidence in e-commerce.

Exploring the technology hands-on

Participants were then invited to surf the Internet using the technologies designed for individual users on computers provided by the OECD at the meeting venue. OECD staff and presenters were on hand to provide assistance to participants and further explanation of the functionality of the technologies as they were tested live by participants.

General discussion, questions and answers

During general discussion the following arose:

- Mr. McConkey was asked whether Watchfire Ltd. uses a standard when conducting an audit of a Web site's privacy practices and whether the OECD Privacy Guidelines are used as the basis of this assessment. Mr McConkey noted that data protection issues, when they arise in any jurisdiction, usually fall into four categories and include those related to data collection, data sharing, data spillage and maintaining consistency between a company's intention (*i.e*. its privacy statement) and its action (*i.e.* what is being done in practice).He explained that the Webco program operates by conducting a search of a corporate Web site with a view to isolating whether and where these potential issues exist so that staff are able to make any necessary improvements to ensure compliance with relevant laws/principles/guidelines.
- There was detailed discussion/clarification on the P3P protocol and some confusion among participants as to whether it goes further than cookie management. H. Lindskog confirmed that cookie filtering is one aspect of P3P but that it is much more than this — it is a tool to assist users in having ready access to a Web site's privacy policy and to be able to easily compare it to their own privacy preferences. Ms Valet-Harper indicated that, in the context of Microsoft Internet Explorer 6, users are able to use the technology to distinguish between providing information or blocking cookies that communicate personally identifiable information.
- The issue that there is no way of enforcing the reality of the privacy practices presented by PETs was raised. That is, PETs can represent that they offer certain protections but there is often no way of checking whether the level of protection actually provided matches that which the PET has represented it provides.
- It was mentioned that the P3P technology may be anti-competitive — that is, if a Web site/enterprise has a good privacy policy but does not implement P3P, would not its traffic be diverted?
- Finally, the question of whether it would be appropriate to work towards the development of international management standards (which is currently being examined in the European context) was raised.

Session II: Educating users/consumers and business

This session focussed on highlighting through a series of presentations, the challenges of, and methods for educating users/consumers and businesses about PETs. In this session, an academic provided an overview of the nature of privacy risk perception among individuals and how education about PETs fits into this framework. This was followed by two speakers focusing on a more pragmatic level — one on the concept of "privacy-by-design", and one on the education of users/consumers.

Privacy risk perception and education about PETs

Perri 6, Director, The Policy Programme, Institute for Applied Health and Social Policy, Kings College, London presented his research paper which he undertook in the capacity of consultant to the OECD (see Appendix II). Mr. 6 explained that he would concentrate on the inter-relationship between privacy risk perception and education about PETs.

One of the key points Mr. 6 made in his presentation was that when designing effective education for business and consumers, the issue of education needs to be examined as a *persuasion* issue. By this, he meant that the issue of whether or not businesses can be persuaded to invest in PETs — and that consumers can be persuaded to ask for them — is the key to determining when, for whom and under what circumstances 'communication' about PETs will be most effective.

For business, Mr. 6 stressed that the challenge is one of persuading them that they should internalise certain costs (to invest in PETs) in a market where they fear their rivals may externalise such costs. For consumers, he noted that the challenge of persuasion is shaped first, by the extent to which different types of consumers care about privacy risks and which risks they care about most; second, how preferences for protection against various kinds of risks are traded off against price increments; and third, how consumers will trade off their privacy preference against the cost of searching out and moving to another supplier.

Further, Mr. 6 asserted that 'who can be persuaded of what' needs to be considered bearing in mind differing and particular perceptions of risk. His argument is that not everyone is equally open to persuasion about everything but that classifying and segmenting businesses and consumers can assist understanding of varying levels of 'openness' to persuasion on the basis that it is location and institutional context that determine what information one can hear, accept and also what information one will reject.

In his analysis of 'openness' Mr. 6 first segmented the populations of businesses and consumers in relevant ways stressing that it is through distinguishing sectors of firms and by grouping consumers according to their situation in social organisation that risk perception can be explained. He separated business for example into the *criminal sector*, the *orderly sector*, the *entrepreneurial sector* and the *sector under the spotlight* and characterised consumers into the groups of *isolate*, *hierarchy*, *individualism* and *enclave*. He then identified which kinds of privacy protections would be expected to be of greatest interest in each segment/group and then discussed the means by which persuasion might be applied most effectively to each of these segments/groups.

Mr. 6 then discussed the dynamics of the relationship between business' ability and willingness to offer privacy-respecting services and consumers' ability and willingness to demand those services. He noted that it may be possible for the institutional processes governing businesses and consumers to create a sorting process which leads consumers and businesses with similar characteristics, institutional styles and constraints, and responsiveness to similar concerns to gravitate towards each other. He stressed that this sorting process is never perfect given market dynamics but noted that a reasonable level of sorting between the different segments of business and consumers might be achieved.

In concluding, Mr. 6 highlighted the following for public policy makers endeavouring to persuade business and consumers of the value of PETs: there is scope for persuading business and consumers to be interested in PETs but this scope is circumscribed by the fact that certain kinds of PETs will be more attractive to businesses and consumers in certain situations. By bearing in mind the differing constraints, institutional contexts, basic assumptions and outlooks of businesses and consumers, policy makers may be able to target communications about PETs to specific groups of business and consumers in ways that will make a significant difference.

Privacy-by-design

Stephanie Perrin, the Chief Privacy Officer of Zero-Knowledge Systems Inc. gave a presentation entitled Privacy by Design: Thoughts on progress to date.

Ms. Perrin first provided an overview of the Zero-Knowledge experience since the company was founded in 1997 and then described its key products. She explained that the company's first focus was on developing tools for consumers and its flagship product was *Freedom Premium Services 2.2* — the product enabled consumers to regain total control of their privacy; create their own identity; decide what they wanted to reveal to whom; and to protect themselves from being monitored and profiled. However, recognising that customer demand was for privacy and security tools, Zero-Knowledge recently redesigned and replaced *Freedom Premium Services 2.2* with *Freedom Privacy and Security Tools 3.0*. This newly released product is a software package for online security and online privacy protection which consists of a Personal Firewall plus a flexible suite of applications (including a From Filler/Password Manager, Cookie Manager, Ad Manager and Keyword Alert) that enables consumers to secure their PC against security threats while protecting their privacy and personal information on the Internet.

Zero-Knowledge's other key product is the Enterprise Privacy Manager (EPM) which is a tool aimed at assisting organisations in achieving secure and private management of customer and corporate data within their organisation. Ms. Perrin explained that the product operates as a tool that enables business to identify, analyse, manage and report on the location and handling of customer information throughout the enterprise. Zero-Knowledge developed the product recognising that organisations are collecting and storing an increasing amount of information but are in a difficult position to manage this information effectively. As an automated tool which assists in tackling this issue, the product is aimed at enabling business to reduce operating and regulatory compliance costs, build customer loyalty and trust, and mitigate the risks associated with information management.

In addition to the EPM, Ms. Perrin explained that Zero-Knowledge provides technical consulting, training and development services to assist companies in a number of areas. These include establishing priorities for a business privacy plan, analysing information-handling practices and in tailoring the EPM system to their unique business-operating environment to ensure its smooth integration into the business.

Finally, Ms. Perrin discussed some of the challenges of communicating privacy by design to both consumers and business. She noted a number of key issues including that: the level of understanding of privacy technologies is still very low; consumers are reluctant to pay for privacy/security protection and are suffering from 'information overload' on new issues; business must be reminded of the importance of putting mechanisms in place to manage privacy/security risks and provided with incentives to invest; law enforcement issues and data retention are still problematic and there has been a chilling in the marketplace; authentication issues are still unsolved; and the newest applications (*e.g.* wireless Internet and geo-positioning) are such that the challenge of building in privacy/security protection is a non-trivial issue and perhaps one not able to be surmounted.

Educating consumers about PETs

Naja Felter, Policy Officer, E-Commerce and Trade, Consumers International (CI), discussed issues related to educating consumers about PETs. Ms. Felter started her presentation by providing background information on Consumers International and an overview of its education initiatives. CI promotes public education primarily through release of its various reports, by educating national members groups and through interactions with the international business community. In seeking to educate consumers effectively particularly in the area of PETs, Ms. Felter noted that the bar must be set low as the people that most need privacy assistance are likely to have low technical knowledge.

Ms. Felter discussed the findings of CI's Privacy@Net publication which reports on a cross-country survey on privacy in e-commerce. The study investigated Web sites' data collection practices. Of the 751 sites investigated, 2/3 of sites were found to collect various kinds of personal information but few had privacy policies that provided information on data rights. Further the study found that, of the sites that did have privacy policies, a number were found to be in breach of these policies.

Ms. Felter noted that privacy and security, access to redress and prevention of fraud are of paramount importance to consumers but that PETs can only help consumers seeking to protect their privacy to a limited extent. The key weaknesses of PETs identified include that they do not have a high degree of usability and consumers are therefore not able to make informed decisions and they only cover a subset of the Fair Information Practices of the Privacy Guidelines. Further, Ms Felter noted that PETs are frequently offered as an alternative to legal protections rather than an extension and that this is unfortunate as they are, at the very best, an incomplete remedy.

Ms. Felter concluded by noting that CI encourages the development of new privacy protection technologies as a complement to the legal framework that regulates the collection of data but believes the burden should not be on the consumer in this area. Further, Ms. Felter noted that business should therefore be encouraged to do more work to ensure that PETs better implement and enforce the OECD Privacy Guidelines and have a much higher degree of usability so they are more useful and effective in safeguarding privacy.

General discussion

During discussion, participants asked a number of particular questions on the content of the presentations:

- Perri 6 was asked to indicate the percentage of consumers that fall into each defined category or group as outlined in his study. He noted that people move from group to group as they move between contexts. For example they may be more 'enclaved' about health data than they are about the identity data stored in a supermarket privilege card. He emphasised that in order to understand what drives risk perception, further study is necessary to look at how people from a community behave when the context changes. He also stressed the need for further empirical/economic data in the area of privacy as there is, at present, no good quantitative data available on a cross-national basis. Mr. 6 finally emphasised the importance of tailoring education and persuasion strategies to the particular situation of the audience being targeted.
- Stephanie Perrin was asked to elaborate on the concept of the 'tagging of data' with corresponding privacy rights/obligations and how this might be achieved. She noted that the issue is one of trying to tag data in the first instance recognising that most large organisations are often not sure where the data they receive has come from and what rights were attached to it/promises made when it was received. The idea is therefore to code all rights to information and to stop it at its aperture so the lawyers can then make a decision as to what is to be done with that information.
- David Banisar, on behalf of Consumers International, was asked to provide practical examples of educational actions. He explained that the many consumer organisations which constitute its membership undertake a variety of activities including consumer reports, research on privacy, information campaigns through the media/TV, lawsuits and boycotts. CI is also hoping to see some large groups doing usability testing and verification tests. Consumers International has also released its 'Five Ways to Improve Privacy Online' publication in five languages. The Council of Europe and Electronic Frontier Foundation (EFF) recommendations on how consumers can protect themselves on the Internet were also noted.

- Stephanie Perrin also commented further on strategies for educating business. Zero-Knowledge's strategies include that it has general information on its Web site (*e.g.* why businesses need tools), publishes a newsletter, responds to ad hoc questions on privacy issues and holds annual conferences on Privacy by Design with a view to encouraging business to build in privacy to boost customer loyalty and trust. She noted that educating consumers is important but business must also be encouraged to think about these issues seriously.
- With regard to the issues of privacy in the mobile environment, identified as an area that will raise a new set of issues in the future, H. Lindskog stressed that developments in the wireless industry indicate that users will have their identity in a device and privacy issues in this context will therefore need to be re-evaluated.

Concluding remarks

The Chair closed the Forum by thanking speakers and participants for their contributions. He noted the diverse range of issues that had been discussed during the Forum. He also noted the need for further efforts by governments, business, privacy experts and consumer representatives to notably raise the awareness of users and businesses about PETs, build user confidence in these tools, and influence their development in the interest of greater privacy protection.

NOTES

1. www.ntia.doc.gov/ntiahome/privacy.
2. See Chapter 12.
3. Ibid.
4. Dr. Burkert is at the Institute for Media Communication of the GMD German National Research Center for Information Technology.
5. For example: A March 2000 *Business Week*/Harris survey found that 63% of Internet users who have not purchased anything online were "very" concerned that the company they would buy from would use their personal information to send them unwanted information. A September 2000 Gallup poll found that 53% of Internet users were "very concerned" about the privacy of personal information they gave out online, as well as the privacy of their online activities. The *Economist* magazine noted in October 2000 that the most serious obstacle to e-commerce success is "customers' terror of launching their financial details into cyberspace."
6. See, for instance, the findings of focus groups conducted for the "Consumer Privacy in the Information Age" report issued by the National Consumer Council of the United Kingdom in December 1999.
7. See page 33 and, in general, "Appendix 3: Technologies of Privacy".
8. Other agencies from member countries have similarly issued statements supporting P3P and other privacy-enhancing technologies.
9. "A Survey of Consumer Privacy Attitudes and Behaviors," conducted for the Privacy Leadership Initiative by Harris Interactive, released 2 April 2001. In contrast to these low numbers for PETs usage, the survey found that significantly higher numbers of people do take other proactive steps to protect their privacy, including reading privacy policies, refusing to give information they consider too personal or unnecessary, and avoiding visiting specific Web sites with dubious privacy practices.

APPENDIX I: A STUDY OF PRIVACY-ENHANCING TECHNOLOGIES[1]

Objective, scope and method

Objective

The objective of this study is to identify the privacy-enhancing technologies (PETs) used on the Internet and show their impact on privacy protection in the light of the OECD Guidelines for the Protection of Privacy and Transborder Data Flows of Personal Data.

Scope of the study

The research focused on tools specific to the Web and, to a lesser extent, e-mail. It is not intended to be exhaustive. Our priority was to concentrate on tools with the following functionalities:

Functionality	Definition
Encryption	Significant but not exclusive use of cryptography.
Anonymity/pseudonymity	Makes users anonymous or conceals their identity by using a pseudonym.
Personal data management	Preference management. Any means that makes it possible to select the information collected.
Cookie filter	Cookie filtering or management.
Ad filters	Filtering or blocking of advertising.
Spyware filters	Detection and deletion of spyware (understood as 1/ transparent GIFs or 2/ client-side ad software).
Marketing consent management	Direct marketing solution respecting privacy.
Mail privacy	E-mail protection (security and/or anonymity of e-mail).
Online payment security	Payment security.
Access control	Centralised password management.
Privacy auditing/compliance	Auditing of the means available and their compliance with current protection principles.
Tutorial	Educational application (educational software).
Complex scheme	Complex technical scheme for protecting privacy (such as Encirq).

and their effects with respect to the privacy guidelines:

- Security.
- Collection limitation/choice.
- Collection avoidance.
- Notice.
- Use limitation.
- Access.
- Educational tools/information/awareness.
- Accountability.

1. This study was prepared by Laurent Bernat, Head, Information and Strategy, Projetweb in his capacity as a consultant for the OECD.

Due to constraints of time and resources, the tools providing the following main functionalities could not be examined:

- Pure cryptography tools (such as PGP).
- Tools for protecting children (such as MS Kids passport).
- Deletion tools, whether they permanently delete the traces physically left on the disc in general (true deletion) or delete normally the traces left while surfing the Internet (cookies, temporary cache files, history, etc.).
- Tools designed to secure the PC network: personal and professional firewalls, anti-virus, packets sniffers.
- Anonymous access security tools, for example, via a biometric system (such as mytec.com).

Nor were solutions such as "service bundles" proposed by Internet Service Providers (ISP) and hosts taken into account.

Method

Research on the tools targeted was carried out using:

- Major general directories (yahoo.com, about.com).
- Search engines (google.com, alltheweb.com).
- Downloadable software (download.cnet.com).
- Reference sites in the field of privacy protection (epic.org, cdt.org, etc.).

Over 130 sites were visited. Some 83 were selected as providing a privacy-enhancing tool on the basis of the criteria selected.

We eliminated from the final list sites that were:

- Clearly obsolete.
- Deemed to have low credibility given their content (*e.g.* an anonymizer that devoted half of its home page to touting the aphrodisiac effects of pheromones[2]).
- Presenting products not yet available, even in beta version.
- Unavailable or inaccessible at the time of the test (these sites were visited several times).

It should be pointed out that the fact that a site is functioning does not always mean that the company responsible is still in business.

Each tool was analysed on the basis of:

- The presentation of the product available on the site.
- A short test, if necessary.

The results of this analysis are listed in a breakdown (see attached table) that shows:

- Information about the company: organisation name and URL, type of organisation, founding date, geographic origin, privacy policy on Web Site.

2. www.aixs.net.

- The name of the product and, if applicable, its version.
- Information about the product: characteristics, principal functionality, policy effect in the light of the OECD Guidelines, principal target audience.

Figures

The figures obtained can be broken down as follows:

Number of sites targeted and selected	83	
Targeted audience		
Individual	69	83%
Organisation	17	20%
Geographic origin		
United States	63	76%
Canada	6	7%
International (such as W3, OECD)	3	4%
?	2	2%
Germany	2	2%
Russia	2	2%
France	1	1%
Gibraltar	1	1%
Sweden	1	1%
Thailand	1	1%
United Kingdom	1	1%

As the research was conducted using keywords in English, it is possible that some tools may not have been identified if the sites presenting them were drafted in another language. This may explain the fact that there were few tools on sites other than North American ones.

Privacy policy on the Web Site		
Yes	63	75%
No	20	25%
Type of application		
Web based	24	29%
Install.	42	51%
Web based/install.	4	5%
Install (java).	2	2%
Install (ActiveX).	1	1%
Other	10	12%
Pay or free?		
Pay	30	36%
Free	38	46%
Both	11	13%
Not clear	4	5%
Registration required	9	11%
Subscription required	14	17%

Principal functionality		
Encryption	16	19%
Anonymity/pseudonymity	30	36%
Personal data management	10	12%
Cookie filter	39	47%
Ad filters	15	18%
Spyware filters	15	18%
Marketing consent management	2	2%
Mail privacy	15	18%
Online payment security	4	5%
Access control	5	6%
Privacy auditing/compliance	6	7%
Tutorial	2	2%
Complex scheme	7	8%
Policy effect		
Security	22	27%
Collection limitation/choice	37	45%
Collection avoidance	33	40%
Notice	11	13%
Use limitation	2	2%
Access	2	2%
Educational tools/information/awareness	2	2%
Accountability	4	5%

Summary

An examination of the characteristics of these tools and an assessment of their limitations confirms that they can be of value in helping users to protect their privacy, but also that they are necessarily complementary to other tools (educational, contractual, regulatory, etc.).

Benefits and limitations

From a technical standpoint, none of the tools identified uses a full range of functionalities that would make it possible to provide total privacy protection in line with the OECD Guidelines.

If we count the number of tools that have an impact on the OECD Guidelines, we see that:

- Only one tool concerns five of the eight principles.[3]
- Two tools concern three principles.[4]
- 22 tools concern two principles.
- 58 concern only one principle.

3. Auditing/compliance tool for businesses (TrustFilter, a product of PrivacyRights).

4. Freedom Internet Privacy Suite, a product of Zero Knowledge, for Internet users, and IBM's Tivoli Secure Way Manager, for organisations.

Consequently, no tool identified in this study provides a complete solution for privacy protection. Users who wish to protect themselves most effectively should therefore combine several tools to optimise their level of protection.

Permission marketing and privacy: the birth of a new market?

The tools and solutions discovered in this study constitute an emerging market, and users' demand for privacy protection is being met by a supply that is divided into a number of segments. Some companies are proposing original solutions involving technological intermediation (similar to the concept of "infomediary" developed by John Hagel and Marc Singer[5]) aimed at enabling companies to use personal data for marketing purposes with users' consent (permission based marketing) while guaranteeing respect for their privacy. These companies appear to have been established quite recently and are currently looking for economic and financial partners.[6]

Technical barriers to wider use

51% of the tools examined in this study must be installed on the user's computer. This can sometimes be an obstacle to their wider use for the following reasons:

- Users may view this process as being potentially dangerous and refuse to install the tool.
- It may go against company policy, since companies often prohibit employees from installing non-standardised applications on their computers; this would place employees in an ambiguous situation vis-à-vis their employer and make them take conflicting risks in order to protect their privacy.

Furthermore, for a product to be widely used, it must be compatible with all the user systems available, and, when used as a browser plug-in, it must be available for a number of browser versions. In reality, these products are rarely this flexible, as their publishers concentrate on making them compatible with one or two versions of the user systems or browsers on the market.

Psychological barriers: the importance of trust

Some sites provide very little information on the organisation behind them, their country of origin, their nature (commercial company, association, natural person, etc.), the identity of their founders or even their exact address and telephone number. Often, an e-mail address is the only connection between the user and the publisher of the site.

Some free sites provide no information that would enable users to identify their origin, even by querying the Whois database in order to identify the owner of the site's name.[7] As for pay products,

---

5. "Net Worth", Harvard Business School, 1999.

6. For example, the solutions available from Lumeria, Encirq and Persona.

7. For example: www.the-cloak.com, a Web interface that makes it possible to anonymize Web surfing via a proxy. No information on the origin of the service or the identity of the service providers is available on the site. On the basis of the information on the Whois database, it is not possible to identify clearly its country of origin.

which require remote payment in order to use the product, they do not always provide the information necessary.

Internet users will only use PETs type tools if they can trust:

- The technology used by the tool. This means that users must understand this technology and what it can provide.
- The tool itself: is it reliable, without defects or bugs that, instead of protecting users, might make them more vulnerable?
- The organisations or individuals who developed the tool: are they really pursuing the goals that they say they are?

The software developed by the Open Source community provides a high level of transparency. A number of Open Source projects being developed are specifically aimed at privacy protection.

Educating users

As the preceding summary shows, educating users is an indispensable component of the policy mixture that addresses online privacy. In this regard, many of the sites visited make a serious effort to educate users as a necessary preliminary for persuading them to use their product.

In this regard, three different approaches can be distinguished in the sites visited:

- Sites presenting technologies that are being developed and that are therefore intended mainly for advanced users, whether they are power-users or developers.[8] In this case, the information is highly detailed and technical, and probably too complex for final users.
- Sites that combine their commercial documentation or the presentation of their aims with high-quality educational information[9] and links to other reference sites.
- Sites that primarily describe the advantages and benefits of the tool without really informing users of how the benefit provided (such as anonymity) is related to the technical functioning of the product.

Possible future work

Optimising classification of technical functionalities

A more complete classification of the functionalities and techniques used, together with accurate definitions, would make it possible to describe better how each technology is linked to its policy effect.

8. For example, the site of the Freenet project (http://freenet.sourceforge.net) or of IBM's P3P policy editor (www.alphaworks.ibm.com/tech/p3peditor).

9. For example, Anonymizer's site presents clear information on how the product works and, by extension, on the principle of proxy anonymizers (www.anonymizer.net).

For example:

- Regarding cookies, a distinction could be made between display, blocking, filtering, editing, deleting and recognising cookies from other sites. Some tools may limit collection via user choice (collection limitation/choice) or systematically prevent collection (collection avoidance) depending on the functionalities used.
- For anonymity tools using a non-transparent proxy, a distinction might be made between tools that:
  - Use their own proxy.
  - Select, test and use other proxies, thereby considerably increasing the degree of anonymity of the user.
  - Authorise HTTPS to scramble the traces left on the local network.
  - Filter certain information (cookies, last page visited, advertising, javascript, images, etc.).

Further investigation of these questions would also make it possible to take certain technical subtleties into account. For example, a persistent cookie is a risk for users of the site that sets the cookie, but also for third parties that have access to these users' hard disc. This means that cookie management tools might have a "security" policy effect, as understood in the OECD Guidelines.

Specific studies on certain types of tools

Specific studies might be carried out on the technologies that have not been analysed, such as:

- Pure cryptography tools.
- Tools related to e-mail use.
- Personal security tools.
- Tools designed more specifically for children.
- Tools using other protocols besides e-mail or the Web, such as newsgroups, chat rooms (ICQ, IRC, AOL's buddy list, etc.), telnet or file transfer (FTP) that have not been specifically addressed in this study, even though they are now widely used.

Special attention should be focused on:

- Tools being developed in the free software community: when the keyword "Privacy" was entered in the search engine of the main site that lists these projects,[10] it showed some 25 projects under way.
- Projects that use distributed network or peer-to-peer (P2P) technologies, especially the Freenet project aimed specifically at ensuring the anonymity of its users, whether they are publishing or using information.
- Tools and technologies intended to ensure the security of a system or access to a system without divulging the identity of users (such as, mytec.com, mentioned above).
- Tools and solutions oriented towards permission-based marketing, which respect the privacy of users.

10. www.sourceforge.net.

Usability of tools and educational aspects

An analysis of the usability of tools might provide an interesting perspective. This would mainly involve evaluating the ability of final users to grasp fully the purpose of each tool, install it effectively and use it continuously on a daily basis.

Although few tools are primarily aimed at educating users and enabling them to take responsibility for protecting their own privacy, most of them do help keep users better informed and some give this aspect great importance. It might be interesting to identify the tools that have specific functionalities for this purpose and to analyse the means that they use.

Other possibilities

More in-depth research on the tools available, *i.e.* aimed at compiling an exhaustive list, might be carried out, in particular by using search terms in other languages besides English.

Table 1. **Surveyed PETs**

Organisation name and URL	Type of organisation	Founding date	Privacy policy on Web site?	Geographic origin	Name of main PETs product(s) and version	Product characteristics	Principal functionality	Policy effect	Principal targeted audience
@nonymouse http://nonymouse.com/	Association	1997 (copyright)	Yes	Germany	AnonWWW AnonEmail AnonNews	Free, Web-based	Anonymity/ pseudonymity, mail privacy	Collection avoidance	Individual
AbsoluteFuture, Inc. www.safemessage.com	Software company	1998	Yes	United States	SafeMessage v. 2.0	Paying, subscription required, install	Encryption, mail privacy	Security, collection avoidance.	Organisation
adScience, Ltd.	Software company	1997?	Yes	United Kingdom	Filtergate v. 4.03	Paying, Install	Cookie filter, ad filters, spyware filters	Collection limitation/choice	Individual.
Agenetics www.superyou.net	Internet company	?	Yes	United States (domain name)	SuperYou Messaging	Free, registration required, Web based, beta version.	Encryption, mail privacy	Security	Individual
American Express www.americanexpress.com	Credit card provider	1850 (Private payments : 2000)	Yes	United States	Private payments	Free, registration required, install, free for cardholders	Online payment security	Security, collection limitation/choice	Individual
AnalogX www.analogx.com	Software company?	1998?	No	United States	CookieWall v. 1.01	Free, install, adds on to browser	Cookie filter	Collection limitation/choice	Individual
Anonymizer www.anonymizer.com	Privacy/ security company	1996	Yes	United States	Anonymous surfing, secure tunnelling	Paying, subscription required, Web-based/install, very basic is free	Anonymity/pseudonymity, cookie filter, ad filters, spyware filters	Collection avoidance	Individual
AOL/Netscape www.netscape.com	ISP/software company	?	Yes	United States	Netscape cookie manager, password manager v. 6.1	Free, included in browser	Cookie filter, access control	Security. collection limitation/choice	Individual
Ascentive www.ascentive.com	Software company	1998 (copyright)	Yes	United States	ActivePrivacy v. ?	Paying, install, free for a limited time	Cookie filter	Collection limitation/choice	Individual
AT&T	Telecommunications company	AT&T founded in 1875	Yes	United States	Crowds	Free, registration required, install, only for non commercial use in the US	Anonymity/ pseudonymity	Collection avoidance	Individual
AT&T www.research.att.com/projects/p3p/propgen	Software company	AT&T founded in 1875	Yes	United States	P3P proposal generator	Free, Web-based	Personal data management	Notice	Individual
Barefoot Productions	Software company	1994 (incorporated	No	United States	Zdnet's CookieMaster v. 2.0	Free, install, product outdated	Cookie filter	Collection limitation/choice	Individual

Organisation name and URL	Type of organisation	Founding date	Privacy policy on Web site?	Geographic origin	Name of main PETs product(s) and version	Product characteristics	Principal functionality	Policy effect	Principal targeted audience
www.barefootinc.com		1997)				(only for IE 3.0), distributed by ZiffDavis, the links to zdnet are broken			
Basta Computing www.basta.com	Software company	1996	Yes	United States	Buzof v. 1.6	Paying, install	Cookie filter, ad filters	Collection limitation/choice	Individual
Camtech 2000, Ltd. www.camtech2000.net	Software company?	?	No	United States (domain name)	CT Cookie Spy v. 2.0	Free, install	Cookie filter	Collection limitation/choice	Individual
Checkflow www.flowprotector.com	Software company	?	Yes	France	FlowProtector v. 2.0	Free/pay, install, pay for advanced version	Cookie filter, ad filters, spyware filters	Collection limitation/choice	Individual
Direct Marketing Association www.the-dma.org/privacy	Trade association	1917	Yes	United States	Privacy policy generator	Free, Web-based	Personal data management	Notice	Organisation
Disappearing Inc./Omniva www.disappearing.com www.omniva.com	Software company	1999	Yes	United States	Omniva policy manager v. ?	Paying, install	Encryption, online payment security	Security	Organisation
Distinctly.com, Inc.	Internet technologies company	1997 (domain name)	Yes	United States	SilentSurf	Free, Web-based	Anonymity/ pseudonymity	Collection avoidance	Individual
Ditto Technologies www.dittotech.com	Software company	2000 (copyright on the site)	No	United States	Cookie eater	Free, install	Cookie filter	Collection limitation/choice	Individual
Ditto Technologies www.dittotech.com	Software company	2000 (copyright on the site)	No	United States	MiLk v. 2.0	Pay, install	Cookie filter	Collection limitation/choice	Individual
Dr. Jon's Software www.angelfire.com/il2/drjsoftware/	Individual developer (?)		No	United States	MagicCookie Monster v. 1.0 fc 1a	Free, registration required, install, e-mail registration	Cookie filter	Collection limitation/choice	Individual
Encirq www.encirq.com	Privacy/ security/ marketing services company	1998	Yes	United States	Illuminated statement	Paying, business-based tool	Anonymity/ pseudonymity, complex scheme	Collection avoidance	Organisation
Eric Murray Consulting www.meer.net/~ericm/cookie_jar/	Privacy/ security consultant	?	No	United States	Cookie Jar v. 2.01	Free, install	Cookie filter	Collection limitation/choice	Individual
Free Network Project	Non-profit	1999	No	United States	Freenet v. 0.3.9.2	Free, install, beta	Encryption,	Security, collection	Individual

Organisation name and URL	Type of organisation	Founding date	Privacy policy on Web site?	Geographic origin	Name of main PETs product(s) and version	Product characteristics	Principal functionality	Policy effect	Principal targeted audience
http://freenet.sourceforge.net/	corporation					version open source project, the corporation was created only to get donations	anonymity/ pseudonymity, complex scheme	avoidance	
George Mason Society http://freedom.gmsociety.org	Advocacy group	?	No	United States	Freedom remailer	Free, Web-based	Anonymity/ pseudonymity, mail privacy	Collection avoidance	Individual
Global Internet Liberty Campaign www.gilc.org/speech/anonymous	Advocacy group	?	No	International	W3-Anonymous Remailer	Free, Web-based	Anonymity/ pseudonymity	Collection avoidance	Individual
Guidescope, Inc. www.guidescope.com/home	Internet technologies company	2000	Yes	United States	Guidescope v. 0.994	Free/paying, install, free for personal/pay for business	Cookie filter, ad filters, spyware filters	Collection limitation/choice	Individual
Hidden surf www.hiddensurf.com	Internet privacy company?	?	Yes	United States (domain name)	Hiddensurf	Paying, subscription required, Web – based	Anonymity/ pseudonymity, cookie filter	Collection avoidance	Individual
Hilgraeve www.hypersend.com	Privacy software company	1980	Yes	United States	HyperSend	Paying, registration required, subscription required, Web - based/install	Encryption, mail privacy	Security, collection avoidance	Individual
Hush Communications www.hushmail.com	Privacy/ security company	1998	Yes	United States	HushMail v. V2	Free/paying, Web-based, free + yearly fee for advanced service	Encryption, anonymity/ pseudonymity, mail privacy	Security	Individual
IBM www.ibm.com	Information technology company	1914	Yes	United States	Tivoli SecureWay Privacy Manager	Paying, install, business-based tool	Complex scheme	Security, use limitation, access	Organisation
IBM www.ibm.com www.alphaworks.ibm.com/tech/p3peditor	Information technology company	1914	Yes	United States	P3P Policy Editor v. beta 1.7	Free, install, beta version	Personal data management	Notice	Individual
Idcide www.idcide.com	Privacy/ security company	1999	Yes	United States (Israel)	Privacy Companion v. 1.0.3	Free, install, browser add-on	Cookie filter, spyware filters	Collection limitation/choice	Individual
Idcide	Privacy/ security	1999	Yes	United States (Israel)	PrivacyWall (site analyzer, site	Paying, install	Privacy auditing/compliance	Accountability	Organisation

Organisation name and URL	Type of organisation	Founding date	Privacy policy on Web site?	Geographic origin	Name of main PETs product(s) and version	Product characteristics	Principal functionality	Policy effect	Principal targeted audience
www.idcide.com	company				monitor)				
IDzap, LLC www.idzap.com	Privacy/ security company	?	Yes	United States	Idsecure, free anonymous browsing	Free/paying, registration required, subscription required, Web – based, subscription for advanced service (idsecure), free for basic (free anonymous browsing), e-mail registration for both.	Anonymity/pseudonymity, cookie filter	Collection avoidance	Individual
Incogno Corporation www.incogno.com	Software company	1999	Yes	United States	SafeZone	Business-based tool	Encryption, anonymity/ pseudonymity, online payment security, complex scheme	Security, collection avoidance	Organisation
iNetPrivacy www.inetprivacy.com	Privacy software company	1997 (copyright)	No	Russia/Canada (domain name)	Anonymity 4 Proxy (A4Proxy) v. 2.52	Paying, install	Anonymity/ pseudonymity, cookie filter	Collection limitation/choice, collection avoidance	Individual
Information and Privacy Commissioner/Ontario www.ipc.on.ca/english/resources/resources.htm	Privacy Commissioner	1990	No	Canada (Ontario)	Privacy Diagnostic Tool (PDT)	Free, install, MS Access file	Privacy auditing/ compliance, tutorial	Educational tools/information/awareness	Organisation
Intelligent Software Modeling Inc. www.surferprotectionprogram.com	Internet privacy company	1997	No	United States	Surfer Protection Program	Paying, install	Cookie filter	Collection avoidance	Individual
Intelytics www.intelytics.com	Privacy software company	?	Yes	United States	Message sentinel	Paying, install	Spyware filters, mail privacy	Collection avoidance	Individual
Intelytics www.intelytics.com	Privacy software company	?	Yes	United States	Personal Sentinel v. 1.5.2	Free, registration required, install	Cookie filter, ad filters, spyware filters	Collection limitation/choice	Individual
Intelytics www.intelytics.com	Privacy software company	?	Yes	United States	Site sentinel	Paying, install	Privacy auditing/compliance	Accountability	Organisation

Organisation name and URL	Type of organisation	Founding date	Privacy policy on Web site?	Geographic origin	Name of main PETs product(s) and version	Product characteristics	Principal functionality	Policy effect	Principal targeted audience
Intermute www.intermute.com www.adsubtract.com	Software company	?	Yes	United States	AdSubtract	Free/paying, registration required, install, free for personal use/pay for more advanced versions	Cookie filter, ad filters, spyware filters	Collection limitation/choice	Individual
Invisible hand software www.privacybot.com	Software company	1991	Yes	United States	PrivacyBot	Paying, subscription required, Web-based	Privacy auditing/compliance	Notice, accountability	Organisation
iPrivacy www.iprivacy.com	Privacy/ security company	1999	Yes	United States	Identity Manager	Free., consumer access tool through credit card companies	Encryption, anonymity/ pseudonymity, online payment security, complex scheme	Security, collection avoidance	Individual
ISL Internet Sicherheitsloesungen GmbH www.rewebber.de/index.php3.en	Privacy/ security company	?	Yes	Germany	Rewebber	Paying, subscription required, Web – based	Encryption, anonymity/pseudonymity	Collection avoidance	Individual
Junkbusters Corporation http://internet.junkbuster.com	Privacy/ security company	1996	Yes	United States	Internet Junkbuster Proxy v. 2.0.2	Free, install, license : GPL.	Cookie filter, ad filters	Collection limitation/choice	Individual
KeepItSecret	Privacy/ security company	?	No	United States (domain name)	KeepItSecret (?)	Free/paying, Web-based, free with registration/daily mailing, pay accounts without mailing	Anonymity/ pseudonymity, cookie filter	Collection avoidance	Individual
Kookaburra Software www.kburra.com	Software company	1996	Yes	United States	Cookie Pal v. 1.6	Paying, install	Cookie filter	Collection limitation/choice	Individual
Lavasoft www.lavasoftusa.com	Software company	?	No	Sweden? United States?	Ad-Aware, Ad-Aware Plus v. 5.5	Free/paying, install, free for basic version, pay for advanced versions	Spyware filters	Collection limitation/choice	Individual
Lumeria, Inc. www.lumeria.com	Privacy/ security/ marketing services company	1998	Yes	United States	Sunshine technology, including SuperProfile	Beta version business-based tool	Personal data management, cookie filter, ad filters, marketing consent management,	Collection limitation/choice	Individual, organisation

Organisation name and URL	Type of organisation	Founding date	Privacy policy on Web site?	Geographic origin	Name of main PETs product(s) and version	Product characteristics	Principal functionality	Policy effect	Principal targeted audience
							complex scheme		
MailEncrypt	Privacy Internet company	1998	Yes	United States	MailEncrypt	Paying, subscription required, Web-based	Encryption, mail privacy	Security	Individual
Mailsafe www.mailsafe.org	Privacy Internet company	1998	Yes	Gibraltar	Mailsafe	Paying, subscription required, Web-based	Encryption, mail privacy	Security	Individual
MetaURL Corporation www.idmask.com	Privacy/ security company (?)	?	Yes	Canada	ID Mask	Free/paying, subscription required, install (java), free gets limited bandwidth, subscription gets unlimited, source code may become publicly available	Anonymity/ pseudonymity, cookie filter	Collection limitation/choice, collection avoidance	Individual
Microsoft www.microsoft.com	Software company	1975	Yes	United States	Internet Explorer 6 (with some P3P elements and cookie filtering) v. 6_PP_Refresh	Free, beta version, free download or part of Windows XP	Personal data management, cookie filter	Collection limitation/choice, notice	Individual
MishkinSoft www.multiproxy.org	Software company	?	No	Russia	MultiProxy v. 1.2	Free, install, free for personal use	Anonymity/pseudonymity	Collection avoidance	Individual
Naviscope Software www.naviscope.com	Software company	?	No	United States (domain name)	Naviscope	Free, install, could become paying in future	Cookie filter, ad filters	Collection limitation/choice	Individual
NetHush	?	2001	Yes	United States (domain name)	NetHush	Free, Web-based, financed with ads	Anonymity/ pseudonymity, cookie filter, ad filters	Collection avoidance	Individual
Orangatango www.orangatango.com	Internet privacy company	2000 (copyright)	Yes	United States	Virtual Browser v. 1.0	Free/paying, subscription required, Web-based, free for one week trial	Encryption, anonymity/pseudonymity, ad filters	Security, collection avoidance	Individual
Organisation for Economic Co-operation and Development http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm	International organisation	1961	Yes	Headquarters in France	OECD Privacy Policy Statement Generator	Free, Web-based	Personal data management, tutorial	Notice, educational tools/information/awareness	Organisation

Organisation name and URL	Type of organisation	Founding date	Privacy policy on Web site?	Geographic origin	Name of main PETs product(s) and version	Product characteristics	Principal functionality	Policy effect	Principal targeted audience
Packetderm, LLC http://freemail.cotse.net/freemail/mail/src/login.php	Privacy/ security company	2000	Yes	United States	Cotse Webmail	Paying, subscription required, Web-based, free Web mail closed, only pay remains	Encryption, anonymity/pseudonymity, mail privacy	Security, collection avoidance	Individual
PC Magazine	Media company	?	Yes	United States	CookieCop, CookieCop Plus v. 1.2	Free, install, source code included	Cookie filter	Collection limitation/choice	Individual
Persona www.persona.com	Privacy/ security/ marketing services company	1998	Yes	United States	p-CRM platform	Paying, business-based tool	Personal data management, marketing consent management	Collection limitation/choice	Individual, organisation
Ponoi Corporation www.ponoi.com	Privacy/security company	2000 (copyright)	Yes	United States	Ponoi	Install (java), no information about the business model, seems free	Encryption, anonymity/pseudonymity, access control.	Security, collection avoidance	Individual
Potato Software www.skuz.net/potatoware/jbn/about.html	Software company?	?	No	?	Jack B. Nymble v. 2	Free, install	Encryption, anonymity/pseudonymity, mail privacy.	Security, collection avoidance	Individual
Privacy Foundation www.bugnosis.org	Advocacy group	?	Yes	United States	Bugnosis	Free, install (activeX)	Spyware filters	Collection limitation/choice	Individual
Privacy Software Corporaton www.nsclean.com	Privacy/ security company	1996	Yes	United States	IEClean, NSClean v. 5.5	Paying, install	Cookie filter, mail privacy	Collection limitation/choice	Individual
PrivacyRight www.privacyright.com	Privacy/ security company	?	Yes	United States	TrustFilter (with special versions for financial services, health care and e-business)	Paying, business-based tool	Access control, privacy auditing/compliance, complex scheme	Security, collection limitation/choice, notice, use limitation, access	Organisation
PrivacyX.com Solutions	Privacy/ security company	1998	Yes	Canada	PrivacyX, PremiumX	Free/paying, Web-based, Web-based service is free but with ads (privacyX), more advanced is pay without ads (PremiumX), user must install a certificate and may use their usual mail	Anonymity/pseudonymity, access control.	Security, collection avoidance	Individual

Organisation name and URL	Type of organisation	Founding date	Privacy policy on Web site?	Geographic origin	Name of main PETs product(s) and version	Product characteristics	Principal functionality	Policy effect	Principal targeted audience
						program			
Rendering Better Avenues Software www.rbaworld.com	Software company	1997 (copyright)	No	United States (domain name)	Cookie Cruncher v. 2.11	Free, install	Cookie filter	Collection limitation/choice	Individual
SafeWeb www.safeweb.com	Privacy/ security company	2000	Yes	United States	SafeWeb Triangle boy	Free, Web-based/install, Web-based for SafeWeb, install for Triangle boy	Anonymity/pseudonymity, cookie filter, ad filters, spyware filters	Collection limitation/choice, collection avoidance	Individual
SendFakeMail www.sendfakemail.com	Privacy/ security company	?	No	Thailand	SendFakeMail	Paying, subscription required, Web - based	Anonymity/pseudonymity, mail privacy	Security, collection avoidance	Individual
SiegeSoft	Privacy software company	1998	Yes	Canada	Siege Surfer	Paying, subscription required, Web - based	Anonymity/pseudonymity, cookie filter	Collection avoidance	Individual
Spyblocker Software www.spyblocker-software.com/spyblocker	Software company	?	Yes	United States	SpyBlocker v. 4.2	Free, install	Cookie filter, ad filters, spyware filters	Collection limitation/choice	Individual
SpyChecker.com www.spychecker.com	Advocacy group?	?	Yes	United States	SpyChecker v. 1.1	Free, Web-based/install	Spyware filters	Notice	Individual
The Cloak www.the-cloak.com/anonymous-surfing-home.html	?	?	Yes	?	The Cloak	Free, Web-based	Anonymity/pseudonymity, cookie filter	Collection avoidance	Individual
The Limit Software www.thelimitsoft.com	Software company	1994	Yes	United States	Cookie Crusher v. 2.6	Paying, install	Cookie filter	Collection limitation/choice	Individual
Watchfire www.watchfire.com	Internet technologies company	1996	Yes	Canada	WebCPO	Paying, business-based tool	Privacy auditing/compliance	Accountability	Organisation
World Wide Web Consortium www.w3.org	Industry consortium	1994	Yes	International	Platform for Privacy Preferences (P3P) v. 1.0	To be incorporated in browsers and on organisation web sites	Personal data management	Collection limitation/choice, notice	Individual, organisation
YOUPowered	Privacy/ security/ marketing services company?	?	Yes	United States	Orby v. 3.0 beta	Free, install, beta version	Personal data management, cookie filter, spyware filters, access control	Collection limitation/choice, notice	Individual

Organisation name and URL	Type of organisation	Founding date	Privacy policy on Web site?	Geographic origin	Name of main PETs product(s) and version	Product characteristics	Principal functionality	Policy effect	Principal targeted audience
YOUPowered	Privacy/ security/ marketing services company?	?	Yes	United States	SmartPrivacy Publisher	Paying, install	Personal data management	Notice	Organisation
Zero Knowledge www.zeroknowledge.com	Privacy/ security company	1997	Yes	Canada	Freedom Internet Privacy Suite v. 2.0	Free/paying, install, free for standard/pay for premium	Anonymity/pseudonymity, cookie filter, ad filters, spyware filters, mail privacy	Security, collection limitation/choice, collection avoidance	Individual
ZipLip, Inc www.ziplip.com	Privacy/ security company	1999	Yes	United States	ZipLip Plus	Free, registration required, Web-based	Encryption, anonymity/pseudonymity, mail privacy	Security, collection avoidance	Individual

APPENDIX II: CAN WE BE PERSUADED TO BECOME PET-LOVERS?[1]

Introduction

Over the last decade and a half, the community of data protection regulators, technologists interested in privacy and others have developed both the concept and the tools of privacy-enhancing technologies.[2]

By privacy-enhancing technologies, we may understand those digital systems, as used by and embedded in products and services, that attempt to limit risks to privacy and support the exercise of data subjects' claims to privacy, including those that attempt to control the processing of personal information in ways that reduce the risks of illegitimate processing, for example, by supporting claims to anonymity or pseudonymity, allowing data subjects to express preferences about the use of their information and to obtain secure access to what is held on them, supporting consent to collection or processing, limiting what is collected or how or to which systems it may be disclosed, and so on.[3] This is a wider definition than some people's: I do not confine privacy-enhancing technologies just to those tools that provide pseudonymity. Moreover, I do not here use a distinction between privacy-enhancing and privacy-enabling tools: I use the same term to cover both. At the appropriate point in the argument, a taxonomy will be offered (see Figure 3 below). In the present sense, however, privacy-enhancing technologies are one of the informational equivalents of the plethora of safety devices which are increasingly designed into everything from chemical and nuclear power plants to airliners.[4]

---

1. This study was prepared by Dr. Perri 6, Director, The Policy Programme, Institute for Applied Health and Social Policy, King's College, London, in his capacity as a consultant for the OECD. The author is grateful to Anne Carblanc of the OECD for commissioning this paper, and to Anne Carblanc, Charles Raab, Phil Boyd, Brendon Swedlow, James Tansey and Mary Culnan for their comments on an earlier draft. The author feels that none of these people should be thought necessarily to agree with his arguments, still less do they bear any responsibility for his errors.

2. Information and Privacy Commissioner, Ontario, Canada and Registratiekamer, The Netherlands, 1995, *Privacy-Enhancing Technologies: The Path to Anonymity, Vols I and II*.. See also Registratiekamer for Netherlands, 1999, *Intelligent Software Agents: Turning a Privacy Threat into a Privacy Protector*, Information and Privacy Commissioner for Ontario, Canada and Registratiekamer for Netherlands, Toronto and Rijkswijk. See also the typology offered in Burkert H, 1997, "Privacy-enhancing Technologies: Typology, Critique, Vision", in Agre PE and Rotenberg M, eds, 1997, *Technology and Privacy: The New Landscape*, Massachusetts Institute of Technology press, Cambridge, Massachusetts, 125-142.

3. Cf. the general characterisation given in Burkert H, 1997, "Privacy-enhancing Technologies: Typology, Critique, Vision", in Agre PE and Rotenberg M, eds, 1997, *Technology and Privacy: The New Landscape*, Massachusetts Institute of Technology press, Cambridge, Massachusetts, 125-142.

4. Indeed, many of the same debates will, no doubt, in due course, arise about them as arise in connection with safety devices: do they work, do they induce complacency and undermine vigilance, do they add to complexity in ways that may actually lead to privacy failures? For the major presentation of the argument that designing risk-reducing features into systems adds to complexity and can lead to failures, see Perrow C, 1999 [1984], *Normal Accidents: Living With High Risk Technologies*, 2nd edn, Princeton University Press, Princeton, New Jersey. For a recent statement of the argument that adding risk-reducing systems induces people to be complacent about risk, see

This community is now interested in the questions of whether businesses can be persuaded to invest in them, and whether consumers can be persuaded to demand them. Hitherto, such information as we have about the extent to which online businesses now offer even the simplest privacy practices such as providing information about collection, use and disclosure, offering choice about what information consumers might reveal or over disclosures, and subject access, suggests that only minorities of businesses have made even these modest investments.[5] Proportions offering pseudonymity are almost certainly much lower. Indeed, one academic study soon to be reported involved using a personal computer equipped with the new IE6 software, including the P3P privacy preference definition system, to visit a number of commercial Web sites: the study found that the researcher was asked by a significant proportion of the sampled sites' software to downgrade her privacy preferences in order to use the site.[6] This suggests that if governments want to see wider use of privacy-enhancing technologies, there is a need for some persuading to be done.

I use the word, "persuasion", quite conscious that I am being indelicate. Hitherto, the OECD has, quite understandably, preferred to speak of "education", which sounds much less invasive and manipulative. For although — and no doubt in part *because* — we live in an age which considers that its arts and capabilities of persuasion have been developed quite remarkably exquisitely, it is now considered indecorous to admit that persuasion is indeed what is being done in the name of communication, education, training, the provision of information, and even in advertising. Nevertheless, in trying to assist the OECD in thinking about the question of when, for whom and under what circumstances "communication" about privacy-enhancing technologies (PETs, from now on) might actually work, in the sense of inducing people to be more willing to use them, it is impossible to avoid acknowledging that persuasion and influence are the point of the exercise. Indeed, much of the work on which it is necessary to draw in this paper is explicitly concerned with persuasion. I have no space here to discuss the spectra of more and less invasive, and more and less manipulative forms and strategies of persuasion. However, it is worth noting that those who have researched propaganda of various kinds have generally concluded that the more manipulative and the more insidious strategies are often ineffective, at best tend only to work in the short term, and as their true character emerges over time, tend to be self-undermining.[7] I shall therefore assume that we are interested in how far the more honest ways to seize hearts and minds might be deployed to stir up motivation to use PETs.

Adams J, 1995, *Risk*, UCL Press, London. The principal statement of the argument that designing in risk-reducing features produces inflexible, rigid systems that often increase the likelihood of the very risks these features are meant to reduce, is Wildavsky A, 1988, *Searching for Safety*, Transaction Publishers, New Brunswick, New Jersey. Indeed, Burkert's discussion raises the possibility that there may be privacy failures in systems using these technologies for each of these reasons, although Burkert does not draw the analogy with the wider risk management literature: Burkert H, 1997, "Privacy-enhancing Technologies: Typology, Critique, Vision", in Agre PE and Rotenberg M, eds, 1997, *Technology and Privacy: The New Landscape*, Massachusetts Institute of Technology press, Cambridge, Massachusetts, 125-142.

5. Federal Trade Commission, 2000, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress*, May, Federal Trade Commission, Washington DC, available at www.ftc.gov/reports/privacy2000/privacy2000text.pdf. See also Consumers International, 2001, *Privacy@net: An International Comparative Study of Consumer Privacy on the Internet*, Consumers International, London, available at www.consumersinternational.org/news/pressreleases/fprivreport.pdf.

6. This research is being conducted in the department of management and information technology at Bentley College, Massachusetts: Mary Culnan, personal communication, 3rd October 2001.

7. Jowett GS and O"Donnell V, 1999, *Propaganda and Persuasion*, 3rd edn, Sage, London, 171.

My argument will be that not everyone is equally open to persuasion about anything, still less about everything, but that we can say something about who might be more open to persuasion about what and under which circumstances, and we can say something — albeit a little more modestly — about how differently situated people might be persuaded about the things they may be open to persuasion about. However, classifying and segmenting businesses and consumers is the key to understanding what can be achieved with people in different situations. This is, I know, an annoying conclusion for those who are looking for something more "can do". The one kind of advice that, since the screening of "Yes, Prime Minister", civil service policy advisors now try to avoid is anything that smacks of Sir Humphrey's phrase, "It's all very complicated, Prime Minister". Unfortunately, sometimes, it just is. I shall, however, try to simplify and show that there is order in the complexity of just who is open to persuasion about what.

Contrary to the prevailing wisdom of the less socially oriented psychologists who have dominated the debates about both political and commercial persuasion for a century now, I shall suggest that looking at mental factors will not help us very much: that approach does little more than describe the shape of the problem to be understood. On the contrary, I shall argue that, in the words of one of the greatest studies of who persuades whom, why and how in the last half century, "where you stand depends on where you sit".[8] That is, the openness to persuasion of both businesses and consumers is explained largely by their situation, for it is location in institutional context that determines what information one can hear, accept and use and what information one will reject.[9] Nor indeed is a simple approach of offering incentives enough to open people to persuasion, and, indeed, as I shall note below, many economists are now recognising this too. Incentives may have their place: but not everyone counts the same thing as an incentive, or at least, as an incentive worth having.

The paper has a very simple structure. The next section sets out a short characterisation of the nature of the problem to be tackled. Then there follow two substantive sections that present an account of the openness, first, of businesses, and then, secondly, of consumers, to persuasion, respectively to offer and to demand services in which PETs are used or embedded to protect privacy. In each of these sections, the same strategy is employed. The argument begins with an attempt to segment the populations of businesses and consumers in relevant ways. The analysis of segmentation is then used to identify which kinds of privacy protections would be expected to be of greatest interest in each segment. In each, a short subsection then discusses the means by which persuasion might be applied. These two central elements of the argument are followed by a final substantive section which shows that the basic approaches used in respect of businesses and consumers are not only compatible, but are in fact identical in underlying structure, even though this may not have been obvious at first sight. This enables a discussion of the dynamics of interest in and openness to persuasion about PETs in which I examine consumers and suppliers in the same frame. A short concluding section summarises the main lessons for public policy makers who want to try to persuade businesses and consumers to show more interest in PETs.

---

8. Allison GT, 1971, *Essence of Decision: Explaining the Cuban Missile Crisis*, Little, Brown, Boston: see Allison GT and Zelikow P, 1999, *Essence of Decision: Explaining the Cuban Missile Crisis*, 2nd edn, Addison Wesley Longman, New York, 307. The original formulation of this maxim is attributed to Rufus Miles, a US federal administrator in the 1960s who managed a number of "Great Society" programme agencies under President Johnson, and worked both in the Executive Office of the President and in the Bureau of the Budget, and has been called 'Miles' Law": see Stillman R, 1999, "Where you Stand Depends on Where You Sit" (or, Yes, 'Miles' Also Applies to Public Administration Basic Texts)", *American Review of Public Administration*, 29, 1, 92-97.

9. Douglas M, 1986, *How Institutions Think*, Routledge and Kegan Paul, London; Thompson M and Wildavsky A, 1986, "A Cultural Theory of Information Bias in Organisations", *Journal of Management Studies*, 23, 3, 273-286.

The structure of the problem of persuasion and what we need to learn

Offering consumers products and services designed using privacy-enhancing technologies (PETs) requires investment by businesses, and businesses are only willing to incur the costs of investment if they believe that it will be sufficiently profitable to do so. In many situations where PETs are retrofitted into information systems — though, of course, by no means all — the effect is to increase unit costs. The effect may be much less for new products that are designed from the beginning to use PETs. If companies fear that they cannot pass on those additional costs in the form of higher prices, then they will fear that their rivals will be able to undercut them by offering services and systems that do not feature PETs. The direct benefits of privacy redound to consumers (and perhaps to wider publics), not to the businesses: for businesses, the benefits are indirect. The problem of persuading businesses to invest in PETs, then, is a conventional one, like that of attempting to induce them to behave ethically, or to adopt environmentally beneficial practices. To put the problem in economic terms, the challenge is to persuade businesses that they should internalise certain costs that they have been able to externalise, where market competitive conditions might — at least in many markets — favour those who externalise over those who internalise.[10] This is not, as I shall show, necessarily an insoluble problem, but it does represent a challenge, to which there are only a finite number of basic types of response. However, to learn something about those types of available response, we can look to the lessons from attempts to influence businesses to adopt environmentally beneficial technologies, or to behave ethically in a variety of ways, and we can consider whether there are lessons for the situation in respect of PETs.

To make this paper manageable, I am going to ignore the problem of persuading government agencies, either providing services or purchasing them from the private sector, to adopt PETs in their service specification.[11]

---

10. For a discussion of the economics of inducing businesses to internalise costs that they could externalise and might fear others will externalise, see Baumol WJ, with Blackman SAB, 1991, *Perfect Markets and Easy Virtue: Business Ethics and the Invisible Hand*, Blackwell, Oxford, *passim* but especially chapter 3. Some people would say that this is a problem of getting businesses to internalise the costs of providing public goods. I avoid putting the problem in this way for two reasons. First, there is a debate about just how far privacy protection is a public good, and how far the divisible character of the management of personal information makes it a private good: see *e.g.* Spinello RA, 1998, "Privacy rights in the information economy: review of Legislating privacy: technology, social values and public policy, Priscilla Regan, Chapel Hill: UNC Press, 1995", *Business Ethics Quarterly*, 8, 4, 723-742. I have no wish to enter that arcane question here. Secondly, the question of what counts as a public or a private good also depends "on where you sit": see Wildavsky A, in Wildavsky A, ed. by Chai S-K and Swedlow B, 1998, "At once ubiquitous and elusive, the concept of externalities is either vacuous or misapplied", in Wildavsky A, 1998, *Culture and Social Theory*, Transaction Publishers, New Brunswick, New Jersey, 55-84. In any case, the argument can be stated without the assumptions involved here, and the usefulness of analogy between PETs and environment-protecting technologies or business ethics does not depend on making these assumptions about externalities and public goods.

11. One might assume, for the present purpose, that it can be solved by administrative means, such as managerial directive or by internal regulation within government. In practice this is not straightforward, as two generations of implementation research have shown. However, the experiment within the British National Health Service since the report of the Caldicott Committee will provide an invaluable case study against which to test the rival claims about the efficacy of administrative direction as a strategy for securing compliance with privacy compliance in the public sector: see Department of Health, 1997, *The Caldicott Committee report on the review of patient-identifiable information*, Department of Health, London: and see also the subsequent guidance and reports on implementation available at <www.doh.gov.uk/nhsexipu/confiden/>. It is too early as yet to evaluate

Now consider the nature of the challenge of persuading consumers to demand PETs. The key issue is the nature of consumer preferences. Not all consumers care to the same degree about privacy: some care about some privacy risks more than they care about others, some have more faith in the efficacy of technological protections against privacy risks than others and some have more faith in some technologies than in others. This means that the first thing we need to understand is how consumers are distributed in terms of their *risk perception* about a variety of privacy risks. That is to say, recognition of risk drives consumers' desire for protection. Moreover, in order to understand the scope for persuasion, we need to know how open to influence and change risk perceptions about privacy are.

In a market in which the price charged for those products and services in which PETs are embedded is higher than the price of those in which they are not (a "worst case" assumption that we can well follow in order to make the argument most widely useful), the consumer must decide how much (s)he values the kinds of privacy that the service offers protection for, against the actual size and cost of the price increment. The second thing we need to learn about consumers, then, is how preferences for protection against various kinds of privacy risk are *traded off* against price increments. If these trade-offs are to be influenced, presumably then (unless someone has a new idea about how to increase consumers' levels of discretionary income without causing corresponding price inflation!) the only way in which to persuade people to be willing to pay more for privacy protection is to increase the seriousness with which they take privacy risk in the first place.

In the unlikely event that the market were perfectly competitive and consumers could (nearly) costlessly find and move between suppliers, consumers would sort themselves by their preferences and their willingness to pay for goods and services according to the trade-offs between privacy "quality" and price that they are prepared to make, with the information that they can (in a perfectly competitive market) acquire about the privacy protecting characteristics of rival services at negligible cost. In many real markets, of course, there are real costs for consumers of search, information acquisition and checking and of exercising mobility between suppliers — further there may be oligopoly or other limitations upon the range of services available to be chosen between, and companies may offer misleading information about the privacy-protecting characteristics of their services. The third thing, then, that we need to learn about, is how consumers value the *transaction costs* — which may not all be monetised, but may be expressed in terms of lost time — of search, checking and mobility.

---

the lessons from this experience. In practice, many of the considerations that apply to the account of the openness of businesses to persuasion also apply to government agencies, but with some complex differences that cannot be explored here. For an overview of the constraints and incentives for frontline staff not to internalise costs that the centre might like them to, see Lipsky M, 1980, *Street Level Bureaucracy: Dilemmas of the Individual in Public Services*, Russell Sage Foundation, New York. On the general issues of implementation challenges of using managerial direction to induce subaltern agencies to internalise costs, see Bardach E, 1977, *The Implementation Game*, Massachusetts Institute of Technology Press, Cambridge, Massachusetts. Those interested in the difficulties of using internal regulation should consult, *e.g.* Hood C, Scott C, James O, Jones G and Travers T, 1999, *Regulation Inside Government: Waste-Watchers, Quality Police and Sleaze-Busters*, Oxford University Press, Oxford. At least in theory, if public sector agencies were to offer services that provided better respect for privacy and made greater use of PETs, this might raise consumers" expectations and increase their familiarity with the technologies, which might have spillover effects into their behaviour vis-à-vis the commercial bodies with which they deal, and through public purchasing of services from the private sector, there might be supply-side influences too. However, the history of, for example, equal opportunities practices in the public sector suggests that we might want to be cautious about the speed and the strength of these spillover effects, and their robustness to shocks and their power to overcome the resistance of countervailing commercial and institutional pressures.

Persuading businesses

Why should businesses internalise costs that they might otherwise externalise, and that they might fear that their competitors might externalise if they internalise them? In general, there are four basic types of situation in which businesses might have reasons to do this which can be grouped under two general headings. The first group consists in situations in which businesses are given *sanctions* and *incentives* to internalise those costs, and the second comprises situations where there are *constraints* upon them that make it difficult for them to think of choosing not to internalise the costs.

Sanctions and incentives

1. *Fear*: Here, businesses fear that if they do not internalise the costs and invest in PETs, they will face sanctions from regulators. If there are standards for PETs created by national and international standards bodies, for example, they will adopt those standards because the standards can be used in signalling to the regulators that they are acting in the ways that regulators demand, and so they can create a reputation with regulators for their commitment to the values for which the regulators call.
2. *Hope*: In this situation, at least some groups of consumers of importance to the business demand PETs in the design of their services or products, and therefore investment in PETs can represent competitive advantage vis-à-vis rival firms in seeking the business of those groups of consumers. Here, adopting PETs standards serves a signalling function toward and helps to create a reputation with those groups of consumers.

Constraints

1. *Habit*: In this situation, for businesses within a particular industry or niche in that industry, the use of PETs has become the norm, and, independently of any incentives or sanctions, they are adopted and the costs internalised because all competitors do this as a matter of implicit routine, and they are no longer conceived as a separate issue. The habit in effect limits the "thinkability" of not using them.
2. *Unavoidability*: Here, PETs become embedded in other products and services that have to be used because there are no alternatives to using at least one of them. For example, product standards might specify PETs have, in this situation, become universally adopted. Typically, this situation arises in cases of technological path-dependency, where, independently of any competitive advantage or regulatory pressure, certain technologies achieve "lock-in" — to use some other systems becomes impossible in part because the power of expectations and the power of costs of change for businesses and consumers are now too great, so institutionalised has the technology become and so established is the infrastructure around it.[12]

For the present purposes, we must — unfortunately — ignore habit and unavoidability, for as historical studies on the lock-in of the QWERTY keyboard and the internal combustion engine have shown, there is no direct route to the habituation or unavoidable ubiquity of a technology that does not

12. Arthur B, 1990, "Positive Feedbacks in the Economy", *Scientific American*, Feb, 92-99; Rosenberg N, 1994, *Exploring the Black Box: Technology, Economics and History*, Cambridge University Press, Cambridge; David PA, 1985, "Clio and the Economics of QWERTY", *Economic History*, 75, 2, 332-337; Pool R, 1997, *Beyond Engineering: How Society Shapes Technology*, Oxford University Press, New York, ch.5.

first pass through the dynamic pressures of hope and fear. All habits and innovations are new at some point, and to survive the "liability of newness", they must be adopted explicitly at first and on the basis of some balance of hope and fear.

However, situations in which hope and fear can motivate the internalisation of costs that rivals might externalise are not universal, but are to be found in quite distinct types of sectors. For the same reasons that explain their particular distribution, combining the powers of hope and fear is also far from straightforward.

Consider situations first in which fear of regulatory sanctions is most likely to be effective. Regulators are, of course, most effective in the most regulatable sectors of the economy. These are typically the most stable, because the costs to regulators of acquiring information about such free riding behaviour as exploitation of consumers' privacy are very great in highly volatile, highly competitive sectors.[13] Moreover, in markets and sectors where companies appear, disappear and reappear in new guises with bewildering speed, enforcement is difficult for regulators.

In those market sectors where consumers cannot readily know whether their privacy is being respected, perhaps because they are not aware that those industries possess much information about them (or perhaps because they are not aware that certain kinds of information about themselves is in fact highly valuable, because it may provide excellent predictors of other kinds of information), there are many more opportunities for firms to exploit personal information unscrupulously without the detection of regulators who often rely upon consumers to alert them of violations.

Markets and sectors differ in the degree to which they exhibit institutionalised arrangements for sharing information around the market about what other firms are doing to create good and bad reputations for firms and for senior executives. Those sectors without such institutionalised information sharing systems offer more opportunities to the less scrupulous firms to evade the not-so-long arm of the regulator.

However, the economic characteristics of markets are not the only features that make for ease of regulation. The degree of scrutiny by pressure groups including consumer pressure groups concerned with privacy issues also matters. Those industries to which these groups choose to devote their scarce resources are thereby made easier to regulate, because the pressure groups bear some of the costs of acquiring information that would otherwise fall to regulators.

The internal institutionalised characteristics of firms also matter greatly. Firms where leaders are committed to consumer privacy are more likely to have institutionalised controls to ensure that PETs are used, to support whistleblowers who would report violations, and to be willing to co-operate with regulatory requests for information. However, these institutionalised characteristics are not randomly distributed: commitment to such controls will appear where it makes sense to do so, and this sense-making differs according to context, including market niche.[14]

Now consider those sectors in which hope-based strategies might work to discipline businesses to invest in PETs. Hope rests essentially on consumer demand, which we shall consider in more detail in

---

13. On the information asymmetry between regulators and the regulated in favour of the latter, see Klein RE and Day P, 1987, "The regulation of nursing homes", *Milbank Quarterly*, 65, 3, 303-347.

14. For a discussion of sense-making, which shows that it is not simply a reflection of instrumental economic calculation, see Weick KE, 1995, *Sensemaking in Organisations*, Sage, London and Weick KE, 2001, *Making Sense of the Organisation*, Blackwell, Oxford.

the next section. However, whatever one's account of how consumers differ from one another in the importance they attach to privacy in general, and to protection against different particular privacy risks, it is generally recognised that some consumers have preferences that, if businesses can profitably attract those consumers, might leave those businesses more open to persuasion that PETs are worth investing in than otherwise. The key questions for hope-based strategies are these: how big is the constituency of consumers who want any of the available kinds of PETs, how much are they prepared to pay, and how costly will it be for businesses to attract them?

The field of environmentally sensitive consumption may provide a good analogy here. Research on the "green consumer" trend, and on the take-up of composting of household organic waste, recycling, use of "fair trade" coffee and tea, minimal packaging, willingness to use organic whole food co-operatives for groceries, and other environmentally protective consumption behaviours has shown that these are classical niche markets. That is to say, a modest number of people with very intense preferences can sustain a small market with many small firms, but there are limits to the scope that these markets exhibit for growth, because although other consumers would be interested in some of these products, either the price differential puts them out of their reach, or the transaction costs of time and effort are too great.[15] Unless these products represent good value for money, and unless environmental preferences are very strong, demand is limited, and even modest price incentives have only marginal effects.[16] Just occasionally demand for such products can be increased by powerful marketing, where a large and powerfully branded company is prepared to adopt these products as a way to internalise the costs. For example, supermarket chains in the United Kingdom and continental Europe have expanded demand for GMO-free and organic foods, at least for a while, but even here they have had difficulty in sustaining this, and households on lower income still find these products unaffordable. Research on "buycotts" — that is to say, positive campaigns by consumers with very intense preferences to buy only goods and services where suppliers have internalised certain costs to offer desired features even at a premium — suggests that they are few in number,[17] that they rarely work in eliciting positive supply response on a really large scale without powerful backing of fear-based factors such as the regulatory action to prohibit alternatives,[18] and that they are very difficult to sustain especially where demand is essentially niched and where there is an unfavourable price differential.

This suggests that the key question about services with PETs is whether demand for privacy is like demand for eco-friendly products, or whether it is something that attracts wider consumer commitment, especially where there are unfavourable price differentials between services using PETs and those which do not. I shall consider the evidence in more detail in the next section, but most surveys suggest that very intense preferences for privacy that lead consumers to be willing to pay price

15. On the high transaction costs of time and effort that have limited willingness to engage, for example, in home composting, see Åberg H, Dahlman S, Shanahan H, and Säljö R, 1996, "Towards Sound Environmental Behaviour: Exploring Household Participation in Waste Management", *Journal of Consumer Policy*, 19, 1, 45-67.

16. Bech-Larsen T, 1996, "Danish Consumers" Attitudes to Functional and Environmental Characteristics of Food Packaging", *Journal of Consumer Policy*, 19, 3, 339-363; Thøgerson J, 1999, "The Ethical Consumer: Moral Norms and Packaging Choice", *Journal of Consumer Policy*, 22, 4, 439-460; Thøgerson J, 1994, "Monetary Incentives and Environmental Concern: Effects of a Differentiated Garbage Fee", *Journal of Consumer Policy*, 17, 4, 407-442.

17. Friedman M, 1996, "A Positive Approach to Organised Consumer Action: The "Buycott" as an Alternative to the Boycott", *Journal of Consumer Policy*, 19, 4, 439-451.

18. Neuner M, 2000, "Collective Prototyping: A Consumer Policy Strategy to Encourage Ecological Marketing", *Journal of Consumer Policy*, 23, 2, 153-175 at 172.

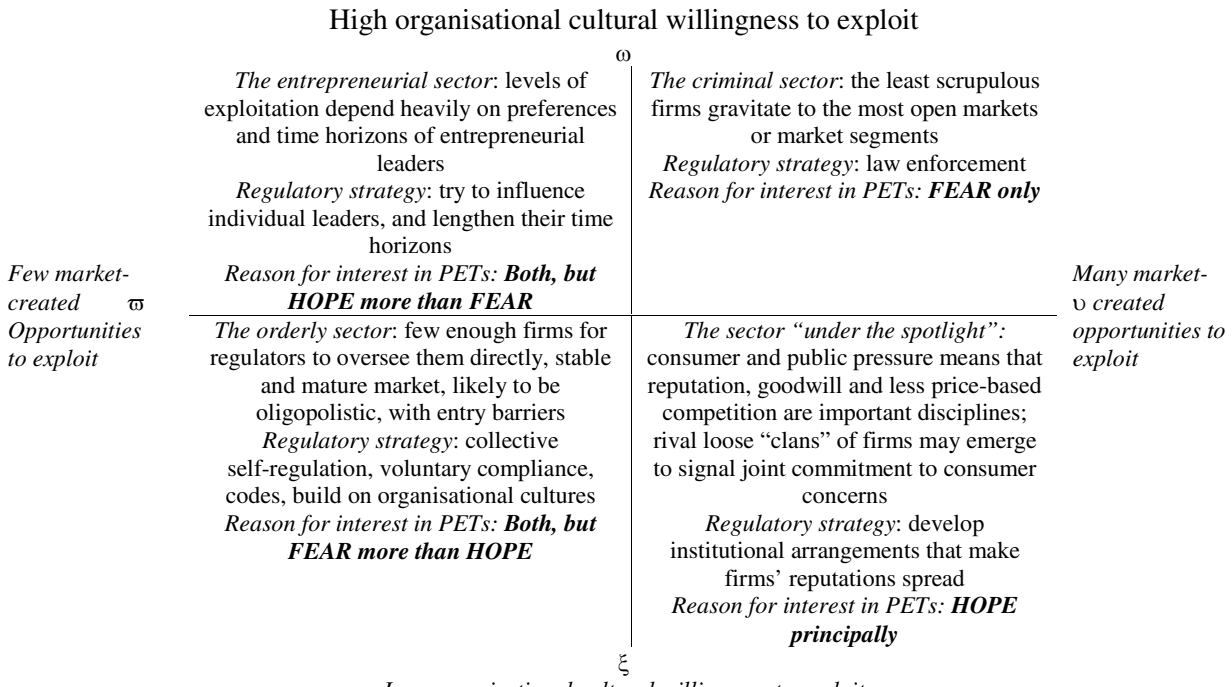
premia over prolonged periods are probably a minority taste in most countries, but that there are certain goods and services around which those preferences cluster more than others. In particular, because so many people regard as uniquely "sensitive" data about their health and their finances, there may be more widespread willingness to pay a premium for services using PETs in such industries as financial services, insurance and medical care than elsewhere.

These are all simply cases of the problem of persuading companies to internalise costs that they fear their rivals might gain competitive advantage by externalising, and the balance of hope and fear in that persuasion. A good summary of this argument that the drivers of fear and hope (that might lead companies to internalise costs that they might fear that their rivals might externalise) are unevenly distributed across the economy, is provided by the business economist S. Prakash Sethi, writing with Linda Sama.[19] In their account of the differential pressures on business to behave ethically, quite generally, Sethi and Sama identify a number of strategies for regulators seeking to persuade businesses to internalise costs, that might make sense in each of these situations. Figure 1 below is, I hope, a reasonably faithful gloss or adaptation of their graphical representation of this analysis of the problem, although the titles of some of the sectors and the balancing of hope and fear factors are my own.[20] These authors structure the nature of these different situations along two intersecting dimensions describing the distribution of incentives. These two dimensions are the degree to which organisations' own internal institutions militate against consumer exploitation and the degree to which the organisation of the market creates opportunities for exploitation.

19. Sethi SP and Sama LM, 1998, "Ethical Behaviour as a Strategic Choice by Larger Corporations: The Interactive Effect of Marketplace Competition, Industry Structure and Firm Resources", *Business Ethics Quarterly*, 8, 1, 85-104.

20. I have made one change of a substantive nature to the Sethi and Sama analysis. I have renamed and amended the analysis of the sector described by the quadrant with low willingness to exploit but many opportunities to exploit. Although I have followed them in deriving from the characteristics of its location, the importance here of consumer pressure, reputation and good will, I have dropped their stress on certain other factors. In Sethi and Sama's account, this is described as the "high growth" sector, associated with what they call the middle stage of the technological and product cycle, before innovative products have yet reached mass markets. However, these features seem to be highly contingent: in many niche markets which the basic structural position on these dimensions describes, indeed, high growth and readiness for mass markets do not seem to be observed. I have tried to focus on those features that follow logically or causally from the structural position on the two dimensions.

Figure 1. **The institutional situation of businesses shapes their openness to persuasion**
(adapted from Sethi and Sama, 1998, 93)

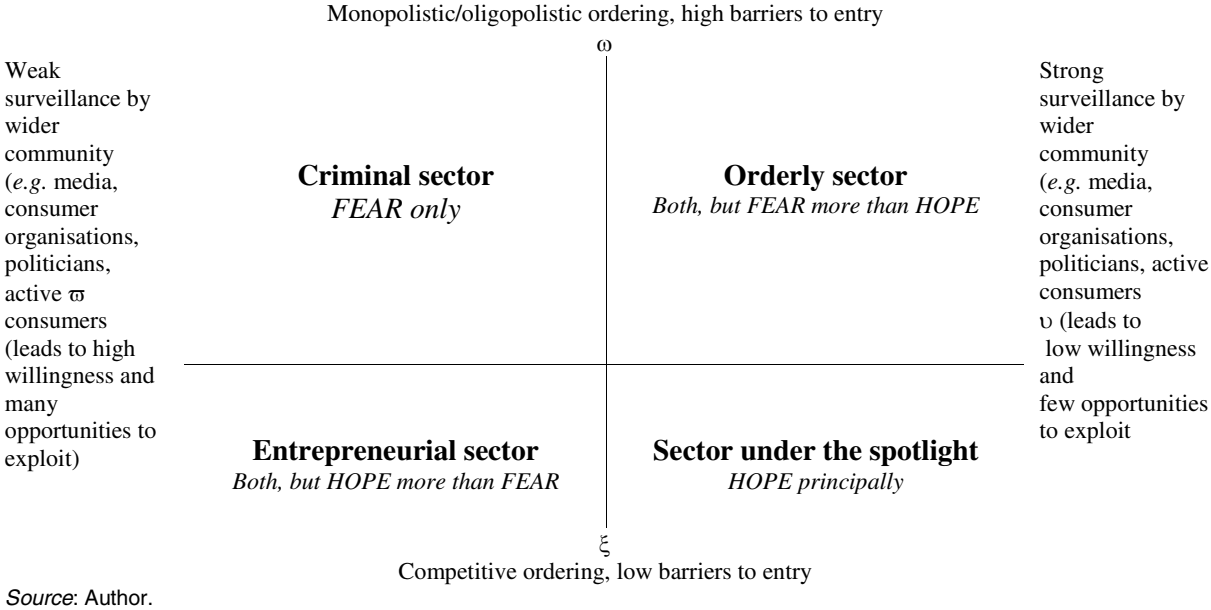


It will be important for the argument in the next section to see that this matrix can be rearranged, using slightly different dimensions. The extent of opportunity and the extent of willingness to exploit are not settled or caused wholly independently, on institutionalist accounts of the origins of preferences: indeed, willingness and preferences often emerge and become definite partly in response to what are perceived as opportunities.[21] Behind both of the two Sethi and Sama dimensions is the extent to which surveillance by the wider community disciplines both the ability and the willingness of businesses to exploit, for it is in the sectors in which there is less surveillance due to the costs of its exercise, that the least scrupulous gravitate, and where they are cultivated, for the sense of being under surveillance acts as an institutional pressure that induces willingness to restrict exploitation and that limits opportunities. Now, we can helpfully introduce a dimension that is implicit in the Sethi and Sama analysis, namely, the degree to which the market ordering is structured by monopoly or oligopoly with barriers to entry — creating something akin to a kind of authority within the market — at one end of the spectrum, and, at the other, the degree to which it is organised by relative openness to competition with free barriers to entry. This measure of the structure of markets also indicates the nature of the ways in which surveillance is mediated. Where there is oligopoly and there are high barriers to entry, direct consumer power is attenuated; conversely, where there is greater openness,

21. For an institutionalist account of the dynamics of markets which explains the production of preferences as well as the structure of opportunities in the same process, see Douglas M, 1986, *How Institutions Think*, Routledge and Kegan Paul, London; Powell WW and DiMaggio PJ, eds, 1991, *The New Institutionalism in Organisational Analysis*, University of Chicago Press, Chicago; Thompson M, Ellis R and Wildavsky A, 1990, *Cultural Theory*, Westview Press, Boulder, Colorado; see also Wildavsky A, 1994, ""Why Self-Interest Means Less Outside of a Social Context: Cultural Contributions to a Theory of Rational Choices", *Journal of Theoretical Politics*, 6, 2, 131-159, repr. in Wildavsky A, 1998, *Culture and Social Theory*, ed Chai S-K and Swedlow B, Transaction Publishers, New Brunswick, New Jersey, 231-258. esp. at 251ff.

direct consumer power can — depending on the other variable of surveillance — have more weight. Cross-tabulating these two dimensions enables us to produce exactly the same analysis of sectors as Sethi and Sama. However, rearranging the matrix in this way will turn out to be very important in examining the relationship between the differential openness of differently situated businesses to persuasion and the differential openness of differently situated consumers, for it will enable us to map the situation of businesses in a way exactly comparable to that which will be introduced for consumers. This transposition of the classification of situations that make for differential openness to persuasion, yields Figure 2.

Figure 2. **Transposition of Figure 1**



Source: Author.

What kinds of PETs are firms in each of these sectors of the economy (faced with these structural pressures from the market, consumers and wider publics and regulators) most likely to be open to persuasion to using?

In order to answer this question, we need a classification of PETs, in the wide sense used in this paper and defined in the introduction. There are of course a great many in use, but for the present purpose, we need a classification by function — that is to say, by the category of risk against which the PET offers protection — rather than by technological type.[22] For it is function that is of the first concern to businesses, although cost will of course come a close second. Figure 3 presents such a functional classification.

22. The recent OECD study offers what is, in the terms used here, a technological classification (at para 2) and a functional classification (at para 12). Closest to the present risk type approach is what the OECD study calls "policy effect" (at para 12): Working Party on Information Security and Privacy, 2001, *Appendix 2: A Study of Privacy-Enhancing Technologies*, Directorate for Science, Technology and Industry, Organisation for Economic Co-operation and Development, Paris.

Figure 3. **Functional classification of types of privacy-enhancing technologies (PETs)**

PETs might be designed to carry out any of the following functions:

1. *Notification*: provide for notification of collection, identity of data controller, nature of use, disclosure etc.
2. *Consent*: allow for consent prior to collection by:
   a. Opt-in, or by
   b. Opt-out mechanism.

   Which may be for:
   i. Any collection.
   ii. Collection of defined categories (*e.g.* categories deemed particularly "sensitive").
3. *Collection type limitation*: limit quantity or type of information collected by some rule independent of consent, and typically by some coding which is defined by the legitimate purpose.
4. *Collection context limitation*: limit contexts in which information can be collected to those falling under defined descriptions (defined independently of consent, and perhaps by legitimate purpose).
5. *Subject access*: allow subject access.
6. *Data change opportunity*: allow subject access and
   a. Request for correction.
   b. Request for deletion of excessive and irrelevant information.
   c. Request for complete deletion of their individual record.
7. *Alerting*: introduce "tripwires" in the use of information *e.g.* "stop and think", "stop and check" instructions before using information:
   a. For certain purposes.
   b. To carry out certain types of inference *e.g.* about derived classifications, marked as suspect for certain offences.
8. *Identification limitation*: limit identifying presentation: *i.e.* limit capability to identify the individual from the information available to non-authorised persons through the use of pseudonymity, and/or blocking out of other key collected information.
9. *Destination limitation*: limit by rule the possibilities of disclosure destination, *e.g.* prevention of copying of data.
10. *Information*: notify data subject of rules, codes, etc. accepted by data controllers governing collection, purpose, actual uses, disclosure, and of any available redress, internally or to public regulatory authorities.

Source: Author.

The next stage in the argument is to work out what the relative cost implications of each type of PET might be. What matters here is not the initial purchase price, but the long run economic costs of running a data management system subject to the constraints that a type of PET imposes, where one examines the implications for the basic business model as well as the implications for administrative costs. It is not possible to say very much about relative differentials in the long run projected costs of technologies that would perform these tasks, since over the medium term those costs are in part dependent on the level of demand for them: greater demand would typically in the short term increase prices, but as supply response builds up and as investment costs are recouped, prices are likely to fall in the medium to long term. Cost over the long run is in part a function of the size of the customer base, the value of the services in which the PETs are embedded, and the longevity and value of the relationship with the consumer. However, it seems reasonable to suppose that, in the short run, those systems that involve the greatest change to existing data management practices are the ones that are most likely to represent the highest total costs to businesses. Over the long run, the integrity of the data set (its adequacy in covering the people the business wants to reach, and the consistency of the data held about each person) determines the use that can be made of it. Therefore, when PETs impact on these things, we should expect the greatest true economic (opportunity) costs to arise from them, even if the greatest cash accounting costs do not show up here.

On this basis, therefore, we should expect that the cheaper PETs to implement will be those that would provide staff with alerting (7), or that would provide consumers with information (10). These involve no major changes to standard designs of databases. Into the next band might fall subject access

systems (5) and those that would provide individual level notification (1). Secure online real time subject access is expensive, but when many more services are being provided online in any case, the marginal additional cost may typically not be too great. Identification presentation limiting systems (8) may be costly to retrofit, but are negligibly more costly to design into new systems, and not always particularly expensive to operate thereafter, depending on just who is locked out of identifying information and how much inconvenience this causes them. However, this does involve substantial additional complexity in the basic design of a database, and in the rules governing retrieval and reports that can be run upon it, etc. Systems that allow individual level data change requests (6) are costly to operate, because they involve a lot of individual record level work some of which cannot be fully automated, although it can reduce other costs that would arise from inaccuracy (although secure real-time online subject access involves individual level display, it does not involve individual level authorisation for change). Most expensive are those technologies that could threaten the coverage of the database that a company wants to assemble — such as technologies supporting consent (2), limitation of collection (3) and (4) — and those that could disrupt plans for commercial relationships — such as destination limitation (9). Figure 4 summarises this very rough hypothesised banding. I accept, of course, that this is very rough and very provisional. However, if a better banding can be offered, it could be used in much the same way as this will be used in the argument that follows, without disrupting the basic argument of the paper.

Figure 4. **Suggested rough cost bands for PETs**

Band	Type of PET
A: cheapest	7: alerting, 10: information
B	5: subject access, 1: notification
C	8: identification presentation limitation
D	6: data change request
E: most expensive	2: consent, 3, 4: collection limitation, 9: destination limitation

Source: Author.

To some extent, it is clear, the hot breath of consumer preferences on the necks of companies in different sectors will shape their openness to persuasion to invest in different kinds of PETs. These will be examined in detail in the next section: however, for the present, the following assumptions can reasonably be made.

1. *Criminal sector*: Here "criminal" is a term of art: we are concerned only with those firms that unscrupulously ignore privacy. Many businesses supplying illegal products are highly responsive to consumer preferences about both products and privacy: illegal businesses supplying illicit drugs are highly responsive to changes in tastes for drugs and respect consumers' privacy very carefully. However, the present concern is only with businesses prepared to use methods of personal data handling that are illegal, so in this sector, by definition, consumer preferences specifically for privacy have little impact. Such firms may well of course not be engaged in any other illegal activity.
2. *Orderly sector*: Here consumer preferences are quite powerful, but the stability and oligopolistic nature of the market mean that they are often more powerfully refracted through regulatory action (fear) than directly (hope).
3. *Entrepreneurial sector*: Here firms are small and mobile enough to be able to sort themselves according to their understanding of the segmentation of consumers, and so those that want to respond to those consumers with strong privacy preferences will find ways to situate themselves to signal their responsiveness to those consumers, and those which are

less scrupulous will search for niches where either they can serve consumers less concerned about their privacy, or else where their data handling practices will not be so obvious to consumers.

4. *Sector under the spotlight*: Here consumer preferences about privacy are likely to be at their most powerful, and most powerfully amplified through consumer and human rights movements, as well as influencing ways in which regulators allocate their attention. The ways in which firms will form loose "clans"[23] — using, for example, trust seals (such as BBB Online, Truste™ and Trust UK) — to display their joint commitment to privacy issues, will also provide consumers with important signals and "hostages", increasing their exposure to consumer privacy preferences.

Trade associations may act as forces for compliance with privacy standards and for the use of PETs, sometimes almost as regulators, and sometimes as "clans". In either of these cases, however, we should expect their ability to attract members to be greatest in the orderly sector and in the sector under the spotlight. Ideally, one might want such trade associations to be most effective in the small and medium-sized enterprise sectors — which would be distributed between the entrepreneurial sector and the sector "under the spotlight" — for these firms are the ones likely to have the fewest resources to afford the costs of search, evaluation, adoption and learning the use of PETs. However, their ability to attract members in the entrepreneurial sector is typically lower, for here the competitive pressure of fear that rivals will externalise costs is greatest.

Taking together these considerations of the different functions PETs can serve, suggested bandings of cost differentials and the different pressures that firms in the four different sectors face, we can offer the following hypothesis as to which sectors will feature firms most open and least open to persuasion about each type of PET. The key issue is how far down the hierarchy of costs bands for PETs businesses in each situation might be prepared to go. Figure 5 sets out the hypothesis that emerges from the application of the framework set out in Figure 2 to the cost banding set out in Figure 4.

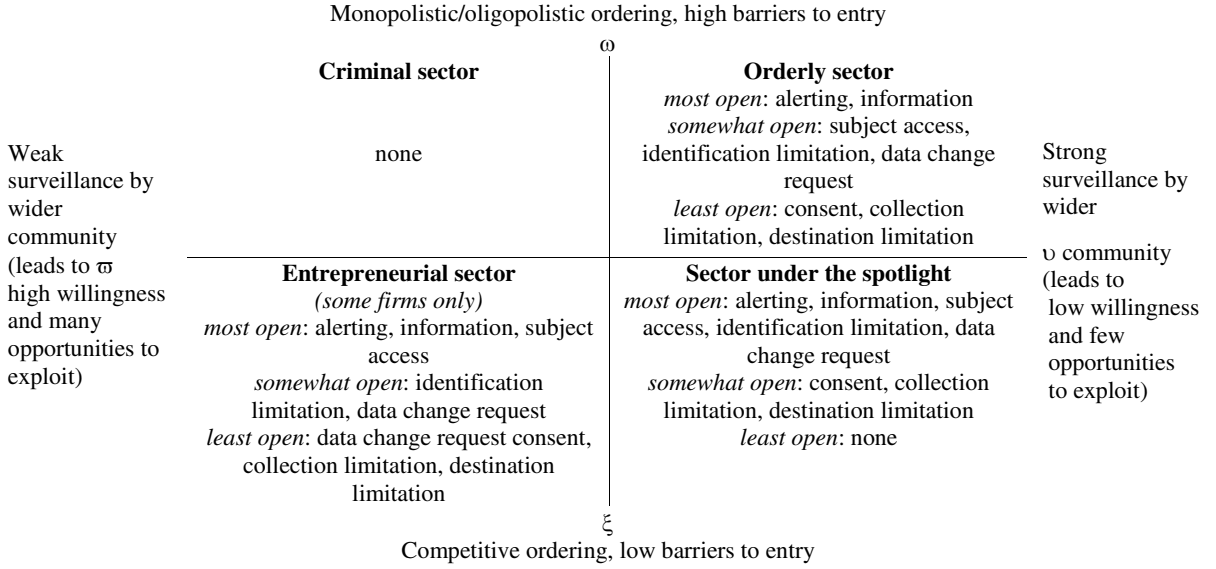
If the argument so far is accepted, then what does it suggest should be the strategy of data protection regulators, government departments with policy responsibility for oversight of the business community's data management practices, and for consumer and human rights social movements concerned with privacy in the commercial sector, and self-regulatory bodies ranging from trade associations through to privacy seal bodies, in attempting to persuade businesses to invest in PETs?

The first strategic issue is whether to focus scarce resources available for persuasion upon the businesses that are easiest to persuade — which are of course likely to be the ones least likely to exploit consumers in any case — or on the most difficult to persuade. In theory, this is a difficult social policy choice because it requires the balancing of urgency against feasibility, but in practice, government bodies invariably decide on the first course of action: feasibility wins every time. Politically, the imperative to show "quick wins", the need to build up skills in persuasion and capabilities in gathering information from those being persuaded, and the fact that in a developed country with a basically law-governed system of capitalism, larger numbers of firms are open to some persuasion, means that there is little choice but to focus on those who are easiest to persuade, even though the worst risks arise in connection with the most difficult to persuade. It is on this assumption, presumably, that Sethi and Sama's general advice to regulators is based (see Figure 1).

---

23. Ouchi WG, 1980, "Market, Bureaucracies and Clans", *Administrative Sciences Quarterly*, 25, 2, 120-142.

Figure 5. **Relative openness to persuasion to invest in types of PETs by sector**



Note: In this figure, "most/somewhat/least open" means "most/somewhat/least open to persuasion to invest in the following types of PETs" by comparison with *other types of PETs*. I assume that the cost bandings between types of PETs set out in Figure 4 are the same between sectors, and so the general ordering is the same. However, in some sectors, the willingness to internalise the costs of the most expensive costs bands of PETs should be expected, on this account, to be greater than in other sectors.

Source: Author.

As Sethi and Sama note, with the criminal sector, the only really persuasive force is law enforcement: here, hope has little grip and fear is the only persuasive tool available to government agencies.

There has been a great deal of development of formal training programmes for businesses in privacy protection: law firms, management consulting houses, privacy trust seal groups, professional networks of chief privacy officers and dedicated specialist data protection consulting advisory agencies have developed such programmes in many countries. The account of openness to persuasion offered here would suggest that these formal training structures are most likely to be of use in the *orderly* sector, where stable market shares, mature markets and technologies and hierarchical and bureaucratic systems of data management are most likely to be found. Secondly, these means of persuasion should attract at least some interest in the sector *under the spotlight*, where specialist compliance officer roles may not be expected to exist, but where a variety of personnel with data management roles might be attracted by formal training. The greater interest of these sectors in such support follows from their greater exposure to surveillance. However, in the entrepreneurial sector, this rather bureaucratic approach is much less likely to be successful. If there is interest in these training programmes from the criminal sector, it will usually be from law firms that act for these companies or else from managers interested only in using what they learn on such courses to work out better ways of disguising their sharp practices.

With firms in the *entrepreneurial* sector and perhaps some in the small-firm-dominated industries in the sector *under the spotlight*, much more informal techniques of delivering information for persuasion are more likely to be effective than formal training. In the entrepreneurial sector, we would expect that looser, more individualistic structures such as casual networks would be more appropriate. These may have some appeal in some parts of the sector under the spotlight, but in that area, working

though the clan-like systems to develop commitment to PETs as part of the "membership criteria" for trust seal clubs and other reputation-enhancing and consumer-signalling institutions is more likely to be effective.

PETs could perhaps be introduced, as it were, by stealth, by marketing a technology and tool to businesses purely on the basis of its data processing functionality, so that its introduction does not alarm those businesses that might otherwise be concerned about the cost implications of supporting consumer privacy, by suggesting that these are simply the normal running costs of handling data about consumers. This is achieved by embedding PETs in a variety of products without necessarily making a great deal of noise about the privacy-enhancing aspects. The aspiration behind these strategies is to obviate the need for persuasion in order, it is hoped, to proceed directly to unavoidability or at least habit. It is, I have noted above, unlikely that such manipulative techniques are likely to be successful for very long. However, this is a very different thing from routine creation of agreed product and process standards through the national, European and international standards authorities for management, organisational and operational processes for ensuring best practice in data protection privacy including the use of PETs. This has been extensively debated at European level, but appears to be on ice at least for the time being, due to business opposition.[24] However, the Canadian Standards Association adopted such a standard in 1996 - (in Canada, unlike other countries, it appears that the small business lobby appears sometimes willing to support regulation that their counterparts elsewhere would not, where they believe that it helps create a more level playing field between their members and big businesses). However, the decisions of at least the first businesses to adopt a proffered standard reflect persuasion: only when only the last few laggards are left on the conventional "S"-curve that economists use to model the rates of adoption of innovations,[25] can unavoidability be relied upon to secure adoption without persuasion. The development of PETs standards is something that should be understood, not as a persuasive strategy for regulators in its own right, but as a way of supporting the very different hope-based business strategies of firms in each of the three non-criminal sectors.

This completes the account offered in this paper of the openness of businesses to persuasion to internalise the costs of PETs that they might fear their rivals might externalise, the types of PETs each sector is structurally most open to persuasion about, and the means by which such persuasion might most effectively be delivered within each sector. The next section will examine the variations in the situations of consumers in order to explore how consumers and businesses in different situations face one another.

---

24. CEN, the European Standards Institute, put out a first version of a consultation paper on precisely this. However, the revised version recommended that management standards should not, after all, be initiated but that developments in the International Standards Organisations and other bodies should be monitored, and that the only work to be taken forward should be on contract terms and on criteria for Web-based privacy seals, and to produce a further report on PETs: see *Comité Européen de Normalisation* (CEN: European Committee for Standardisation), 2001, "Initiative on privacy standardisation in Europe (IPSE): Discussion draft - report by Project Team for the second CEN Information Society Standardization System (ISSS) Data Privacy Open Workshop, Paris 27th September 2001", CEN, Brussels, available at www.cenorm.be/isss.

25. See *e.g.* Gomulka S, 1990, *The Theory of Technological Change and Economic Growth*, Routledge, London, ch. 6, esp. 93.

Persuading consumers

It was argued above that, in order to understand which consumers will want the kinds of privacy protection that embedded technologies can offer, we need to understand the differences between consumers in respect of their:

- *Risk perception:* differences between perceptions of privacy risk, and how open to influence those perceptions might be.
- *Price-sensitivity:* how preferences for privacy are traded off against price differences between services that use PETs and services that do not.
- *Transaction costs:* how consumers differ in their willingness to bear the sometimes non-monetary transaction costs of search, mobility between providers, and making available their own time and effort to use the privacy protections afforded (*e.g.* actually invoke subject access rights or request corrections), and how these might differ between market situations with more and less competition.

I have reviewed elsewhere the literature on privacy risk perception,[26] in order to argue that the conventional segmentation of the population into a small group of the "unconcerned", a tiny group of privacy "fundamentalists" and a large group of privacy "pragmatists" is in fact seriously misleading.[27] In the first place, risk perceptions change according to context[28]: they are not the applications to privacy of stable underlying psychological types. Secondly, the category of pragmatism is too vague and too capacious to be a useful one (many surveys using this concept find between two thirds and three quarters of the population to fall under it!), and it tends to lead businesses into a misplaced complacency that they can always offer consumers enough that they will then cease to care about privacy issues. It is also a problem that this taxonomy bears no relationship to the ways in which we understand people to think about other risks or other consumption relationships and practices. It would be very odd indeed if people thought differently and sorted themselves quite differently in relation to concerns about their privacy from the ways in which they think and sort themselves in relation to almost any other concern. This taxonomy is also very static. It offers no way of thinking about how people's responses might change as their relationship with businesses and government changes. Finally, it is a major weakness of the unconcerned-pragmatist-fundamentalist taxonomy that it offers no explanation of where these categories come from, or just why anyone might come to think about their privacy in one of these ways. "People's mind sets are just like that" is not an explanation at all, still less one that is very helpful to regulators or to businesses who want to understand who might be open to what kinds of persuasion about what kinds of risks, opportunities and safeguards.

If we are to look for an approach that recognises that there are shifts according to context (albeit that some shifts are much more difficult than others), that is more precise, that does not induce misguided complacency, that recognises dynamism, that is grounded in some explanation of risk

---

26. 6 P, 1998 with Lasky K and Fletcher A, 1998, *The Future of Privacy, Vol. II: Public Trust in the Use of Private Information*, Demos, London.

27. Equifax 1995, *The Harris-Equifax Mid-Decade Consumer Privacy* survey, Equifax, Atlanta, Georgia; Henley Centre for Forecasting, 1995, *Dataculture: Privacy, Participation, and the Need for Transparency in the Information Age*, Henley Centre for Forecasting, London; Direct Marketing Association and Informix, 1997, *The new information trade*, Direct Marketing Association and Informix, London.

28. C.f. Sniderman P, 1993, "The New Look in Public Opinion Research", in Finifter AW, ed, 1993, *Political Science: The State of the Discipline II*, American Political Science Association, Washington DC, 219-245 at 233.

perceptions come from, and that is better integrated with what we understand to drive the ways in which people think about other concerns, then it makes sense to look beyond psychology. For, although psychological research on the perception of risks can tell us quite a lot about the variety of biases we can observe,[29] it has mainly offered accounts of what are claimed to be typical heuristics, rather than ways of thinking about differences and distributions, and it has had rather little to say about which biases will be exhibited by which people in which circumstances.[30]

It makes more sense to begin with an understanding of where and how people are situated in social organisation, in order to explain the perception of risks.[31] However, there is not an indefinite variety to the basic forms of social situation in social organisation in which people can find themselves,[32] and we can use a basic taxonomy of forms of social organisation to help us to understand how differences in risk perception about such things as privacy, will emerge and can be understood.

It may help to begin with some definitions of terms that will be used in this section to describe the situational factors that shape risk perception. By a person's "basic" or "primary situation", I mean the long term, underlying position that a person occupies in relation to the major institutionalised forces in their society, such as the labour market, the housing market, public services, key suppliers of goods and services, their peers as colleagues, friends and acquaintances, fundamental institutions such as religion, family organisation and the like. By "contexts", I mean the range of specific fields in which someone may yield up personal information about themselves, such as dealing with retailers, dealing with one's bank, dealing with one's physician, claiming a public service. It is the former which, on the view that I shall argue, is the really important factor, because it is this which shapes one's sense of identity, one's general outlook, one's capabilities, one's preferences and it does so by creating both constraints and opportunities and limiting accountability to institutions and to particular others. However, the primary situation is itself plural: we are differently situated in different contexts.

---

29. The psychometric tradition has been a fertile source of observation of the distribution of types of bias in risk perceptions — in short, it has been helpful in describing the dependent variable. For overviews, see Slovic P, 1992, "Perception of risk: reflections on the psychometric paradigm", in Krimsky S and Golding D, eds, 1992, *Social Theories of Risk*, Praeger, Westport, Connecticut, 117-152; Slovic P, 2000, *The Perception of Risk*, Earthscan, London; Kahneman D, Slovic P and Tversky A, eds, 1982, *Judgment under Uncertainty: Heuristics and Biases*, Cambridge University Press, Cambridge; Kahneman D and Tversky A, 2000, *Choices, Values and Frames*, Cambridge University Press, Cambridge. This approach has been developed in the recent work on "mental maps": see Morgan G, Fischhoff B, Bostrom A and Atman CJ, 2001 forthcoming, *Risk Communication: A Mental Models Approach*, Cambridge University Press, Cambridge; Bostrom A, Fischhoff B and Morgan GM, 1992, "Characterising Mental Processes of Hazardous Processes: A Methodology and an Application to Radon", *Journal of Social Issues*, 48, 4, 85-100, repr. in Löfstedt R and Frewer L, eds, 1998, *The Earthscan Reader in Risk and Modern Society*, Earthscan, London, 225-238; Jungermann H, Schütz H and Thüring M, 1988, "Mental Models in Risk Assessment: Informing People about Drugs", *Risk Analysis*, 8, 1, 147-155, repr. in Löfstedt R and Frewer L, eds, 1998, *The Earthscan Reader in Risk and Modern Society*, Earthscan, London, 213-224. For slightly different approach, see Renn O, "Three Decades of Risk Research: Accomplishments and New Challenges", *Journal of Risk Research*, 1,1, 49-71.

30. For a critique of these and other weaknesses, see Douglas M, 1985, *Risk Acceptability According to the Social Sciences*, Russell Sage Foundation, New York and Routledge and Kegan Paul, London.

31. This is an argument that is hardly controversial in anthropology and sociology, where since Durkheim and Evans-Pritchard, the sociology of knowledge has developed this argument.

32. Contrary to the post-modernists who hold that there is indefinite variation, entirely unanchored in the realities of social life.

For example, many of us have a quite different institutional relationship with our physician from that which we have with the supermarket we regularly use, and so we bring quite different thoughts styles to bear on our perception of privacy risk in relation to medical and retail data about us. By "secondary situation", I mean the much more short-run context of the particular conversations and interactions that a person may have with people who may deliberately or unintentionally try to persuade one to take a view of a privacy risk other than the view one would have, springing from one's primary situation. I shall argue that such psychological factors as personality traits tend to be shaped by the primary situation, modulated by context, rather than being independently caused and independently shaped by biases in the perception of risks.

Figure 6 presents a summary of the best-developed approach to understanding the perception of risks in general in recent social science. The figure presents a taxonomy of the basic varieties of primary situations which produce a basic and limited plurality of types of risk perception. This classification is produced by cross-tabulating two dimensions into a matrix. The dimensions are labelled using slightly more accessible descriptions of the two dimensions around which social science has circled since its inception. In 1897, Durkheim introduced these two concepts in order to understand how people's situation in social organisation shaped propensity to suicide. In "*Suicide*", he called what is here shown as the vertical axis, "social regulation", and what is here shown as the horizontal axis, "social integration".[33] They have been given various names since then, such as "grid" and "group" by the theorist who first presented this matrix.[34] Cross-tabulating them yields four basic types of social organisation, all of which will spring up in any human society. The basic types recur in economics as markets (individualism), hierarchies and clans (enclaves),[35] and the isolate category is

33. Durkheim É, 1951 [1897], *Suicide: A Study in Sociology*, tr. Spaulding JA and Simpson G, Routledge, London.

34. Douglas M, 1970, *Natural Symbols: Explorations in Cosmology*, Routledge, London; Douglas M, 1982 [1978], "Cultural Bias", in Douglas M, 1982, *In the Active Voice*, Routledge and Kegan Paul, London, 183-254. For the application to the perception of risk, see Douglas M, 1992, *Risk and Blame: Essays in Cultural Theory*, Routledge, London; Douglas M and Wildavsky A, 1982, *Risk and Culture: an Essay on the Selection of Technological and Environmental Dangers*, University of California Press, Berkeley; Adams J, 1995, *Risk*, UCL Press, London; Thompson M, Ellis RJ, and Wildavsky A, 1990, *Cultural Theory*, Westview Press, Boulder; Coyle DJ and Ellis RJ, eds, 1993, *Politics, Policy and Culture*, Westview Press, Boulder, Colorado; Dake K and Wildavsky A, 1993, "Theories of Risk Perception: Who Fears What and Why?", in Burger EJ, jnr, ed, 1993, *Risk*, University of Michigan Press, Ann Arbor, Michigan; Douglas M, 1990, "Risk as a Forensic Resource", *Daedalus*, 119, 4, 1-16; Douglas M, 1997, "The Depoliticisation of Risk", in Ellis RJ and Thompson M, eds, 1997, *Culture Matters: Essays in Honour of Aaron Wildavsky*, Westview Press, Boulder, Colorado, 121-132; Ellis RJ and Thompson F, 1997, "Seeing Green: Cultural Biases and Environmental Preferences", in Ellis RJ and Thompson M, eds, 1997, *Culture Matters: Essays in Honour of Aaron Wildavsky*, Westview Press, Boulder, Colorado, 169-190; Gross JL and Rayner S, 1985, *Measuring Culture: A Paradigm for the Analysis of Social Organisation*, Columbia University Press, New York; Thompson M, Grendstad G and Selle P, eds, 1999, *Cultural Theory as Political Science*, Routledge, London; Rayner S, 1992, "Cultural Theory and Risk Analysis", in Krimsky S and Golding D, eds, 1992, *Social theories of risk*, Praeger, Westport, Connecticut, 83-116.

35. Ouchi WG, 1980, "Market, Bureaucracies and Clans", *Administrative Sciences Quarterly*, 25, 2, 120-142. For a collection of papers on the three fold conception, see Thompson G, Frances J, Levačić R, and Mitchell J, eds, 1991, *Markets, Hierarchies and Networks*, Sage, London. The major early theoretical statements in economics on markets and hierarchies are contained in Coase RH, 1937, "The nature of the firm", *Econometrica*, 4, 386-405. A more recent major statement in Williamson OE, 1986, *The Economic Institutions of Capitalism*, Free Press, New York. See also Pitelis C, 1991, *Market and Non-market Hierarchies: Theory of Institutional Failure*, Blackwell, Oxford, and Miller

widely recognised in sociology and anthropology.[36] Essentially, the matrix presents a set of hypotheses that have been successfully tested in a wide variety of research about the relationships between situations and thought styles about risk in general.

These four basic types can be found in the ways in which consumers think about privacy risk too. In a recent qualitative study conducted for the UK government, I presented the following application of the taxonomy, in order to explain the distribution of attitudes to privacy observed in connection with proposals for and practices of sharing of personal data between departments and agencies in the public services in order to promote "joined-up" or holistic government (Figure 7).[37] Within each of the four basic outlooks on risks, in the context of the focus group conversations, it was possible to distinguish more moderate and more extreme forms of the ways in which these basic outlooks applied to privacy risk. The application of the basic outlooks yields "frames", or specific styles of thinking about privacy risk that are governed by an overarching concept.[38] Figure 7 provides a complete mapping of the eight available frames, produced by counting both the moderate and extreme forms of each of the four basic positions set out in Figure 6. Again, it should be remembered that many people will move between positions as they move between contexts.

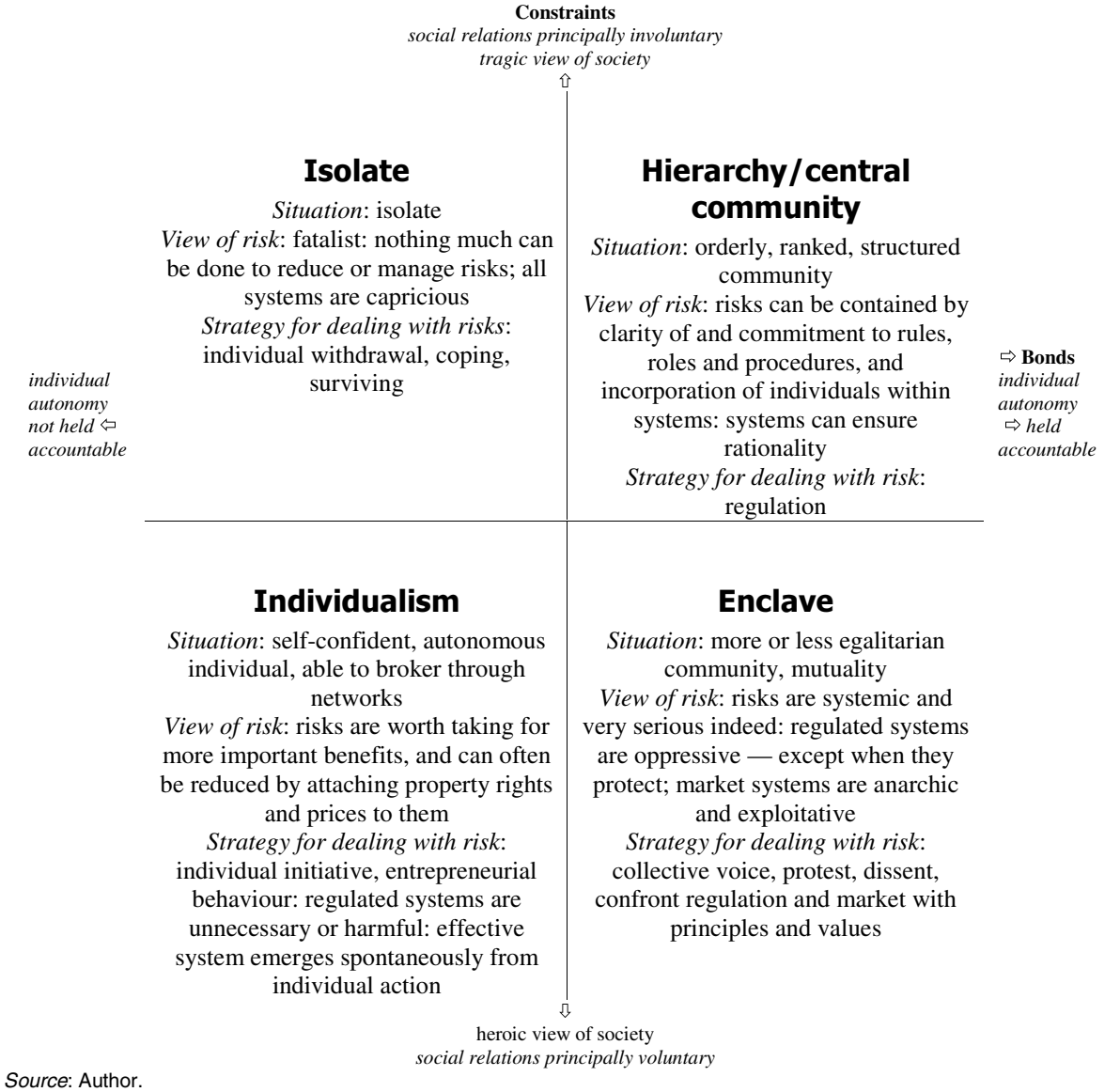
GJ, 1992, *Managerial dilemmas: the political economy of hierarchy*, Cambridge University Press, Cambridge.

36. In sociometric analysis of social networks, there are well developed structural measures of isolation: see *e.g.* Wasserman S and Faust K, 1994, *Social Network Analysis: Methods and Applications*, Cambridge University Press, Cambridge; there are also many qualitative studies examining the outcomes associated with isolate positions, especially in studies on adolescence: see *e.g.* Cotterell J, 1996, *Social Networks and Social Influences in Adolescence*, Routledge, London. The "social capital" literature has in effect contrasted outcomes associated with isolate forms with outcomes associated with all other forms: see Putnam RD, 2000, *Bowling Alone: the Collapse and Revival of American Community*, Simon and Schuster, New York; Lin N, 2001, *Social Capital: A Theory of Social Structure and Action*, Cambridge University Press, Cambridge. The sociological and social network analytical traditions also contain plenty of studies of enclaves — *e.g.* Elias N with Scotson JL, 1994 [1977], *The Established and the Outsiders: A Sociological Enquiry into Community Problems*, Sage, London — and of individualism — most famously Granovetter 1994 [1974], *Getting a Job: A Study of Contacts and Careers*, 2nd edn, University of Chicago Press, Chicago, and Burt RS, 1992, *Structural Holes: The Social Structure of Competition*, Harvard University Press, Cambridge, Massachusetts. For an overview, see 6 P, 2001, "The Governance of Friends and Acquaintances? Public Policy and Social Networks", paper presented at the Economic and Social Research Council and Institute for Public Policy Research joint seminar, "Public Policy and Social Networks: Promoting Social Inclusion", 15 March, London. A classical study of the fatalistic outlook on risk associated with comparatively isolate forms is Banfield EC with Banfield LF, 1958, *The Moral Basis of a Backward Society*, Free Press, New York.

37. See 6 P, 2001, *Strategies for Reassurance: Public Concerns about Privacy and Data Sharing in Government*, Performance and Innovation Unit, Cabinet Office, London.

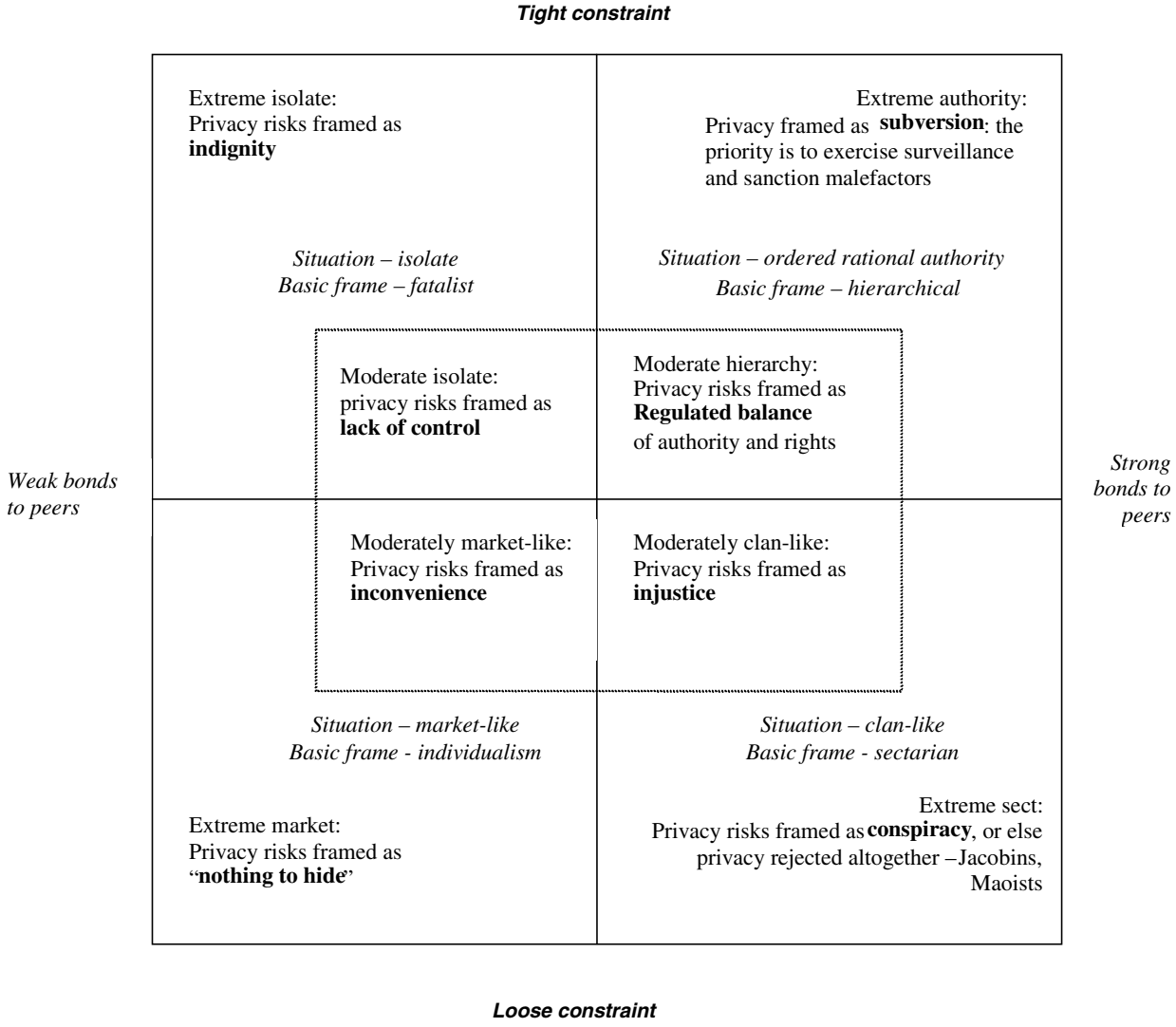
38. Gamson WA, 1992, *Talking Politics*, Cambridge University Press, Cambridge; for a discussion of the concept of a frame, see 6 P, 2001, "What's in Frame? Social Organisation, Risk Perception and the Sociology of Knowledge", unpublished typescript, King's College, London.

Figure 6. **How situation shapes basic range of risk perceptions about any kind of risk**



Source: Author.

Figure 7. **How primary situation shapes the way consumers frame privacy risks**



Source: Author.

In the study mentioned, the most socially excluded people, who were long term claimants of benefits, tended to be isolated and tended to exhibit the "indignity" in frame which they experienced data collection and data sharing as humiliating and demeaning, but as inevitable and part of the unavoidable fabric of life. The self-employed males, by contrast, who operated as brokers in networks, might sometimes begin with the "nothing to hide" frame, in which they would claim that no one with anything to hide need be concerned about privacy at all, but quickly shifted to the "inconvenience" frame, in which data collection and sharing was seen more as a nuisance than as a threat. Some of the older people who had grown up in the post-war years with their experience of commitment to a variety of solidaristic institutions in contexts such as health care, but who were now outside the labour market and its particular hierarchical rankings of status and had adopted a new identity as retired people with its sharply defined membership criterion, looked at privacy risks as matters of injustice, or as the violation by the state of general principles. The more extreme "conspiracy" frame tends to be associated mainly with privacy activist movements. Finally, the more hard-nosed members of the law

enforcement community exhibit the frame in which they see privacy claims as subversive, insisting that without general surveillance, the control and prevention of crime would be impossible. More common among central civil servants, for example, who are charged with finding some settlement between the law enforcement authorities' concerns and those of a range of wider publics, is a "regulated balance" frame,[39] in which it is hoped that some quasi-constitutional order can be defined and enacted in explicit rules that will reconcile the conflicting pressures in such a way that it can be administered by conventional administrative means.[40]

It is not really meaningful to produce quantitative estimates of what proportions of the population might be described by each of these situations, precisely because there is such mobility in everyone's life between contexts that constitute the cues for these situational dynamics. That is to say, the primary situation is itself plural for most of us. Many of us are prepared to be quite individualistic about taking a supermarket loyalty card with all the disclosure of personal information about our buying habits, yet feel much more enclaved about the way in which we want our primary care physician to manage the use and disclosure of our health records, while being content, deferentially to trust that some combination of regulatory oversight and professional codes will adequately govern the proper use by our bank of the data about our transactions on our accounts. This mobility reflects the plurality of our institutional relationships with large retail organisations, individual physicians and banks, as well as facts about the wider contextual aspects of our lives — education, religion, social networks, class, gender, and so on — that we bring to each of these contexts.[41] (This is not to say that people can or do make any move around this matrix with equal ease. As I shall show below, there are important differences in the height of the hurdles to be crossed between positions.) Although there have been attempts to produce estimates of an aggregate "worldview" bias using very general, context-free attitudinal statements in Likert scales (developed by the late Karl Dake) to measure individual positions within the taxonomy presented in Figure 6,[42] precisely because these statements are so general and context-free, one has to have doubts about their meaningfulness, let alone the meaningfulness of attempts to draw cross-national comparisons.

If we had cross-nationally comparative data collected on differences in public perceptions of a variety of different types of privacy risk in specific contexts, that might be more useful. Still more useful would be cross-nationally comparative research that compared variations in perceptions of

---

39. For a critique of the argument that "balance" can be made as determinate a criterion for policy making as this bureaucratic hierarchical way imagines, see Raab CD, 1999, "From balancing to steering: new directions for data protection", in Bennett CJ, and Grant R, eds, 1999, *Visions of Privacy: Policy Choices for the Digital Age*, University Toronto Press, Toronto, 68-93.

40. 6 P, 2001, *Strategies for Reassurance: Public Concerns about Privacy and Data Sharing in Government*, Performance and Innovation Unit, Cabinet Office, London. For an earlier version that situates many of the leading writers and thinkers about privacy within this two dimensional space, see 6 P, 1998, *The Future of Privacy, Vol I: Private Life and Public Policy*, Demos, London, ch.4.

41. On the case for the "mobility" hypothesis, see Rayner S, 1992, "Cultural Theory and Risk Analysis", in Krimsky S and Golding D, eds, 1992, *Social Theories of Risk*, Praeger, Westport, Connecticut, 83-116.

42. See *e.g.* Grendstad G and Selle P, 1997, "Cultural Theory, Postmaterialism and Environmental Attitudes", in Ellis RJ and Thompson M, eds, 1997, *Culture Matters: Essays in Honour of Aaron Wildavsky*, Westview Press, Boulder, Colorado, 151-168; Dake K and Wildavsky A, 1993, "Theories of Risk Perception: Who Fears What and Why?", in Burger EJ, jnr, ed, 1993, *Risk*, University of Michigan Press, Ann Arbor, Michigan; Grendstad G, 2001, "Nordic Cultural Baselines: Accounting for Domestic Convergence and Foreign Policy Divergence", *Journal of Comparative Policy Analysis, Research and Practice*, 3, 5-29.

privacy risk both by context and by differences in primary situation. For this purpose, the survey techniques by Dake and his successors are only useful if they can be exactly correlated with information about people's primary situation. There are some methodological approaches developed for doing this,[43] but it has not been attempted to date.

Because the perception of privacy risk is a key element in shaping interest in PETs, we should expect, all other things being equal, that people in each of these different situations will exhibit significant differences in the kinds of PETs, if any, that will be of greatest interest to them. The most fatalistic are unlikely to have much faith in either the efficacy or the relevance of most PETs to their lives. After prolonged periods of being at the informational mercy of large bureaucratic organisations, benefit claimants tended, in the study in which this analysis was refined, to feel that they have little chance of influencing, still less controlling the use of their personal information by those organisations by any technological means. The most cynical even doubted if they were able to see their records online, that the information that would be made available to them in the name of subject access would in fact be the true record. More moderate "lack of control" frames could be associated at least with a willingness to be interested in online subject access. Those with at least more moderate individualistic "inconvenience" frames tended to be interested, as we would expect, in those instruments that might provide some more individual access to their information, including the forms of consent that present the lowest barriers to any benefits that may come to them through the exchange of information — such as opt-out rather than opt-in consent systems. For them, information about the uses to which their data are put, is of most importance. Those with more enclave-type "injustice" frames, and certainly with more extreme social movement outlooks are much more likely to be interested in technologies that limit data collections or that provide for anonymity or pseudonymity: indeed, the scale of data collection and the lack of anonymity *per se* has long been a central concern of social movements dedicated to organising for privacy.[44] Finally, those consumers with more hierarchical outlooks are more likely to be trusting of the agendas and rationales of large organisations as data controllers, and will therefore mainly want those PETs that enable them to correct minor errors, and at most may be willing to use some tools that provide pseudonymity in those fields where they feel that this is appropriate within the prevailing norms, more as a protection against other individuals than against abuse by large regulated organisations, in the procedures of which they have at least provisional trust. For this group, the existence of a law expressing a commitment to a social value — for example, data protection law — has a symbolic power that gives weight to that value.[45] Figure 8 summarises what we should expect.

If we accept then that this provides a reasonable guide to the range of ways in which consumers perceive privacy risk, then we can address the question, how far are people within any of these frames as initial starting points, open to persuasion to shift frame?

The argument that underpins this analysis suggests that, while persuasion is possible, there are in fact some clear limits to the openness of consumers to persuasion to be interested in PETs other than those that their initial basic bias would direct them toward, just as the argument of the previous section showed that there are clear limits to the openness of businesses. For what really drives risk perception

---

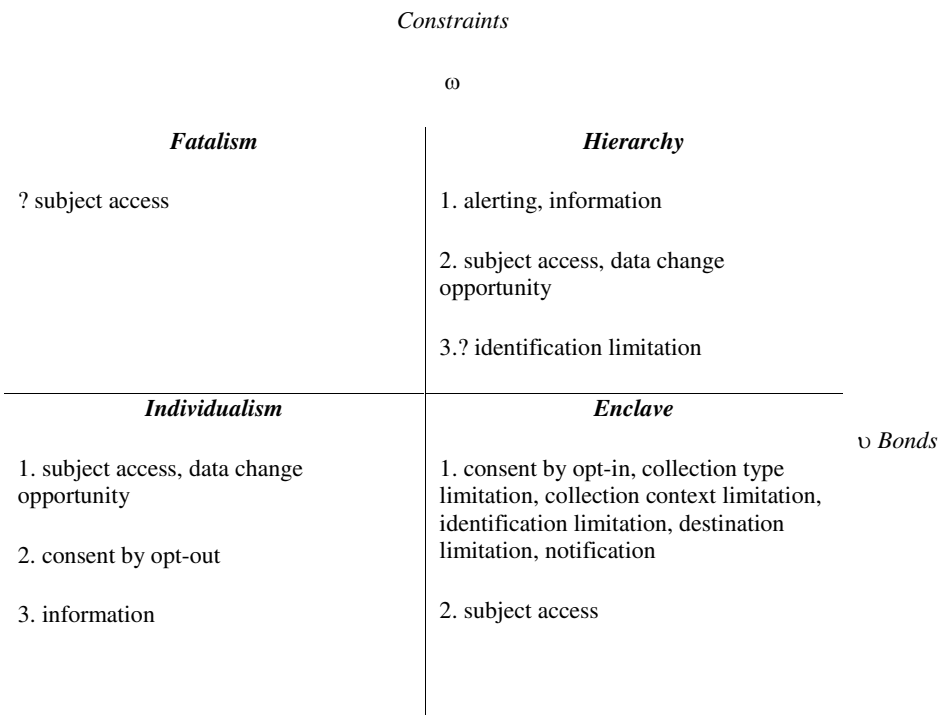
43. See Gross JL and Rayner S, 1985, *Measuring Culture: A Paradigm for the Analysis of Social Organisation*, Columbia University Press, New York.

44. See *e.g.* Davies S, 1996, *Big Brother: Britain's Web of Surveillance and the New Technological Order,* Pan, London.

45. Sniderman PM, Piazza T, Tetlock PE and Feld PJ, 1991, "The American Dilemma: The Role of Law as a Persuasive Symbol", in Sniderman PM, Brody RA and Tetlock PE, eds, *Reasoning and Choice*, Cambridge University Press, New York.

is situation. Bluntly, if we cannot change the real situation of consumers, then we should not expect their risk perception to shift greatly.

Figure 8. **What PETs might consumers with different patterns of risk perception be most interested in?**



Source: Author.

That said, there is a limited scope for frame shifting. So far, we have looked at the dominant influence of what we might call the *primary* situation — the long term, basic, underlying position in their society that a person occupies *vis-à-vis* large organisations, markets, the labour market, their peers, as modulated by specific institutional settings in particular contexts.

Some people may show very limited mobility, and for them, the survey methods on which some doubts were cast above, may have some limited validity if those surveys could distinguish the relevant people. Typically, those who remain within a single quadrant or frame across all the contexts of their lives are likely to be at the extremes of the matrix in Figure 7. For it is typically at the extremes where a single set of overarching features of the primary situation cast their shadow over every part of someone's life — for example, in acute poverty, great wealth, the engagement of one's whole life in a movement or community, or the dominance of a church or an all-consuming organisation of employment. Probably in most developed societies, it is a minority of the population whose lives are in these kinds of situations, and so we should expect significant proportions of people to show at least some mobility between contexts, typically between the more moderate positions.

By contrast, the most that we can expect by way of frame shifting persuasion from secondary situations (conversations or encounters in which information is offered that might run counter to the thought style engendered by the primary situation, modulated by the context) might be short-range moves between adjacent frames, which can only be sustained — if at all — as long as active persuasive pressure is sustained.

These arguments can be formalised by the following three hypotheses about the scope for persuasion to achieve these short-range moves:

A. *Moves from one extreme to the other extreme of either diagonal frame face lower hurdles than do vertical and horizontal moves*

For example, one reason why some business and law enforcement interests can sometimes ally on privacy issues, is that there is an affinity between the extremes along the positive diagonal. Some business leaders, for example, take the view that "if you have nothing to hide, then you shouldn't care about privacy": it became clear in the study discussed above that this is a stance typically used to mark out oneself as a decent person and to challenge others to put themselves in the clear by agreeing: in short, it functions as a blame-deflection tool. The law enforcement agents who take the view that unknown but large numbers of people do indeed have something to hide and that is precisely why privacy should not be protected can therefore ally with those who work with the "nothing to hide" frame, for each is principally interested in sorting sheep from goats among potentially suspect populations. Conversely, the "conspiracy" frame of the privacy activists and their deterministic view of information technology as intrinsically oppressive has an affinity with the "indignity" frame's view that large organisations necessarily exploit people: in effect, the affinity reflects the blame-mobilising role of these extreme frames.[46] These affinities make moves between these frames easier to make, in certain kinds of conversations, than certain other moves.

B. *Moves along diagonals within quadrants face lower hurdles when they are moves outward than when they are moves inward toward the centre, where the primary situation makes for any vulnerability in the anchoring to the reference frame*

Where, for example, people are insecurely situated in the labour market, it is much easier for them to move from a "lack of control" frame about their privacy vis-à-vis employers and government bodies to an "indignity" frame, when they are put into the secondary situation of a conversation with others whose reference frame is that of indignity. Likewise, those who are insecurely situated in their community of residence and feel under surveillance can move more easily from an injustice to a conspiracy frame if they are in conversation with less moderately enclaved persons than themselves.

C. *Vertical and horizontal moves between any of the moderate positions are easier than moves between the moderate form of any quadrant and the extreme form of another quadrant related horizontally or vertically (i.e. not diagonally, for a group for whom the baseline or reference frame is anchored reasonably securely as a moderate one.*

In the study discussed, there were some focus groups in which people came from relatively diverse primary situations. In conversation together, many of them were able to move relatively smoothly between, for example, "lack of control" and "injustice" frames, but in no case did we observe people moving from "indignity" to "inconvenience" frames. However, some of the income support claimants were able, after a lot of work together, occasionally to reach along the diagonal to speak from an "injustice" frame.

---

46. On the central importance of understanding risk perception as essentially about the organisation of what to do with social processes of blame, see Douglas M, 1992, *Risk and Blame: Essays in Cultural Theory*, Routledge, London.

By what means can regulatory bodies either change primary situations or create secondary situations, in which consumers might be influenced to shift frames? Firstly, regulators have no monopoly upon risk communication in this area, nor do they have a captive audience: there are many commercial and other organisations offering alternative messages. Secondly, it should be noted that all the means of persuasion and propaganda available to governmental bodies are relatively blunt instruments. That is to say, there is no certainty at all that applying any particular tool that might lead to someone abandoning a certain way of thinking about privacy will necessarily lead to them taking up the particular other frame about privacy risk that the governmental body would prefer them to adopt. Once people are dislodged from one anchoring, their path is not predetermined.[47] The greatest change in influencing where people end up is to influence their primary situation, rather than only to offer information to influence the secondary situation.

Changing the basic primary situations of populations is the most ambitious goal of policy, and involves complex mixes of the uses of incentive, authoritative regulation, information and persuasion that go far beyond the scope of the present paper, for such things are in general undertaken for much larger and wider reasons than simply to influence preferences for privacy.[48] Changing secondary situations basically involves using informational tools — education, information provision, persuasion, etc., whether through formal organisations such as schools or through informal systems such as the media. Research has generally found that the results of such strategies are highly variable and contingent upon the particular circumstances.[49] If they can be sustained over very long periods, with enormous commitment from all local institutions, on defined target groups, and delivered at such intensity that the information comes to have some of the power of an institution, then, public health research suggests, effects can be achieved, but this involves vast resources.[50] In these situations, in effect, the sustaining and embedding of the information campaign is beginning to impact upon the primary situation of local populations in the context of their health behaviour. For example, it is a now well established finding in media studies — for example, in studies on the impact of the deliberate attempt to make use of the media to "improve the public understanding of science" (which almost invariably means to attempt to attenuate public perception of some technological risk[51]) — that messages from the media are not passively received but are considered by lay publics much more critically than many "experts" imagine, according to their local knowledge, prior worldviews and

47. Thompson M, 1992, "The Dynamics of Cultural Theory and Their Implications for the enterprise Culture", in Hargreaves Heap S and Ross A, eds, 1992, *Understanding the Enterprise Culture: Themes in the Work of Mary Douglas*, Edinburgh University Press, Edinburgh, 182-202.

48. For discussion of the tools of government, see Hood C, 1983, *The Tools of Government*, MacMillan, Basingstoke; Salamon LM with Lund MS, 1989, *Beyond Privatisation: The Tools of Government Action*, Urban Institute Press, Washington DC; Bemelmans-Videc M-L, Rist RC and Vedung E, eds, 1998, *Carrots, Sticks and Sermons: Policy Instruments and Their Evaluation*, Transaction Publishers, New Brunswick, New Jersey; Peters BG and van Nispen FKM, eds, 1998, *Public Policy Instruments: Evaluating the Tools of Public Administration*, Edward Elgar, Cheltenham; 6 P, Leat D, Seltzer K and Stoker G, 1999, *Governing in the Round: Strategies for Holistic Government*, Demos, London.

49. Linder SH and Peters BG, 1998, "The Study of Policy Instruments: Four Schools of Thought", in Peters BG and van Nispen FKM, eds, 1998, *Public Policy Instruments: Evaluating the Tools of Public Administration*, Edward Elgar, Cheltenham, 33-45.

50. See *e.g.* Maccoby N *et al*, 1977, "Reducing the Risks of Cardiovascular Disease: Effects of a Community-Based Campaign on Knowledge and Behaviour", *Journal of community health*, 3, 1, 100-114.

51. Although practitioners in that field are not agreed on whether to admit that this is the case! See: Dierkes M and von Grote C, eds, 2000, *Between Understanding and Trust: The Public, Science and Technology*, Harwood Academic Publishers, Amsterdam.

basic situation.[52] When experts attempt risk communication and persuasion beginning from hierarchical or individualist assumptions, as they tend to do, and where segments of the public do not share those assumptions, because of their particular situation, they will not be persuaded and may simply not engage with the information offered.[53] There are many examples where extensive public information campaigns have effected no significant change in the opinions of most people — indeed, this is the now well-established finding of political scientists studying general election campaigns which goes back to the 1940s[54] — election campaigns have no significant net effects and indeed often no very large individual-level effect, unless it is to polarise still further those who began with more extreme positions. In general, on those occasions when the media sustains attention beyond the usual "issue attention cycle" upon some major issue, they are thought to be more effective in focusing attention than in persuading — as the cliché has it — in telling people what to think about rather than what to think.[55] However, for issues such as privacy that do not tend to be focused upon by the media beyond the issue attention cycle, even this is not particularly promising. Social psychological work has found that even those persuaded to adopt a more positive attitude to something may still not actually buy it.[56] This would, presumably apply to a privacy-respecting service using PETs as much as to anything else. Even where messages can be sustained over time, despite the "issue attention cycle" of the media, "cultivation" effects in inducing people to change their preferences cannot be relied upon.[57] This psychological finding makes sense when understood as a symptom of the dominance of the primary situation on thought style in the manner set out above. Only when people are persuaded to shift their sense of their own identity — that is, in the terms used here, when a change can first be made in the primary situation — have psychologists observed significant attitude change effects, to adopting attitudes that they consider consonant with the identity being adopted.[58] Yet most public information campaigns are addressed at the level of the particular risk, or the particular context — such

---

52. Irwin A and Wynne B, eds, 1996, *Misunderstanding Science: the Public Reconstruction of Science and Technology*, Cambridge University Press, Cambridge; Irwin A, 1995, *Citizen Science: a Study of People, Expertise and Sustainable Development*, Routledge, London; Bush J, Moffat S and Dunn CF, 2001, "Keeping the Public Informed? Public negotiation of air quality information", *Public Understanding of Science*, 10, 2, 213-229.

53. Schwarz M and Thompson M, 1990, *Divided We Stand: Redefining Politics, Technology and Social Choice*, University of Pennsylvania Press, Philadelphia; Robins R, 2001, "Overburdening Risk: Policy Frameworks and the Public Debate about Gene Technology", *Public Understanding of Science*, 10, 1, 19-36.

54. The original finding was by Lazarsfeld PF, Berelson B and Gaudet H, 1948, *The People's Choice: How the Voter Makes Up His Mind in Presidential Campaigns*, Columbia University Press, New York.

55. O"Guinn TC and Faber RJ, 1991, "Mass Communication and Consumer Behaviour", in Robertson TS and Kassarjian HH, eds, 1991, *Handbook of Consumer Behaviour*, Prentice-Hall, Englewood Cliffs, New Jersey, 349-400 at 363. One recent British study claimed to find a much greater effect of newspaper biases on readers, at least some major issues, but the data are in fact consistent with the possibility of much greater reader selection than newspaper influence: Lacey C and Longman D, 1997, *The Press as Public Educator: Cultures of Understanding, Cultures of Ignorance*, University of Luton Press, Luton.

56. Zimbardo PG and Leippe MR, 1991, *The Psychology of Attitude Change and Social Influence*, McGraw Hill, New York.

57. O"Guinn TC and Faber RJ, 1991, Mass Communication and Consumer Behaviour", in Robertson TS and Kassarjian HH, eds, 1991, *Handbook of Consumer Behaviour*, Prentice-Hall, Englewood Cliffs, New Jersey, 349-400.

58. Valins D, 1966, "Cognitive Effects of False Heart-attack Feedback", *Journal of Personality and Social Psychology*, 4, 4, 400-408.

as online shopping, or the medical setting, or banking — rather than at the larger level of the primary situation.

This is not to say that only in rare and very exceptional cases can public information campaigns work. Rather it is to suggest that they may not work in the ways intended, that they cannot necessarily overcome the effects of other forces, and they have to be designed with the greatest care, targeted very carefully rather than attempt blanket coverage, focus on very specific risks and offer very specific reasons to adopt quite specific solutions, be sustained over long periods, and work with the basic moral norms of the target segment of the public and engage their sense of identity and situation.[59]

The issues of price sensitivity and transaction cost recognition can be dealt with more briefly. The more *individualistic* are most likely to be attuned to a basically proportionate and linear sensitivity to price increments. Among them, in a roughly proportionate manner, we should expect that as price differentials for privacy-enhanced services rise above prices for services that offer less respect for privacy, the less they will be willing to demand privacy-respecting services and the PETs embedded in them. Conventional economists' demand curves make most sense for this group. The more *enclaved* groups are likely to exhibit a kinked curve for price sensitivity, in the sense that they are more likely to be willing to pay higher prices for privacy protection, and as the cost of privacy rises above a certain threshold, unlike the individualists, they will not simply give up on it, but exercise voice rather than exit,[60] in order to demand regulation to reduce the cost of the more drastic privacy protections that they care about most. The more *hierarchical* will be price sensitive, but will show a kink at a higher point than the enclaved, for although regulation will be important to them, they will be more willing to accept that, within a defined band, it is reasonable for organisations to charge prices that reflect costs. Price sensitivity is likely to be lowest for the *isolates*, for they will see little benefit from technologies of these kinds in the context of their dealings with the organisations they face. Figure 9 summarises what we should expect using conventional simplified demand curves.[61] Again, it should be remembered that many people will exhibit a different curve in different contexts.

In order to understand how open to influence consumer demand for PETs might be, it remains to consider the sensitivity of consumers to the non-monetary transaction costs of search, mobility between providers, and their own time and effort in use. It is to be expected that individualists, again, will be proportionately sensitive, for to them, time is money in a straightforward way. By contrast, those willing to price their own time and effort at the lowest rate in order to secure the privacy protections they care most about are likely to be the more enclaved, while the more hierarchical will be willing to bear moderate time costs. The issue hardly arises for isolate/fatalists about privacy, for their interest is so low in any case. Therefore, the quasi-price sensitivity curves for the partly non-monetised transaction costs will look very similar to those for price differentials between privacy-respecting services using PETs and non-privacy-respecting services using none.

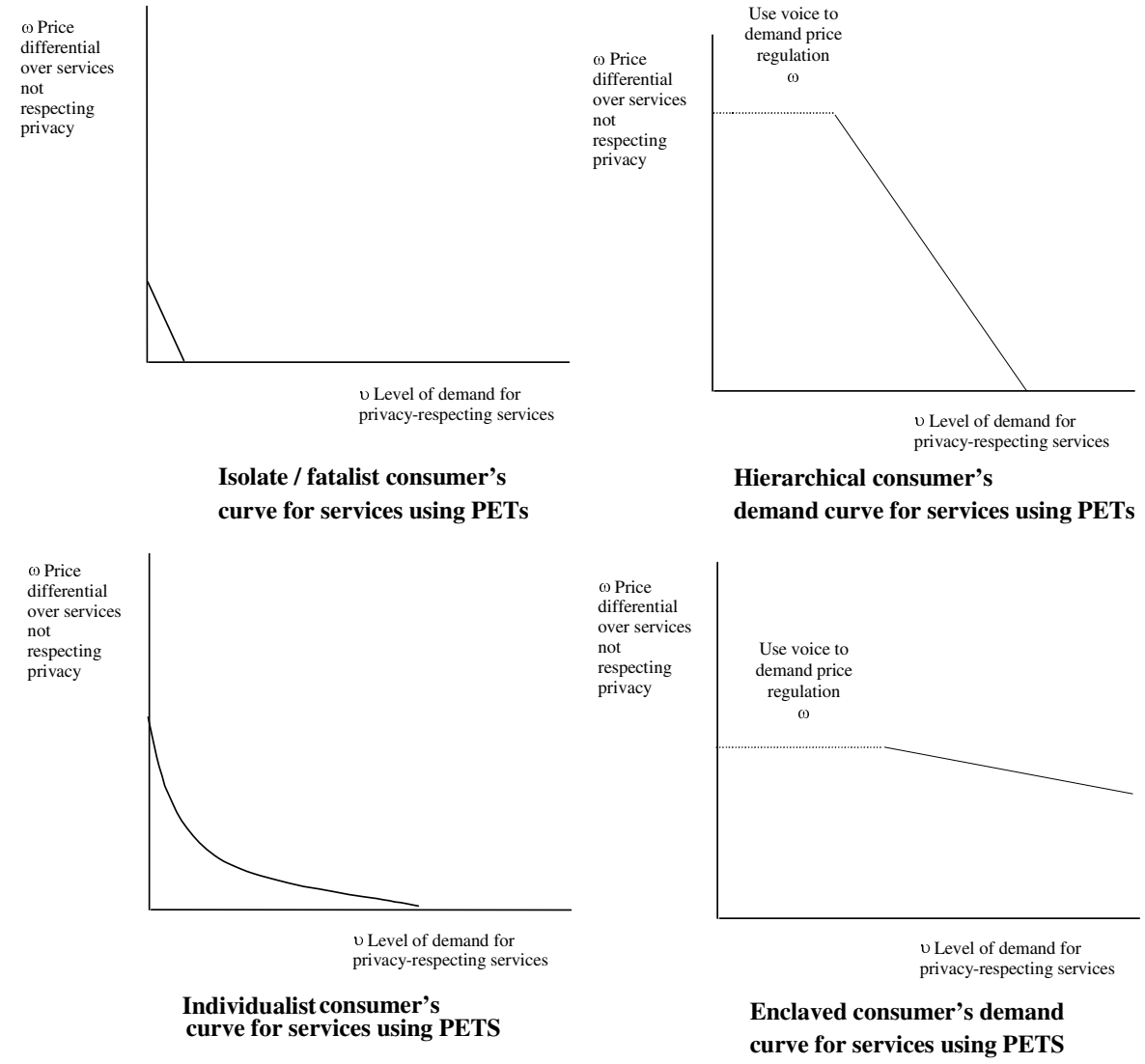
---

59. Weiss JA and Tschirhart M, 1994, "Public Information Campaigns as Policy Instruments", *Journal of Policy Analysis and Management*, 13, 1, 82-119.

60. Hirschman AO, 1970, *Exit, Voice and Loyalty: Responses to Decline in Firms, Organisations and States*, Harvard University Press, Cambridge, Massachusetts; Dowding K, John P, Mergoupis T and van Vugt M, 2000, "Exit, Voice And Loyalty: Analytic and Empirical Developments", *European Journal of Political Research*, 37, 469-495.

61. For an example of representing the impact of the four basic styles upon economic representations of demand, see Wildavsky A with Fogerty D and Jeanrenaud C, 1998, "The Concept of Externalities is Either Vacuous or Misapplied", in Wildavsky A, 198, *Culture and Social Theory*, ed Chai S-K and Swedlow B, Transaction Publishers, New Brunswick, New Jersey, 55-84.

Figure 9. **Demand curves for PETs for consumers in the four basic situations**



Source: Author.

Bringing business and consumer interest together

It will not have escaped the reader that Figure 2, describing the basic situations of businesses, and Figure 7, describing the basic situations of consumers, at root use the same analysis. They are both applications of Figure 6 to their respective fields. The vertical dimension in Figure 2 that describes the extent of monopolistic or oligopolistic ordering of markets is essentially the same thing as the "constraint" dimension in Figure 7 upon consumers, for it captures the issue of the degree to which the market is ordered by something, that is by coercive or by competitive power (social regulation). Likewise, the dimension of surveillance by the wider community in Figure 2 that explains both willingness and opportunity to exploit, is essentially the same as the dimension of "bonds" for consumers, for it captures the extent of accountability to others (social integration). This is important, because it enables us to understand the dynamics of the relationship between businesses' ability and willingness to offer privacy-respecting services and consumers' ability and willingness to demand those services.

The institutional situation that shapes consumers' risk perceptions and hence their preferences about privacy will, of course, be shaped by aspects of people's lives that go far beyond their encounters with businesses. Those additional institutional factors are shaped by their encounters with peers, with governmental bodies, with the law, with family and a host of other relationships. Nevertheless, in many situations, it may be possible for the institutional processes governing businesses and consumers to create a *sorting* process which would lead consumers and businesses in corresponding quadrants to gravitate toward each other.

The main sorting processes in any market, which enable businesses and consumers with similar characteristics, institutional styles and constraints, and responsiveness to similar concerns, to find each other, are, quite simply:

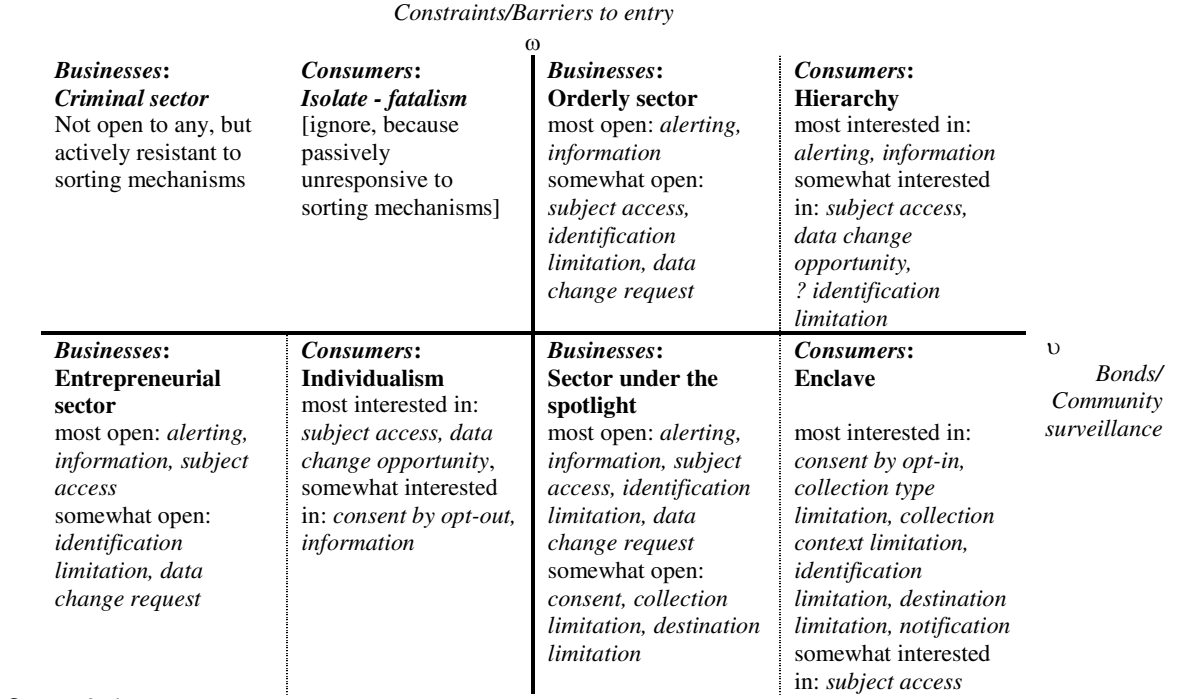
- In competitive markets, consumers' willingness and ability to bear the transaction costs of search and mobility until they find suppliers they can trust or that offer them the protections they seek.
- In non-competitive markets, the ability and willingness of regulatory action or the fear of regulatory action, as a substitute for consumer action in search and mobility.
- Business strategies, based on hope, to invest in marketing in order to signal to consumers with the relevant preferences and, at least at the margin, in using advertising and other frame-shifting means of persuasion to influence those preferences.

Sorting is never perfect, of course, because in competitive markets where, unavoidably, there are significant search and mobility costs, new incoming consumers lack the experience that older, exiting consumers possess, and so, even if their preferences are stably formed — which is often far from being the case — they take some time to find the sector that most suits their preferences.

How much sorting, then, can we expect, even in the case most favourable to sorting? It can be argued that a reasonable level of sorting can be expected, at most, in three of the matching quadrants. Businesses in the sector under the spotlight may be able to attract enough enclaved consumers with strong preferences and those consumers will be willing to bear the transaction costs of search and mobility from other suppliers so that they can find businesses willing to meet their preferences. Likewise, more entrepreneurial businesses may be able to secure the interest of more individualist consumers for the range of price/privacy ratios that their menu of services can offer. Again, the large bureaucratic world of the orderly sector could attract enough hierarchical consumers for each sector to be sustainable, even if there is volatility among individual firms in each. However, there is a sector of businesses for which and a segment of the consumer population for whom sorting is necessarily limited. By definition, the criminal sector will catch whoever it can, and not only isolate-fatalist consumers even if they are the most vulnerable; conversely, isolate-fatalist consumers may show up in any of the economic sectors of businesses and will, again by definition, be unlikely to see much point in bearing the costs of search and mobility to shift sector, even in this "sorting" scenario.

Suppose a reasonable level of three-quadrant sorting were achieved. Even then, it is important to note that there might still be some conflicts, for the match of PETs which businesses and consumers might want may not be exact. Figure 10 shows the extent of the match in a "sorting" scenario, by bringing together the key elements of Figures 5 and 8.

Figure 10. **The extent of match and mismatch under a three quadrant "sorting process" scenario**



Source: Author.

As we might expect, the area of least conflict is the hierarchical/orderly sector, (when adequately regulated), where consumers can most readily adjust to what cost pressures and situations lead businesses to be most open to offering. However, it is quite possible that individualist consumers might demand readier access to data correction requests and more consent than businesses in the entrepreneurial sector might find profitable in the time horizons they prefer to work in, and even more likely that the more extreme enclaved consumers will demand privacy protections that are more expensive than the small and medium sized niche market businesses of the sector under the spotlight will find profitable. This is in line with the expectation on wider theoretical grounds that this zone would, at least under many situations, exhibit great tendency for conflict and schism between suppliers and consumers.[62]

If, on the other hand, there are institutional blockages to sorting — for example, because there are insufficient numbers of enclaved consumers to sustain a highly responsive sector of businesses responding to those enhanced levels of preference for privacy, or if the costs of mobility for at least some groups of consumers to the sector that might otherwise best suit their preference profile are high — then we can expect even greater conflict. In situations of conflict, a number of outcomes are possible. One interesting outcome is the possibility that conflict itself represents a significant change to the primary situation of the consumer, which causes them to shift frame altogether. They may find that they adjust their frame to the sector they find themselves in which would produce a delayed or lagged sorting process. Alternatively, they may react against the institutions of that sector.[63] There

62. For the larger theoretical argument about schism and conflict in this sector, see Thompson M, Ellis RJ and Wildavsky A, 1990, *Cultural Theory*, Westview Press, Boulder, Colorado.

63. For an account of the range of possible outcomes here, consider the paths traced in the "theory of surprise" in Thompson M, Ellis RJ and Wildavsky A, 1990, *Cultural Theory*, Westview Press, Boulder, Colorado, ch. 5.

may be pressures in each direction. However, we should expect that in a market where there is limited competition and so the consumer can exercise few choices other than to use the service offered by the incumbent, the pressures would be more powerful to adapt their frame to that of the sector in which the monopolist is located. In the former case, we have an example of persuasion of consumer by business, and in the latter, the reverse. Just as was noted above about public information campaigns, it is not possible in advance to predict just what will be the destinations of people dislodged from their location in social organisation, whether deliberately by policy action or otherwise.

A key question for public policy, then, is whether it should be a goal of policy to remove institutional and market-based barriers to sorting of this kind. The implication of the present argument is that if we want to reduce conflicts, then — all other things being equal (such as the costs and risks of removing barriers, and the possibility of unintended consequences), this might well be worth doing.

Conclusion

The argument of this paper is that there is some scope for persuading businesses and consumers to be more interested respectively in offering and in demanding services supported by privacy-enhancing technologies, even if those services are slightly more expensive than services that do not protect privacy. However, it has been argued that this scope is circumscribed in ways that can and should be understood by governments and movements seeking to promote the use of privacy-enhancing technologies. There is scope to present certain kinds of PETs in ways that will make them more attractive to businesses in certain types of situation and to consumers in certain types of situation. If persuaders can work with the grain of the constraints, the institutional contexts, the basic assumptions and outlooks of businesses and consumers in these situations, and if they can develop rich appreciations of what may interest them, then they may be able to target communications about PETs to quite tightly defined constituencies in ways that will make a significant difference.

On the other hand, the argument here suggests that it would be a mistake to attempt persuasion on a one-size-fits-all basis, or to imagine that any business and any consumer can be persuaded to be interested in any kind of protection against any important privacy risk, still less at any cost. The paper argues for a certain modesty in the ambition of policy makers: the beginning of wisdom for persuaders is to accept that policy failure is the more likely the more ambitious are the goals for those to be persuaded and the range of things about which persuasion is to be attempted. Moreover, the most successful persuasion induces relatively short-range movement in how people think. Dramatic “road to Damascus” conversions are rare, and not usually amenable to being induced by deliberate policy action.

For would-be persuaders for PETs, then, the first task is to understand the ways in which businesses and consumers segment by situation. The second is to derive from this, an appreciation of which types of PETs they may be open to persuasion about. The third is to develop a clear understanding of the basic outlooks within which those PETs will have to make sense. The fourth is to identify the tools and instruments available to persuaders with which to address each of these constituencies.

The good news that is implied in the argument of this paper, is that some privacy protections matter to some degree to people in a very wide variety of situations. The bad news is that it will be a considerable labour for policy makers and persuaders to work out more exactly just what matters to just whom.

REFERENCES

Burkert, Herbert (1997), "Privacy-Enhancing Technologies: Typology, Critique, Vision" in P.E. Agre and M. Rotenberg (eds.), *Technology and Privacy: The New Landscape*, MIT Press, Cambridge.

Ontario Information and Privacy Commissioner and *Registratiekamer* (1995), "Privacy-Enhancing Technologies: The Path to Anonymity", August.

EU (European Union) (2000), "Working Document: Privacy on the Internet — An Integrated EU Approach to Online Data Protection," Article 29 Data Protection Working Party, 21 November, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2000/wp37en.pdf.

Marx, Gary T. (1990), "Privacy and Technology", http://web.mit.edu/gtmarx/www/privantt.html.

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

Chapter 14

TRANSBORDER DATA FLOW CONTRACTS IN THE WIDER FRAMEWORK OF MECHANISMS FOR PRIVACY PROTECTION ON GLOBAL NETWORKS

This chapter discusses the use of transborder data flow (TBDF) contractual solutions in the wider framework of mechanisms for privacy protection and recognises the changing environment for TBDF and the impact of the global information infrastructure (GII) on the processing and transmission of personal data. It examines the two main categories of transborder data flows; business-to-business (B2B), and consumer-to-business (C2B) and highlights the issues raised by applying contractual analysis and structures to online communications, in particular to C2B communications. This chapter also stresses the need for developing tailored dispute resolution mechanisms for C2B online interactions. Where appropriate, this chapter suggests possible further initiatives to foster the widespread use of contractual privacy solutions for TBDF in online communications.

Chapter 14

TRANSBORDER DATA FLOW CONTRACTS IN THE WIDER FRAMEWORK OF MECHANISMS FOR PRIVACY PROTECTION ON GLOBAL NETWORKS

Main points

Fundamental requirements for contractual solutions

A number of fundamental requirements for privacy contractual solutions, as well as additional relevant factors such as constraints or ancillary requirements and other privacy protection mechanisms, are considered important in promoting privacy compliance. Among these requirements are the substantive rules — the minimum level threshold being the Principles in the OECD Privacy Guidelines — which set out the parties' privacy obligations; a workable complaints and investigations process, and the provision of appropriate dispute resolution mechanisms. The substantive rules proposed in the report are intended to serve as a common reference for the discussion of and conditions for what is currently in use or under development, the experience to date, and possible further work in respect of contractual approaches.

Contractual models currently in use or under development

The report highlights the historic focus on TBDF contracts for B2B transfers and examines model contracts, notably the model clauses developed by the International Chamber of Commerce (ICC), as well as current initiatives aimed at using codes of conduct and formal industry standards as a form of contract. It draws attention to the flexibility of model contracts, which allow the modification of the detail of their provisions to accommodate categories of industries/sectors as well as other particular circumstances, such as specific data or the use of a particular medium. While identifying certain constraints on the use of B2B contracts, the discussion recognises the potential of model B2B contracts to satisfy privacy protection expectations regardless of whether or not the transfer occurs in an online or offline environment, in particular with the support of ancillary measures such as online privacy notices to the individuals at the point of data collection.

Recourse of the individual in B2B contracts

Redress for breach of contract is available to the parties to the contract and usually also to third-party beneficiaries of the contract. To ensure that data subjects have the means to enforce a B2B TBDF contract, the ICC Model Contract provides the data subject, or a Data Protection Authority on behalf of the data subject, the right to bring an action for breach of contract against the data exporter for any alleged breach of the data importer under the contract. This ensures that the data subject has a party (the data exporter) to hold accountable in his/her home country. While some express concern that this remedy might not be sufficient to secure compliance by the data importer, it is important to note that the Data Subject may also have enforceable rights through other privacy protection infrastructures such as laws or effective self-regulation.

Issues with consumer-to-business (C2B) interactions

The report considers the characteristics of C2B online interactions, discusses the issues raised by applying contractual analysis and structure to such interactions, and demonstrates privacy issues which arise prior to the conclusion of a contract, calling for other privacy protection mechanisms in such cases. It therefore suggests that privacy protection policies and statements have a significant role to play and that they may provide the means to transform a privacy policy into a binding commitment. Consumer protection agencies, third party organisations, and effective internal organisation review mechanisms are identified as having a significant role to play in providing certification or verification services and tools.

The need for appropriate dispute resolution mechanisms

The issue of dispute resolution is identified as a critical one to build trust in the use of global networks for both businesses and consumers. It is suggested that complaints, investigation, dispute resolution and enforcement mechanisms should be developed in such a way as to address the specific characteristics of C2B online transfers. In that respect, conventional methods of dispute resolution are discussed and their benefits and limitations highlighted. Other current experience of online dispute resolution mechanisms is also presented.

Future initiatives

Finally, the report draws a number of conclusions from the discussion of the above topics. It highlights particular issues to be resolved in order to satisfy the privacy protection objective. The report also seeks to identify: initiatives which could foster the use of privacy contracts; any other matters which require further consideration or investigation; initiatives which could advance the work to date on the use of contractual solutions, especially for online C2B transfers and interactions; and the need for any specific online dispute resolution service tailored for C2B transfers.

The following four themes emerge from the report:

- The importance of promoting privacy awareness and providing educative tools.

  In accordance with the Openness Principle of the OECD Privacy Guidelines, there should be continued emphasis on systemic measures to improve privacy notice and consent procedures such as the OECD Privacy Policy Statement Generator. There may be an opportunity for a dedicated information page to catalogue resources to obtain additional information regarding privacy protection laws, self-regulatory mechanisms, etc.

- How to develop enforceable privacy commitments for online C2B transfers.

  Privacy policy statements could be used in the future, as a basis for establishing the terms and conditions governing the transactions on a Web site. In particular, they could address the substantive privacy rules, any verification measures or certification processes applying to the Web site. The consumer would be notified of these terms and conditions prior to the point in time at which the contract is entered into.

- The various international developments which require monitoring and further collaboration.

  There are many international developments which need to be monitored so that it is possible to learn from these experiences when implementing contractual privacy solutions and ancillary measures. Such developments include any further work based on the ICC Model Clauses or the various projects around the world to develop online dispute resolution measures.

- The potential to develop a framework for effective alternative dispute resolution for online C2B transfers.

Introduction

Globalisation of data transfers and impact of the Internet

The advent of the global economy, and the increasing sophistication of information and telecommunications technologies, are resulting in the globalisation of international data transfers. International information systems are the basic infrastructure of a multinational company's operations in trading goods and services. More and more companies are moving data between countries. Organisations who have control over the collection and processing of personal data, have the means to reuse and transfer those data on an unprecedented scale. This can be high volume TBDF, such as in the form of databases, or multiple one-off collections from activities such as Web browsing on the Internet.

The network of networks that comprises the global information infrastructure is facilitating this transformation in transborder data flows. The GII involves the interconnection of "information highways", comprising telecommunications and computer technologies. The Internet is the most obvious example of these global networks. The online environment provides great benefits to users such as tailored and interactive information, products and/or services and enhanced privacy and security including use of encryption, firewalls, and identification procedures that extend beyond what is used in pre-Internet commerce, but it also creates new challenges for privacy protection.

Consumer trust and e-commerce

In this global trade environment, personal data is growing in economic significance. The information economy (now the knowledge-based economy), leverages off the use of information, including personal data. Data are seen as key business assets.

The nature of the challenge has been recognised both internationally and by national governments. This is illustrated by the linkages which have been made between building consumer trust (such as through effective privacy protection) and the facilitation of electronic commerce. This was one of the themes of the OECD member countries' 1998 Ottawa Conference on "A Borderless World: Realising the Potential of Global Electronic Commerce". The result was a commitment to ensure privacy protection on global networks and, notably, to encourage the use and development of model contractual solutions for online TBDF.

The role of contracts in the wider framework of privacy protection mechanisms

Internationally, there are many different mechanisms for enhancing privacy protection. These range from privacy laws to self-regulatory frameworks (such as codes of conduct or practice and formal industry standards). Other mechanisms include privacy enhancing technology (PET) and

systems for labelling, certifying and attaching privacy seals. Contracts have their place among these mechanisms.

Contracts are intended to be binding agreements, enforceable in law. Used for TBDF, they can provide a degree of flexibility and can accommodate some of the differences between countries, in the way they approach privacy protection in the context of global networks. Contracts may also be a practical and positive measure where there are different or no data protection laws or effective self-regulation regimes. They may also complement or support compliance with a privacy self-regulatory framework or statutory regime. It is possible for the terms and conditions of the contract to reflect the requirements of specific privacy instruments.

For example, some instruments require special treatment for transborder data flows. In particular, Part Three of the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* 1980 (OECD Privacy Guidelines) states that member countries may restrict the flows of certain categories of personal data specifically controlled by their domestic legislation, to member countries which have no "equivalent" protection. This restriction must be balanced with the OECD's stated determination to advance the free flow of information between member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among member countries.

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) and Article 9 of the United Nations Guidelines Concerning Computerised Personal Data Files (1990). The European Union Data Protection Directive (95/46EC) also provides in Article 25(1) that those data transfers from a member country to a third country can only take place where that third country ensures an "adequate level of protection". The possibility of using contracts to ensure that personal data transferred from one country to another receive "adequate protection" under the EU Directive is explicitly recognised by Article 26(2). In addition, for many years some national instruments have made provision for the special treatment of TBDF (*e.g.* Germany, France).

I. Fundamental requirements for contractual solutions

Any discussion on contractual solutions to protect privacy and personal data can be enhanced if there is a common understanding of the objectives of this type of solution. This includes an understanding of the role of contracts within the wider framework of privacy protection mechanisms and of those elements of contractual solutions which are considered important to protect privacy. In terms of TBDF contracts, it may be helpful to collate these elements, which are necessary to deliver an effective contractual solution. Any discussion should also consider ancillary requirements or features of the privacy framework within which the TBDF contract must operate.

Need for a common substantive reference

The parties to the TBDF contract need to ensure that there are substantive data protection rules, which apply to the data transfer. These rules could be a reiteration of the principles of the OECD Privacy Guidelines or drawn from some other instrument which sets out equivalent principles. Contractual privacy solutions can achieve an appropriate level of privacy protection, such as that articulated within the OECD Privacy Guidelines. This objective is qualified by the balancing exercise inherent in the preamble or introductory statement in the OECD Privacy Guidelines,

"Recognising:

that although national laws and policies may differ, member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;

that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices;

that transborder flows of personal data contribute to economic and social development;

that domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows;

Determined to advance the free flow of information between member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among member countries".

The OECD Privacy Guidelines[1] represent a consensus on fundamental requirements and objectives for privacy protection and an appropriate balance between effective privacy protection and the free flow of information. However, the appropriate level of privacy protection can also be drawn from other national law or self-regulatory frameworks, based on the OECD Guidelines.

For the European exporter, it could be the requirements as prescribed by the EU Directive or agreements between the European Commission and third countries. In that respect, the European Union advisory Working Party on the Protection of Individuals with regard to the Processing of Personal Data, ("Article 29 Working Party") has produced a Working Document[2] on the use of contractual provisions for TBDF to third countries. This document which assesses the meaning of "adequate safeguards" as used in the European Directive in relation to TBDF contracts, recognises that the obligations and rights set down in the OECD Guidelines, which are not dissimilar from other international instruments, express "a degree of consensus as to the content of data protection rules which stretches well beyond the fifteen states of the community".

Reference could also be made to codes of conduct and industry standards. For some years there have been self-regulatory moves to adopt such instruments for privacy protection. These measures can take the form of industry-specific or sectoral privacy codes of conduct (practice). They can be administered by the applicable supervisory body for that industry or sector, with the power to impose sanctions on its members or can be enforced by private sector self-regulatory bodies as is the case in the United States. They are a form of industry-wide contracts among participating members. In some jurisdictions, such as New Zealand, the privacy code is given statutory force and is subject to the jurisdiction of the supervisory data protection authority. These standards could be incorporated into TBDF contracts. Another form of consensual standard is that established by the official standards organisation at the national level. An example is the Canadian Standard CAN/CSA-Q830-96. This approach is particularly relevant for those countries which have no privacy laws or where private sector TBDF are not regulated in any way. Any of these can provide a minimum set of privacy principles, an implementation methodology, and a suggested structure within which to implement the privacy protection measure.

The flexibility afforded by the ICC Model Clauses, which recognise that the approach to data protection varies between countries, provides a means of building bridges between these approaches on the basis of the consensus expressed in the OECD Guidelines. Accordingly, the Clauses require the data importer to observe the rules on data protection applicable in the Member State where the data exporter is established, or if appropriate, a set of principles deemed to be adequate for transborder data flows. This means, by way of illustration, that the exporter (and therefore the importer) could be bound to comply with a detailed set of privacy principles as prescribed under the law of New Zealand or Hong Kong (if this is the country of the exporter). Conversely, there may be less comprehensive privacy regulations, or none at all, to be addressed in the privacy obligations of the parties to the contract. Despite the state of any applicable privacy law, the Model Clauses contain a separate obligation prohibiting the onward transfer of the data without the consent of the data exporter. This provides a proper basic level of privacy protection.

Need to ensure compliance with the substantive reference

In order for a contract to achieve effective privacy protection, a second important requirement is that the substantive rules that it includes will be given effect. Such a requirement is consistent with the accountability principle of the OECD Privacy guidelines, which requires that "a data controller should be accountable for complying with measures which give effect to the principles (…)". The Guidelines also provide that:

> *"Member countries should in particular endeavour to:*
> *(…)*
> *(d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; (…)"*

Tests for the effectiveness of a data protection system have been suggested, for example, by the Article 29 Working Party. They proposed the three following general criteria:

- The ability of the system to deliver a good level of compliance with the rules, which includes a high degree of awareness among data controllers of their obligations, and among data subjects of their rights; the means of exercising them; the existence of effective and dissuasive sanctions; and systems for direct verification by supervisory authorities, auditors or independent data protection officials.

- Support and help to individual data subjects in the exercise of their rights which includes a rapid and effective means of redress for the individual, and some sort of institutional mechanism allowing independent investigation of complaints.

- Appropriate redress for the individual, which involves a system of independent adjudication or arbitration. Appropriate measures to ensure compliance with privacy rules can be provided for in a contract. For example, the ICC model contract gives the data subject or data protection Authority a right of action against the data exporter under the relevant law. The data exporter can then seek indemnification from the data importer for breach of contract.

An alternative approach can be found in the US discussion draft of January 1998 on "Elements for Effective Self-Regulation for Protection of Privacy".[3]. In that document, the test for an effective self-regulatory privacy regime is described as having to do more than articulate broad policies or guidelines: effective self-regulation involves substantive rules, as well as the means to ensure that

consumers know the rules, that companies comply with them, and that consumers have appropriate recourse when injuries result from non-compliance.

As concerns enforcement mechanisms, an effective self-regulatory privacy regime should include mechanisms to assure compliance with the rules and appropriate recourse to an injured party when rules are not followed. Such mechanisms are essential tools to enable consumers to exercise their privacy rights, and should, therefore, be readily available and affordable to consumers. They may take several forms, and businesses may need to use more than one depending upon the nature of the enterprise and the kind of information the company collects and uses.

Such enforcement tools include notably consumer recourse (mechanisms by which consumers' complaints can be resolved), verification (attestation that the assertions businesses make about their privacy practices are true and that privacy practices have been implemented as represented), and consequences (failure to comply with fair information practices should have consequences. Among these may be cancellation of the right to use a certifying seal or logo, posting the name of the non-complier on a publicly available "bad-actor" list, or disqualification from membership in an industry trade association. Non-compliers could be required to pay the costs of determining their non-compliance. Ultimately, sanctions should be stiff enough to be meaningful and swift enough to assure consumers that their concerns are addressed in a timely fashion. When companies make assertions that they are abiding by certain privacy practices and then fail to do so, they may be liable for deceptive practices fraud and subject to action by the Federal Trade Commission).

Another approach can be found in the consultation papers of the Australian Government on the protection of privacy in the private sector, and notably in the information paper issued in September 1999.

Many factors, and most notably the privacy concerns that many people have in relation to electronic commerce, have influenced the Government's decision to develop a national legislative framework for privacy protection based on the National Principles for the Fair Handling of Personal Information (National Principles) issued by the Privacy Commissioner [The federal Privacy Act 1988 (Privacy Act) is the principal piece of legislation providing privacy protection in the federal public sector in Australia] in February 1998, following extensive consultation with business and consumers.

Briefly, the legislation will allow for the recognition of self-regulatory privacy codes backed by default legislative principles and a complaint handling regime that will apply where there is no applicable privacy code. The Privacy Commissioner will have a major role in the scheme. He or she will have an overall promotion and oversight role in relation to the private sector, whether covered by a code or not. The Privacy Commissioner will be responsible for approving privacy codes, providing assistance and advice to organisations, handling some complaints, and generally promoting an awareness and understanding of the scheme. As is currently the case in the Privacy Commissioner's limited private sector coverage, a determination of a complaint by the Privacy Commissioner or by a code complaint body will be enforceable in the Federal Court of Australia.

Another approach to be mentioned is the one adopted by Japan. In order to support personal data protection by business entities, the Ministry of International Trade and Industry (MITI) has issued model guidelines for business organisations entitled "Guidelines Concerning the Protection of Computer Processed Personal Data in the Private Sector (MITI Guidelines)". The Ministry of Posts and Telecommunications (MPT) has also issued guidelines for telecommunications services entitled "Guidelines on the Protection of Personal Data in Telecommunications Business (MPT Guidelines)". In addition, in March 1999, in order to encourage the appropriate management of personal data protection by each business entity, MITI established Japanese Industrial Standard (JIS) Q 15001

"Requirements for Compliance Program on Personal Information Protection". JIS Q 15001 requires the business entities to comply with the following:

- Establishment, implementation, maintenance and disclosure of a personal data protection policy.
- Limitation on collection of personal data.
- Limitation on use and disclosure of personal data.
- Receiving and responding appropriately to all complaints and requests for assistance from data subjects.
- Auditing; etc.

Further, JIPDEC (Japan Information Processing Development Center) grants "Privacy Marks" after certifying conformity of business entities to JIS Q15001 and MITI Guidelines. If the business entities granted "Privacy Marks" fail to conform to JIS Q 15001 and MITI Guidelines, JIPDEC should provide advice, request improvements, or may cancel the certification of Privacy Marks. Also, the "Personal Data Protection Registration Center", set up within the Japan Data Communications Association, registers telecommunication business entities which implement appropriate measures to protect privacy and issues a "personal data protection mark" to such businesses.

Conclusions on fundamental contract requirements

It is possible to summarise those elements which afford the core level of privacy protection to be reflected in the contractual provisions, as follows:

- Substantive rules based on the Principles in the OECD Privacy Guidelines. This element can be achieved through the inclusion of substantive principles into the contract or by reference to a relevant law, principles or guidelines.

- Some means of ensuring accountability and verifying that the parties are complying with their privacy obligations[4].

- A workable complaints and investigations process, in the event that there is a breach of the privacy obligations.

- Appropriate dispute resolution mechanisms for affected parties.

The particular circumstances of a data transfer may require more or less than the above-mentioned rules and procedure to be included in the contract. It may be that part of the required privacy protection is properly provided for by the wider legal or self-regulatory framework. Another consideration would be the nature of and risk attaching to the particular data which could either be non-sensitive public data requiring less protection or sensitive data requiring more protection.

II. Contractual models currently in use or under development

Historic focus on business to business transfers

The idea of using contracts for TBDF has been around for some time. In the early 1990s, the prevalent form of TBDF involved business to business (B2B) transfers. The nature of these transfers is very wide-ranging. They include the supply or exchange of personal data between business units or divisions within the same organisation. B2B also contemplates one entity providing data processing services to another, and the transfer of personal data as either the subject of, or ancillary to, a commercial arms-length transaction. The most intensive forms of TBDF occur in the area of human

resources, financial records (banking, insurance, credit), customer-related information (such as for direct marketing and travel reservations), and public sector agencies (law enforcement, border controls, tax agencies).

There has been a growing awareness of the significance of personal data as a key resource of many businesses. Although the impact of telecommunications on TBDF has long been well understood, the advent of the GII (in the form of the Internet and Intranet) has implications, which are only just beginning to be addressed. Global networks make it possible to collect, process and transmit personal data on an unprecedented scale. However, at the time contractual privacy solutions were first being debated, the focus was on more conventional B2B transfers, culminating in the development in 1992 of the Council of Europe Model Contract.

Council of Europe Model Contract (1992)

The Council of Europe Model Contract to Ensure Equivalent Data Protection in the Context of Transborder Data Flows was the result of a joint study by the Council of Europe, the Commission of the European Communities and the International Chamber of Commerce (ICC). The Model 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 Privacy Guidelines, the Council of Europe Model Contract provides a useful reference in determining what may amount to "adequate protection" under the EU Directive.

Under the Model Contract, the party sending the data warrants that the 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 have been stored, the adequacy and relevance of the data, the accuracy of the data and the period for which data storage has been authorised.

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

The remaining clauses deal with liability for the misuse of the data by the data receiver, rights of data subjects, dispute settlement and termination of the contract. The only detail on the mechanics of dispute resolution is in respect of arbitration (including the use of experts); the contractual requirement is for the parties to establish an "*appropriate system of settlement of disputes*".[5] The applicable law is left open as a matter for the parties to determine. This work of the Council of Europe (on contractual solutions) has provided a foundation for further developments.

The ICC Revised Model Contract

The 1992 Council of Europe Model Contract clauses were revised by the ICC, in light of the EU Directive's requirement of "adequate protection" in data exchanges to third countries. The revision takes into account the comments of the European Union's Article 29 Working Party set up pursuant to Article 29 of the EU Directive. The result was the ICC Model Clauses (For Use In Contracts Involving Transborder Data Flows).

The focus of the Model Clauses is on B2B transfers, whether off-line (that is by manual or physical means) or online (via electronic media). The latter medium is contemplated in the explanatory notes to the Model Clauses. They make another valid point; namely, the concepts embodied in the ICC

Model Clauses should become acceptable to a broad spectrum of enterprises. As these forms and practices become more widely known within the general business community, they are more readily adopted and therefore the Model Clauses should be more widely applicable to a range of B2B transactions, including those entered into by small and medium-sized enterprises.

There are certain assumptions within the ICC Model Clauses which may mean that some elements would require modification to tailor the use of the Model Clauses to the particular circumstances of the TBDF. For example, there are several references (in Clauses 2, 3 and 4) to the data importer constraining its subsequent use of the personal data to the purposes which have been notified by the data exporter or as is otherwise allowable under the laws of the country in which the data exporter is established. There is also a prohibition on disclosure (in the form of an onward transfer to a third party or country) without the prior consent of the data exporter.

The point is that these Clauses are a "model" and as such provide a strong basis on which to build or tailor certain clauses to reflect the particular requirements of the data importer/exporter and of the governing privacy laws or regime. If the Model Clauses are endorsed as satisfying the "adequacy" requirements of the EU Directive, then the parties modify those Clauses at their own risk; if the effect of any amendments is to reduce the level of privacy protection, then the parties could not make any assumptions that the arrangements reflected within the amended Model Clauses would be sufficient in terms of the requirements of the EU Directive.

Any detailed discussion of their content or consistency with the EU Directive is outside the scope of this report. However, the ICC Model Clauses have significant value as a foundation document or template for the development of B2B privacy contracts. The issue of individual redress in B2B contracts is discussed further in section 4.

Other work on contractual solutions

There have been a number of studies and initiatives in other fora on the use of model contracts for B2B data transfers. These include: the Working Document, adopted by the Article 29 Working Party on 22 April 1998, containing "Preliminary Views on the Use of Contractual Provisions in the Context of Transfers of Personal Data to Third Countries"; recommendations issued by the Office of the Privacy Commissioner of Hong Kong in Fact Sheet No. 1, April 1997; work of the Information and Privacy Commissioner of Ontario, Canada; the UN/CEFACT LWG work on contractual models for electronic commerce (Trade/Cefact/1999/crp.5/Rev1); and the Privacy and American Business 1999 Model Contracts Project (P&AB). This Project is on-going and involves the development of a contract template for TBDF activities.

Experience with TBDF agreements

The ICC Model Clauses are being used within Europe primarily as a reference point for the development of ad hoc TBDF contracts and in the employment or human resources area. There have been other contractual privacy initiatives which have received considerable publicity as examples of high profile B2B privacy contracts.[6]

One such example is the agreement between German railways (Deutsche Bahn AG) and Citibank. In 1994, German Railways (Deutsche Bahn AG) arranged with the German subsidiary of Citibank for the production of railway cards (offering discounts for frequent travellers) which also functioned as VISA cards. Because the cards were produced by a Citibank subsidiary in the United States, the agreement gave rise to substantial transborder data flows. In response to German data protection concerns, an Agreement on Inter-territorial Data Protection was entered into to give German citizens the same level of privacy protection which they would have had if the cards had been produced in

Germany. In particular, the contract provided for the application of German law, limited the transfer of the data to third parties, allowed for on-site audits by the German data protection authorities at Citibank's subsidiaries in the United States, and held German Railways and the German Citibank subsidiary liable to German data subjects for any violations of the Agreement by their American counterparts.

Although the experience with the Deutsche Bahn/Citibank Agreement is very instructive, its application as a precedent or model is quite limited because these types of contractual solutions may not be sufficiently "scaleable" or amenable to adaptation for smaller scale and lower profile B2B transfers.

Conclusions on current models

The international work on B2B contractual solutions is at a significant stage. There has been sufficient experience with these contracts for the development of a relatively detailed and comprehensive list of contractual requirements (in the form of the ICC Model Clauses). It is expected that there will be further advances on this work, as their uptake and adaptation increases. The expertise gained by those working with the ICC Model Clauses, and the need to tailor or modify their detail to adapt to particular circumstances, could be monitored and fed back into the "loop" for updating the ICC Model Clauses. It may be appropriate to develop variables or different versions to accommodate categories of industries/sectors or particular circumstances. No doubt this work will be further developed. It may also be enhanced by the experience gained from other ongoing projects.

The B2B contractual models are not that sensitive to, or dependent on, the medium of the transfer or communication. The ICC Model Clauses can be applied in the context of online (electronic) TBDF. The challenge, in terms of those contractual solutions which are currently in use or still under development, is that the focus has been on B2B; therefore, there has been little tangible progress on efficient contractual privacy solutions in C2B online TBDF. But the world is changing very quickly in respect of TBDF; there are now new pressures and issues to be addressed. The report will return to this theme in section 5.

III. Recourse of the individual in B2B contracts

To date, the development of TBDF contracts has been predominantly to address B2B transfers (such as the ICC Model Clauses). There is a consensus from experience with B2B contracts that they have the potential to improve significantly the fair information-handling practices and to overcome the potential restriction on the transborder flow of data as a result of different approaches to privacy protection adopted by member state governments.

Individual redress

There are a number of issues affecting the recourse of the individual under B2B contracts. Individuals are reliant on data exporters effectively acting as their agents to secure the requisite privacy protection. The ICC model contract seeks to address these issues by giving the data subject or data protection authorities a right of action against the data exporter who can seek indemnification against the data importer. Lack of contract privacy, however, still remains a problem in the reducing number of jurisdictions which do not recognise third party rights under contracts. B2B contracts complemented by a legal or self-regulatory privacy protection infrastructure might provide an alternative solution to individual redress. The German Railways/Citibank is an example of this possibility.

Logistical and resource barriers

Other logistical and practical drawbacks with ad hoc B2B contractual solutions, such as the barrier of legal costs or the time and resources, can be overcome by model contracts.

Allocating risk and liability

On the issue of jurisdiction and choice of law, one theory is to structure the contract so that the exporter of the data undertakes under domestic law that the data protection practices will be followed by any importer of the data anywhere in the world. This is the approach underlying the ICC Model Clauses. The effect is that the exporter is liable for the foreign treatment of any exported data, and the data subject would be able to seek redress in his or her local jurisdiction against the exporter for the failure of the importer to comply with its privacy obligations.

Verification and certification

There may be a need for some type of verification or certification mechanism to confirm that the importer's data management or processing complies with the contractual privacy obligations. If the individual has easy recourse to an effective complaints-based privacy regime, then there is less need to emphasise verification measures.

The inspection and audit processes required by any verification measure have their origins in B2B contracts, but have been modified to suit the different characteristics of online C2B interactions focusing on proposals to attach labels, seals of approval, privacy marks and otherwise to certify the privacy compliance of a Web site. Contracts could provide for verification if thought necessary by providing for audit inspection arrangements or transparency measures for the benefit of individuals. Verification can be resource intensive and the effectiveness of the measure is dependent on the choice of auditor.

The ICC Model Clauses contain an undertaking by the data importer to, "submit its data processing facilities, data files and documentation needed for processing to auditing and/or certification by the Data Exporter (or other duly qualified auditors of inspection authorities not reasonably objected to be the Data Importer and approved by the Data Exporter to ascertain compliance with the warranties and undertakings in these Clauses)" (see Clause 4).

Difficulty exercising individual rights

B2B contracts transferring personal data without the knowledge or consent of data subjects make it difficult for data subjects to "challenge data" relating to them. Although this does not negate the validity of using contractual solutions, it remains an outstanding issue.

What needs to be addressed is how the individual will know, or give consent to, the collection and transfer of her or his personal data (as required under the Collection Limitation Principle)? How will the contracting parties in a B2B transfer inform the individual of the purposes and uses for which personal data are transferred (per the OECD Purpose Specification Principle)? Will the individual be offered choice concerning or have the opportunity to consent to subsequent uses or disclosure of the data (per the Use Limitation Principle)? As mentioned above, a possible means of addressing these issues might be the solution adopted by the ICC Model Contract of giving the data subject rights of action against the data exporter.

The ICC model clauses solution

Applying the laws of the data exporter

The ICC Model Clauses address the issue of applicable law by requiring the data importer to comply either with data protection rules of the data exporter or a set of principles deemed to be adequate for data relating to citizens from the exporting country. This is consistent with the objective of the ICC Model Clauses: "to assist those who wish to transfer personal data from countries that regulate export of personal data to countries that do not provide protection for personal data that the source country finds adequate." A secondary benefit of the use of the ICC Model Clauses will be enhanced privacy protection for the personally identifiable information transferred pursuant to the contract where the receiving country does not provide effective privacy protection either through law or self-regulation."

The ICC Model Clauses require the data importer to permit the data subject the same rights she or he would have had against the data exporter in respect of the data prior to its export. This is a different issue from the data subject acquiring a directly enforceable right to sue under the B2B contract. The contractual position is that the data importer is assuming an obligation to ensure that the data subject can challenge the data (as this right is expressed in the applicable data protection law), such as by recognising any request for access to and the correction of his or her data.

Involvement of competent authorities

Another measure in the ICC Model Clauses is to incorporate the role of the data protection authorities or government supervisory agencies in redirecting complaints. The Clauses provide for undertakings by the data exporter to the effect that, "*the Data Exporter will promptly respond to inquiries from the Authority about the use of relevant personal data and to any Data Subjects' inquiry concerning use of her or his personal data, (including whether the same has been exported by it) and provide the inquirer with the name of the Data Importer and the individual responsible at the Data Importer who will be informed of the inquiry and who will respond to inquiries from its national authorities*".[7]

The effectiveness of this measure will be enhanced if the data subject is informed that her/his data are being processed and/or exported in the way contemplated by the B2B contract. Data protection rules will most likely require notice and choice. The effectiveness of this measure also depends on the ability of national data protection authorities to respond swiftly to inquiries made in the context of an ICC contract.

Involvement of the data subject

The dispute resolution provisions in the ICC Model Clauses expressly contemplate disputes involving the data subject. The data importer agrees to abide by the decision of the investigating data protection authority. A number of steps need to be taken before any dispute resolution process can commence; namely, notification and investigation of the data subject's complaint. The undertakings of the data importer include identification of an individual to deal with enquiries (and to notify the relevant authority) and to process complaints within the applicable timeframes of any data protection laws or self-regulation in the country of the data exporter.

Sanctions and remedies

"The ICC Model Clauses provide the data subject with the same rights as they would be entitled to in the country of the data exporter. The ICC Model Clauses also provide a right for the data exporter to terminate the agreement or to insist on the return or destruction of the data which is the cause of the data subject's complaint. One of the elements identified in the proposed common substantive reference for privacy clauses in a contract is the availability of remedies. Remedies for privacy breaches are a general issue that governments continue to grapple with and is not limited to contractual solutions. In the context of remedies for breach of contract, it is important to note that remedies vary from country to country. Examples of such remedies may include the following depending on the law of a member state: specific performance, rescission, restitution, and damages. Specific performance requires the party in breach to perform his/her obligations under the contract. Rescission is the cancellation of a contract and a return of the parties to their status prior to the contract. Restitution requires the party in breach to make the aggrieved party whole. In many countries, information is treated as an intangible to which it is very hard to assign a value. The significance is that, in a subsequent dispute the claimant may have difficulty quantifying their loss and proving that he or she has suffered loss or damage which has been caused by the breach of privacy obligations. It is important to note however that this difficulty is not unique to the contractual solution. Predetermined monetary compensation could constitute a remedy for breach of contractual obligations. Yet it may still be incumbent to demonstrate that the specified amount is based upon a genuine estimate of loss. This could be subject to challenge.

The need for directly enforceable rights under the contract

If the data protection authority or government supervisory agency cannot intervene to ensure the data subject obtains redress, the parties can discharge their obligations and take action against the other for any failure in this regard. This raises the issue of the data subject being able to sue the defaulting party under the B2B contract. In some jurisdictions, there may be an impediment in that the data subject is not a party to the contract (that is, there is no "privity of contract"). This impediment is being overcome as many countries have adopted laws which recognise the right of a third party, who is in receipt of a promise or other benefit under a contract, to enforce those particular obligations against the defaulting party.

This issue of the need for directly enforceable rights not only affects the data subject. If there is any onward transfer of the data by the importer to a third party, the exporter may have difficulty in ensuring privacy compliance. The exporter can impose contractual restrictions on the importer, to constrain subsequent processing and re-use (as is contemplated under the ICC Model Clauses). However, the exporter may have difficulties enforcing such restrictions, unless the law governing the contract allows the exporter (as a third party beneficiary to the primary contract between the importer and onwards transferee) to sue on that contract.

Informing the individual

Privacy notices and other awareness measures

The question of how the requirements of knowledge or consent of the data subject (such as under the OECD Privacy Guidelines) can be satisfied in the context of B2B contracts could be addressed by any ancillary measures which would not involve the design or content of the contract, but which would increase the awareness of data subjects as to the proposed uses of collected information.

If the requirements of the OECD Purpose Specification Principle are addressed by data exporters (or other collectors) at the time of collection, those data subjects will have a greater degree of

knowledge and therefore empowerment, to exercise their rights in respect of a data challenge. This could also lay the groundwork for the data subject to take action against the data exporter for misrepresentation.

Contracting directly with the data subject

In the context of providing redress to a data subject, the European Union's Article 29 Working Party[8] has suggested a "tripartite" solution, where the data exporter enters into a separate contractual agreement with the data subject when collecting the data, stipulating that the exporter will remain liable for the consequences of any failure by the importer to comply with an agreed set of data protection principles. This could be used to overcome the problem of insufficient knowledge as well as any lack of privity of contract. The data subject would be granted redress against the exporter for the default or failure of the importer. It would be up to the exporter to recover any damages paid to the data subject by taking a separate action for breach of contract against the importer. Such a suggestion may be helpful in the few countries that do not recognise third party beneficiaries.

This tripartite approach would be feasible where the subsequent TBDF could be anticipated at the time of collection. There may be certain categories where the contract with the data subject would become part of standard terms and conditions on which certain organisations provide services. This would also be consistent with the OECD Openness principle and the need for transparency that aims to ensure the data subject is informed of his or her privacy rights. Nevertheless, these tripartite agreements might prove cumbersome and impractical.

Economies of scale

Where the amount of data to be transferred is minimal, it may not justify the use of a specific TBDF contract. There do not appear to be any cases, which have been widely reported, where ad hoc TBDF contracts have been used between a business and data subject on a one-to-one or one-to-many basis.

Conclusions on recourse of the individual

Concern has been expressed about whether business to business contracts can provide individual recourse. Although B2B contracts may not achieve redress for the data subject in all cases, various measures have been proposed in initiatives such as the ICC Model Clauses to address this issue. These proposals might well provide an adequate remedy in the majority of cases. The contractual approach illustrated by the ICC Model Clauses allows for the involvement of a data protection authority or government supervisory agency. Other contracts might provide for private sector dispute resolution.

There are a number of other issues with B2B contracts, involving jurisdiction and choice of law issues and the impact of the EU Directive, particularly the adequacy requirements. Although these matters are extremely complex, they have been addressed in the course of the development of template or model clauses.

In some respects, the seemingly more mundane and lower profile issues are, in practical terms, more problematic; in particular, issues such as unequal resources between the parties and the data subject, or the lack of information on the purposes of collection and the subsequent re-use of the collected information as required under the OECD Privacy Guidelines. In this regard, certain suggestions that arise in the context of C2B transfers could be equally applicable to B2B contracts; for example, the measures discussed in sections 5 and 6 to provide the data subject with access to

rights-based information or education centres, greater reliance on an organisation's Privacy Statement, verification mechanisms, and recourse to a low cost, readily accessible dispute resolution process.

IV. Issues with C2B interactions

The discussion in this section focuses on the characteristics of consumer to business data interactions in an online environment and the significance of these characteristics in terms of the ability to apply contractual solutions to C2B transfers on the Internet. It explores what mechanisms could be modified, or developed, to realise the aim of improved privacy practices in order to protect personal data collected via the World Wide Web.

Impact of the Internet on privacy

Until the emergence of the Internet, there was comparatively little direct contact between a consumer located in one jurisdiction and a business located in another. Individuals might purchase goods or services when abroad on holiday, but otherwise any international transactions would take place through an organisation with a physical establishment in the consumer's jurisdiction (for example, an airline or credit card company).

The growth in electronic commerce has transformed this situation, especially in relation to contracts for information products and services (such as books, music CDs, software and subscriptions) and increasingly also for other products available by electronic mail order. There is a burgeoning global marketplace. For consumers armed with credit cards and Internet access, the location of a supplier becomes irrelevant.

It is also the case that, historically, some of the most effective privacy protection derived from barriers of cost, distance, inaccessibility, incompatibility and undiscoverability. The capabilities of the Internet have transformed this situation. As stated before, online TBDF (from C2B) creates both new challenges and new opportunities for privacy protection. Online TBDF facilitates the collection of personally identifiable information that can be used to create a personal profile of a user, knowledge and consent regarding the collection and use of the personally identifiable data should be offered and the data subject's choice should be respected. In that respect, the deployment of technological solutions can facilitate consumer empowerment. Personal profiles could then be used to tailor and customise interactions between individuals and businesses.

Common issues between B2B and C2B

Many of the issues relevant to B2B contracts will also be relevant in a C2B context:

- Information to the data subject on the collection of data and the purpose for which it is collected.
- Enforcement of privacy breaches.
- Effective verification mechanisms.

Differences between B2B and C2B

Despite this, some significant differences exist between the two categories of TBDF relationships, which may require the adoption of other strategies. In B2B contracts, both parties will almost certainly be regarded as processing personal data to which the provisions of national laws or the principles in international instruments such as the OECD Privacy guidelines will be relevant. In many cases, the transfer of personal data will be the prime purpose of the agreement; for example, the

sale of a list of names and addresses (increasingly e-mail addresses) which will be used for the purpose of direct marketing. In cases where the transfer is peripheral to the main purpose of the parties, for example the transfer of personal data concerning a passenger's itinerary between airlines within an international alliance, the transfer will take place in the context of an ongoing relationship between the parties.

The situation differs with C2B interactions. Often there will be no pre-existing relationship; the Web browsing may be random, with many first times or intermittent site visits. The exception is where the consumer has an established relationship, such as a history of ordering goods from a particular business or of applying for credit. The participants will also be removed from each other in terms of distance, time and geographical location. Despite this separation, the technical features of the medium are designed to facilitate data transfers. The disclosure of data is made possible through Web browsing software which provide the means to identify the network and machine used to access the Web, the URLs of previously visited sites, and by matching the information derived from the use of "cookies" with personal data. The data collection and storage is facilitated by caching and the availability of search engines, robots and Internet indexes.

The more overt data collection occurs when the consumer provides personal details in the course of a Web site interaction, whether of credit card and other payment details, contact details, personal preferences and so on. In transactions to acquire goods and services, the data transfer is usually incidental to the primary purpose.

As has already been mentioned, perhaps the most significant difference between B2B and C2B transactions is that the transfer of data will generally be initiated without a contract having been concluded between the participants. An example is where a business establishes a Web site from which it offers to supply goods or services. There is an analogy with a traditional shop. At the stage the consumer enters the shop, there is no existing contract with the storekeeper. Similarly, the act of accessing a Web site will not of itself suffice to establish a contractual relationship between the site owner and visitor. This is despite the fact that, where a Web site uses devices such as cookies to derive and match information to an identifiable individual, personal data may be collected from the moment the user accesses the site. As will be discussed further, this characteristic of online C2B interactions requires that any attempt to protect the privacy interests of the consumer begin prior to the contractual stage.

Need for a range of privacy measures to address C2B

If the characteristics of a C2B transfer are considered in light of the common substantive reference (discussed above), it may still be possible to address the privacy protection requirements, even though there may be difficulties in fitting the C2B interaction within a contract structure. It would require other ways to encourage businesses (data importers) to adopt privacy protection measures. There are obvious impediments in giving effect to a national data protection law in a networked environment where there is no geographical proximity of the various participants in an online TBDF and where territorial boundaries have been rendered irrelevant. There are constraints on the extent to which any national data protection law can have extra-territorial effect. Therefore, effective private or self-regulatory measures are an important means of achieving the aims of the OECD Privacy Guidelines.

With regard to the feasibility of a global privacy standard, an ad hoc advisory group on privacy undertook a study on behalf of the International Standards Organisation (ISO) to examine whether there is a need for an international standard to address information privacy, measure privacy protection and ensure global harmonisation. The advisory group concluded that it was premature to reach a

determination on the desirability and practicality of ISO undertaking the development of international standards relevant to the protection of personal data.

Importance of model privacy protection policies

In the context of C2B transfers, there may be an important role for educational measures to assist organisations in developing accurate privacy statements. An example is the privacy statement generated by the use of the Privacy Policy Statement Generator developed by the OECD (the tool is referred to as the "Generator" and its output as a "Statement"). The widespread practice of developing a formal privacy policy for a business (supplier/data importer), and then reflecting that policy in a statement such as the one produced with the help of the Generator, could have a cumulative but significant effect on the general level of awareness of consumers about the information-handling practices of the Web sites and businesses with whom they interact on the Web.

Certification measures for online transfers

Another consequence of the growth in global C2B transfers is the interest in developing verification tools or measures which would be suited to the online environment of the World Wide Web. In a global marketplace, where there is no direct or physical relationship between the parties to an interaction over the Web, issues of consumer trust and confidence become critically important. For this reason, the efforts to develop certification measures (including the use of privacy marks, labels and seals), can be seen as a proactive measure undertaken by the private sector to ensure consumer trust and confidence. This situation can be contrasted with those other privacy measures, which assume a complaints-based regime and place greater reliance on the ability of individuals to enforce and obtain redress in respect of the privacy obligations. The interest in verification measures is a realistic recognition of the logistical and legal barriers facing data subjects (consumers) in C2B transborder data flows.

Individual redress and enforcement

This line of discussion inevitably leads to the difficulties of pursuing individual redress and enforcement and to the need for dispute resolution options which are tailored to the particular characteristics and needs of C2B transfers. This is a conclusion, and area of interest, shared by other organisations who are currently addressing the implications of the GII, whether on the issue of dispute resolution mechanisms for electronic commerce transactions or to resolve complaints over domain name allocation. The significance of the issue of dispute resolution, and the availability of certain options, are discussed in section 6.

Benefits for business

The development of C2B privacy measures, such as Privacy Statements, might be seen primarily as benefiting the consumer. The approach may also assist businesses, especially small and medium-sized enterprises. Where suppliers lack a background in international trade, they may well be unaware of the legal requirements applying in other jurisdictions relating to matters such as data protection and direct marketing. The possibility of adopting model terms and policies may be of considerable benefit in limiting exposure to customer complaints (and even litigation) and to building consumer trust and confidence, which is a pre-requisite to successful competition in electronic commerce. However, a posted privacy statement can create legal liability for a business if it is not accurate. Therefore, any model policy or statement must be carefully reviewed by a business to ensure that it is consistent with the business' information practices and compliant with applicable regulation.

Issues with applying a contractual analysis to C2B

There are various legal requirements for the formation and content of an enforceable contract, and there are significant differences between national laws (on contracts). However, the following analysis aims to identify a number of common elements which, when applied in the context of contractual privacy solutions, pose difficulties for C2B transfers. A significant number of C2B interactions cannot be analysed in contractual terms. They either do not contain the elements of a contract or do not satisfy the pre-conditions to create a contract.

Requirements for the formation of a contract

In general, the doctrine of freedom of contract permits parties to contract in such manner and subject to such terms, as they think fit. Requirements that contracts be attested by the signatures of the parties, or otherwise concluded in writing, have been identified as impediments to the expansion of electronic commerce. Various proposals have been put forward to address these, such as by recognising the legal validity of electronic or digital signatures. These matters are outside the scope of this report.

The key requirement for the formation of a contract is that there should be an intention to creating a binding obligation, as evidenced by an offer from one party, which is accepted by the other. Where contracts are concluded at a distance, it may be important to determine at what point in time or in the ordering process, agreement is reached; that is, when does the contract become irrevocable? Once agreement is reached, neither party can unilaterally modify its terms although the original contract could provide for modification on notice from the business. Those pre-requisites may be of considerable importance in relation to data protection issues. If a consumer has not been informed of, nor agreed to, the supplier's intentions regarding the subsequent processing of personal data at the time the contract is concluded, is there still a binding contract in respect of the subsequent use of those data? On what basis can it be argued that the supplier (business) is constrained by the previous dealings or undertakings to protect the consumer's privacy?

In many legal jurisdictions, for a contract to be binding requires that there should be an offer from one party which is accepted by the other. It will be important to identify when these stages are reached. In general, when a supplier indicates that goods or services are available for supply, this does not of itself constitute an offer; rather the common law courts have treated this as an invitation to the consumer to make an offer. This offer may then be accepted by the supplier. The contract is formed. The exact timing of the formation will be dependent on the applicable rules of acceptance.

The rules of acceptance are now under review within those countries that are seeking to modernise their laws and provide greater certainty as to their application in an online environment. To illustrate, the EU Directive on Electronic Commerce acknowledges that a supplier may be treated as making the offer, but provides that:

> *"Member States shall lay down in their legislation that, save where otherwise agreed by professional persons, in cases where a recipient, in accepting a service provider's offer, is required to give his consent through technological means such as clicking on an icon, the contract is concluded when the recipient of the service has received from the service provider electronically, an acknowledgement of the recipient's acceptance." (Article 11)*

The acknowledgement, which must be sent immediately, will be deemed to have been received when it becomes accessible to the consumer. This is not necessarily the same as having been seen by

the consumer. Delivery of the acknowledgement into the consumer's electronic mailbox may suffice. This is another contract element which is currently under scrutiny.

Work is also being conducted by the International Chamber of Commerce (ICC) on the proposed establishment of Uniform Rules on Electronic Trade Settlement. These adopt a different approach by providing that:

> *"An electronic offer and/or acceptance becomes effective when it enters the information system of the recipient in a form capable of being processed by that system." (Rule 2.1)*

In the United States, the Uniform Computer Information Transactions Act provides that:

"SECTION 203. OFFER AND ACCEPTANCE IN GENERAL. Unless otherwise unambiguously indicated by the language or the circumstances:

(1) An offer to make a contract invites acceptance in any manner and by any medium reasonable under the circumstances.

(2) An order or other offer to acquire a copy for prompt or current delivery invites acceptance by either a prompt promise to ship or a prompt or current shipment of a conforming or non-conforming copy. However, a shipment of non-conforming copies is not an acceptance if the licensor reasonably notifies the licensee that the shipment is offered only as an accommodation to the licensee.

(3) If the beginning of a requested performance is a reasonable mode of acceptance, an offer or that is not notified of acceptance within a reasonable time may treat the offer as having lapsed before acceptance.

(4) If an offer in an electronic message evokes an electronic message in response, a contract is formed:

(A) when an electronic acceptance is received; or

(B) if the response consists of beginning performance, full performance, or giving access to information, when the performance is received or the access is enabled and necessary access materials are received."

Other circumstances influence the contractual analysis for TBDF. A complicating factor in many cases will be the consumer's use of a credit card to finance the transaction and the need to supply these details in advance. The card details may well be processed and verified by the supplier before the consumer is informed that the order has been accepted. Where the supplier has effectively accepted the consumer's money, it may be difficult to argue that a contract has not been concluded.

If Privacy Statements are to be incorporated in C2B contracts, it should be clear which version of a statement applies to any particular contract. Technical or procedural arrangements should be developed to ensure certainty in consumer contracts based on the content of Web pages and similar global network documents.

Reconciling the different approaches to online contracts

These examples demonstrate that the pre-requisites for contract formation in an online electronic environment are not yet settled. There is a range of approaches currently being advocated and considerable international effort is being spent to produce a harmonised approach to online contracts. This has significant implications for applying contract structures to C2B interactions on the Web.

When a consumer visits a Web site, the browsing activity can generate data . This is a form of data transfer; it could well be transborder. However, the consumer has not ordered any goods or services, but has been merely viewing and perhaps downloading information; the consumer is "window-shopping". It is unlikely that the contractual requirements of an intention to be bound, or offer and acceptance analysis, would apply to what is in essence only a communication or interaction.

For those C2B transfers, which are structured so as to form a contract, the outcome of the various initiatives on the contract requirements for electronic commerce transactions will be directly applicable to online C2B privacy contracts. These initiatives include the legal recognition of authentication measures (such as the use of electronic and digital signatures) and rationalising the evidentiary requirements. There is also on-going work to resolve conflicts of laws (choice of law and jurisdiction) in transborder transactions.

Use of the Internet to record contract formation

The information storage and recording capabilities of the Internet may also provide an opportunity. Unlike the vast majority of 'real life' contracts which may be entered into on an informal basis, with little if any recorded evidence of the fact of agreement and still less of the terms which have been negotiated, the use of the Internet provides the opportunity for the maintenance of a complete record of every act which took place during the formation and conclusion of a contract. The fact those data are recorded may be a privacy concern in its own right, but the existence of a record could assist in reconstructing all aspects of the contract formation process should this become necessary.

The potential of privacy policies and statements in C2B transfers

Privacy policies and statements are a means of giving notice to individuals. Such notices are capable of giving rise to both contractual and other legal obligations such as statutory or regulatory liabilities. Those obligations can be enforced depending on the nature of the liability and the rules of the particular jurisdiction - by contractual parties, individual data subjects, or public bodies.

The need for early warning on privacy

In order to afford the consumer genuine freedom of choice as to the transfer of data, notification of the uses to which personal data may be put should not only take place at the stage when a contract for the supply of goods or services is concluded, but privacy protection issues should also be brought to the consumer's attention at the earliest possible stage in the Web site interaction.

It would be quite possible for a site to adopt and publicise a privacy protection policy. This would inform the consumer of the nature of the data, which will be collected from the Web site visit, and the subsequent uses to which it may be put.

Enforcing a Privacy Statement

Privacy protection provisions incorporated into a C2B contract would entitle the consumer to take action to enforce these. But in some jurisdictions the legal status of privacy protection policies or statements may not be clear and there may be limited prospect of enforcement by an individual consumer. Either way, practical impediments should be overcome by any individual consumer who would attempt to issue proceedings against a business which is operating on the Web, given the amount of resources such actions require. There would be the difficulties of determining which court has jurisdiction, assuming it is even possible physically to locate the entity which has responsibility for

the Web site content or the information use and disclosure practices associated with that site. These are all reasons for designing dispute resolution mechanisms which would permit ready access by consumers and businesses alike, and which would gain widespread credibility and acceptance among business. The effort should be on designing online complaints and dispute resolution processes where the benefits of implementing and upholding those processes are self-evident to the businesses, Web site designers and Internet Service Providers who have control over online data transfers.

In the United States, the Federal Trade Commission (FTC) is authorised, under Section 5 of the FTC Act that prohibits unfair or deceptive acts or practices, to take action against organisations that engage in unfair and deceptive acts or practices in or affecting commerce. The FTC has stated that it is a deceptive practice to misrepresent in a material fashion the purpose for which information is being collected from consumers and how the information will be used. Such acts or practices could include misrepresentations by organisations that they adhere to their posted privacy statements, when, in fact, they do not.

The evidentiary, security and authentication requirements of a binding privacy contract would be no different from the issues in electronic commerce B2B contracts. The resolution of these issues (in the electronic commerce context) would need to be applied to C2B privacy contracts.

The need for verification mechanisms

The issue of verification, whether in the form of self-assessment, certification, labelling or otherwise, may be of considerable significance in the area of consumer to business transactions. The consumer must have faith in the information practices of a remote Web site, whose location is unknown and the identity of the persons or businesses responsible may prove to be untraceable. As there is limited prospect of negotiation between consumers and businesses regarding the terms of contracts, some form of third party involvement may be desirable to provide a form of approval that the contract satisfies the requisite standards or expectations for privacy protection and that the site or business is complying with its privacy obligations. A similar suggestion can be made with respect to privacy policy statements.

Options for online verification

The need for some form of verification mechanism has already been addressed in the discussion on B2B contracts. The ICC Model Clauses contemplate a range of options involving third party inspection or audit of the data importer's compliance with its privacy obligations. In the context of C2B transactions, this issue has been seen more as a consumer protection concern. The characteristics of the online environment, where the data are most likely collected via a Web site, has focused attention on the use of privacy marks, labels and seals as a form of certification, rather than the act of physical inspection or audit which presupposes physical proximity. There have been numerous international initiatives to develop verification measures for use on the Internet. Some of these are canvassed below.

The Better Business Bureau Online Privacy Seal, the TRUSTe Web site and the Japanese Mark systems on privacy protection, aim to offer new options to enhance privacy in an online environment. They could also be applied to the trans-national processing of personal data. Web sites always generate transborder data flows and therefore the US Web sites that are licensees of BBB Online and TRUSTe seal are in fact attempts to support privacy protection in a global online environment. They rest on self-regulatory schemes initiated by US private industry.

The Japanese Mark Systems on privacy protection are the Japanese Privacy Protection Mark System and the Granting Mark System. Since April l998, the Japan Information Processing Development Centre (JIPDEC) operates the former and the latter is operated by the Japan Data Communications Association. JIPDEC grants Privacy Marks after a process of certification in which the handling of personal data in compliance with MITI (Ministry of International Trade and Industry) Guidelines of l997 is monitored. The Japan Data Communications Association also grants the marks for telecommunication carriers and service providers, after assessing compliance with the MPT (Ministry of Posts and Telecommunications) Guidelines of l996 and l998.

Role of privacy-enhancing technologies

The World Wide Web Consortium (W3C) has launched the Platform for Privacy Preferences Project (P3P). This is intended to support a contractual agreement between information providers and users on the World Wide Web to allow in a flexible manner for the user's privacy preferences to be taken into account by the provider. Leading software manufacturers have announced that they will incorporate P3P into their latest versions once it is agreed by the W3C.

P3P relies on a number of technical conditions, which may not yet be in place. The browser software at the user end as well as the provider end will have to be compatible to allow for the necessary negotiation process between the PCs and servers. Different preferences may prevail in different parts of the world, (for example, in the EU and the US as opposed to Arab or Asian countries) raising compatibility issues.

Another example, which might be considered as the basis for action, is the Microsoft Merchant Server used to set up an electronic commerce operation. A wide range of retailers makes use of the software. The advantage of such a standardised set up is that there is an opportunity to build privacy policies into the design of the software. At present, however, it appears that privacy protection is addressed only in relation to the inclusion of encryption packages to enhance security for the exchange of financial data. Further consideration could be given to the possibility of working with major software developers and suppliers to ensure that the need for privacy protection is taken into account through all stages of the design, production and use.

Consumer protection initiatives

There are a number of parties, whether governmental or non-governmental, which could play a role in online user consumer protection including privacy. Examples might be Better Business Bureaux in the United States, which are charged to protect the interests of consumers.

The Better Business Bureau Online (BBB Online), TRUSTe, and WebTrust have formed and developed third party enforcement regimes that promote compliance with information practice codes. These enforcement regimes include the display of a seal or trust mark to notify consumers that Web sites follow fair information practices. All of these organisations provide dispute resolution mechanisms, monitor compliance, and impose consequences for non-compliance (sanctions or expulsion from the seal program). Companies that violate their stated information practices are also subject to FTC enforcement under Section 5 of the FTC Act.

Such bodies may well have an input into discussions although in some cases the associations are themselves active in commercial matters. In the United Kingdom, for example, the Consumers' Association sells books and magazines, provides its own credit card and operates as an ISP.

In some cases (for example, the Web Trader Scheme operated by the United Kingdom's Consumers' Association), accredited business is allowed to use an appropriate label on their Web sites. Businesses are required to undertake to observe a code of practice, which includes an obligation to conduct business in accordance with the terms of the Data Protection Act 1998. The Consumers' Association guarantees to make good up to GBP 50 of financial loss resulting from misuse of credit card details transmitted to an accredited trader. No liability is assumed for other losses including those resulting from breach of the Data Protection Act.

The existence of an umbrella organisation for businesses might offer potential for incorporating privacy terms and conditions as a pre-condition to obtaining admission to a Web site. An example of such an organisation is Bizrate. Located in Los Angeles, this operates a Web site containing listings of businesses in a wide range of categories. The condition attached to listing is that the business should accept assessment either by the organisation's staff or by its customers. In both cases, assessment is conducted on the basis of a wide range of features including the posted privacy policies. There may well be a valuable role for certification and labelling schemes to support other privacy measures, such as the use of Privacy Statements. Where the consumer and business are located in different countries, it may prove extremely difficult for the consumer to enforce any rights against the business. If alternative dispute resolution facilities were to be built into these schemes, this might provide a valuable addition to the consumer's legal rights, as discussed in the following section.

Enforcing the privacy commitment in C2B

The privacy rights of a consumer may be found in national laws and may be exercised in the prescribed manner. Most data protection regimes recognise electronic media and data so that if the online activity falls within the local jurisdiction, the consumer should have redress to the competent authority.

Reliance on contractual rights

Where a business indicates its adherence to a privacy protection policy, it is likely that compliance will be regarded as a term of any contract with the consumer. The C2B contract has an advantage over B2B, in that the data subject in a C2B transfer is most likely a party to the contract; and therefore the issue of lack of privity of contract would not be relevant. If a breach occurs, there may be a range of available legal remedies although in the environment of the Internet their efficacy may be questionable. In theory, any breach by the business of a contractual undertaking not to disclose personal data to third parties would be actionable by the consumer. Even though an action might be brought to interdict the business against further breaches, it would not undo the data transfer, and the consumer's redress might suffer from the same limitations as have been discussed under B2B court actions.

In cases where there is no contractual relationship between the consumer and the business (for example, the consumer's details have been recorded when visiting the site but no contract has resulted), it may be that the business would be in breach of its contractual obligations to any third party which has certified the acceptability of the business's privacy policies or which has permitted the use of a commendatory label. Historically, such situations have prompted concerns from common law countries, on the basis that contractual rights and remedies belong only to contracting parties, but as noted earlier, the contracts privity issue has been resolved by many countries enacting specific legislation to recognise third party beneficiary rights. There remains, of course, the query of how effective any available remedy might prove.

Availability of other civil remedies

The range of civil remedies available to a data subject is not limited to those found in privacy legislation. There may be a range of other applicable consumer protection laws. Typically, these prohibit unfair or misleading advertising, (see the OECD Inventory of Instruments and Mechanisms Contributing to the Implementation and Enforcement of the OECD Guidelines in Global Networks). 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, an online agreement (such as the terms and conditions associated with a registration form) or a transborder data flow contract. Such a breach may give rise to a number of possible civil remedies. Essentially, by providing notification of its privacy practices, a Web site represents or offers a commitment that it will follow these practices. Depending on the nature of the breach, most jurisdictions provide consumer protection and trade practices remedies for wrongful misrepresentations and/or fraudulent conduct if that commitment is broken.

Determining which law and jurisdiction should apply

Defining territoriality by geography

In a C2B transfer there can be many participants (or "actors"). It is quite simplistic to talk in terms of consumer to business. The Internet has many intermediaries, whether in the form of service providers or in the way the technology operates (utilising servers to host the Web page files, the routing of data packets through nodes around the world, and the practice of caching). Each of these actors (including data controllers) and activities may be "located" in different legal jurisdictions. It will probably be the norm rather than the exception that the participants in a C2B transfer are unknown to each other (rather than being seen as senders and recipients in a pre-determined relationship). The question, therefore, is which country's substantive legal rules should apply to a data transfer, message content or other activity, accessed via the Internet? Whose courts would have jurisdiction to adjudicate civil disputes and prosecute breaches? The presumptions of physical location and proximity (which are inherent in the linking of territoriality to geographical borders) are fundamentally challenged by the characteristics of global networks.

Choice of law and jurisdiction

The choice of law (jurisdiction to prescribe) will be highly significant in the adaptation and uptake of contractual privacy solutions. Although a forum may have personal jurisdiction and venue, the choice of law rules may require that the dispute be heard under the substantive law of another jurisdiction. Each country has its own private international law (forming part of its national or domestic law). Despite differences, there are on going efforts to harmonise the rules of conflict of laws. Many jurisdictions pursue common objectives and are influenced by the doctrine of comity and the need to respect the civil justice systems of other countries.

The question when and where a contract is concluded is a major factor in determining which legal system is to govern the particular transaction. As discussed, where transactions are conducted over the Internet, the question is not always easy to answer. The Global Top Level Domain name .COM gives no indication where a business is located. Even where the name uses a country code such as .DE or .UK, there is no guarantee that the business is established in that country. Key characteristics of the Internet are its re-routing ability and anonymity features.

In general, it is provided that contracting parties are permitted, subject to a criterion of reasonableness, to select which legal system will govern a particular transaction. Linked to this is the question of which national courts will have authority to rule on the interpretation of the contract.

Where parties are resident in different countries, for example, in Canada and Germany, it would be open to them to provide for example that the contract should be governed by Canadian law but that any disputes should be brought before the German courts.

Consumers' rights

Within Europe, the Brussels and Rome Conventions[9] provide for partial exceptions in the case of consumer contracts. The latter provides that a supplier with a "branch, agency or establishment" in the consumer's country of residence is to be considered as domiciled there. Consumers may choose to bring actions in either their country of domicile or that of the supplier, while actions against the consumer may be brought only in the consumer's country of domicile.

The question whether an Internet-based business can be regarded as having a "branch, agency or establishment" in all the countries from which its facilities may be accessed, is uncertain. The OECD has pointed out, in the context of tax harmonisation, that the notion of permanent establishment, which is of major importance in determining whether an undertaking is liable to national taxes, may not be appropriate for electronic commerce.

The Brussels Convention builds on the Rome Convention's provisions and provides that an international contract may not deprive the consumer of 'mandatory rights' operating in the consumer's country of domicile. The scope of mandatory rights is not clear-cut, but given the emphasis placed on the human rights dimension in many international instruments dealing with data protection, it is arguable that any contractual attempt to deprive consumers of rights conferred under the Council of Europe Convention and the EU Directive, would be declared ineffective on this basis.

In the United States, generally jurisdiction can be established based on a three-prong test: 1. purposeful availment of the privilege of doing business in the forum state; 2. the cause of action must arise from the defendant's activities with respect to the forum state; and 3. there must be a substantial enough nexus between the defendant's acts and the forum state to make the exercise of jurisdiction reasonable.

Developments in electronic commerce

More recent developments may complicate matters. The European Union has recently published a Directive in the field of Electronic Commerce. This provides that, albeit within the European Union, transactions entered into by electronic means should be regulated by the law of the supplier. This approach is justified on the basis of supporting the development of the e-commerce new industry. At the same time, however, the Commission is proposing amendments to the Brussels and Rome Conventions, which would have the effect of subjecting all consumer contracts to the law of the consumer's domicile.

Some believe that there is an inescapable tension between choice of law and jurisdiction provisions designed either to provide a predictable environment for suppliers or, on the other hand, to assist consumers in pursuing their remedies. Online alternative dispute resolution (ADR) may be the most effective means of overcoming this issue. In this regard, the 1999 OECD Guidelines for Consumer Protection in the Context of Electronic Commerce recommend the use and development of ADR mechanisms to address consumer complaints and to resolve consumer disputes arising from business to consumer electronic commerce, with special attention to cross-border transactions. There is a clear link between privacy and electronic commerce. The volume and nature of data transfers occurring in electronic commerce transactions is prompting privacy concerns. The lack of consumer trust and confidence in the level of protection afforded personal data, by the Internet, is an inhibiting

factor in the growth of electronic commerce. Yet, privacy protection (and the ability of data subjects to obtain redress) has its origins in human rights conventions and is also clearly a consumer protection issue. This tension will need to be reconciled. The issue of how much autonomy should the contracting parties have to determine their choice of law and jurisdiction will therefore be a key one.

Conclusions on C2B transfers

There is a need to take steps to protect consumer privacy on the Internet based on the OECD Privacy Guidelines. There is no single solution for the regulation of C2B data transfer. There are mechanisms to assist consumers in making informed choices about the collection and use of personally identifiable data prior to the conclusion of a contract.

Privacy protection policies, resulting in a posted statement, have a significant role to play. Tools such as the OECD Generator may assist companies in developing a privacy statement that may be a binding commitment. A significant role can be identified for consumer protection agencies and third party organisations to provide certification or verification services and tools; perhaps even to oversee the implementation and maintenance of policies by those businesses who have either committed to such an arrangement, or who are members of an industry or association and subject to a governing body or code of practice.

In many cases, in the context of C2B transfers, the focus would stay on preventive and educational measures such as privacy statements and verification. Even if the privacy statements prove ineffectual in terms of their contractual force, there would still be benefit to be derived from this measure because of the role of privacy policies in creating data subject and data controller awareness.

Education should not, however, be the only focus. Work may also be done on the benefits of prescribing in advance the applicable dispute resolution options. It may be possible to adapt the existing online dispute resolution projects to provide a tailored service capable of providing a first tier resolution for privacy disputes; in particular, where these are high volume and originate from individuals with insufficient resources to pursue their other legal remedies.

V. The need for appropriate alternative dispute resolution mechanisms

The availability of dispute resolution mechanisms to resolve disputes between data controllers (businesses) and data subjects (consumers) over TBDF, has been identified as a fundamental requirement by several member governments. There is a range of conventional and alternative dispute resolution mechanisms, which are described in this section. The discussion includes the advantages and disadvantages of each mechanism in respect of the specifics of the online environment that some observers have identified; a description of some of the international developments on online dispute resolution; and projects of interest to establishing mechanisms. Some possible suggestions for developing C2B online privacy dispute resolution mechanisms are provided as food for thought in the final part of this section.

Range of available dispute mechanisms

A critical consideration is what recourse the parties will have if a dispute arises. The following is a general discussion of the advantages and disadvantages of the various options, and of enforcement issues. The discussions on alternative dispute resolution (ADR) for the online environment are at a very preliminary point. In discussing options to address C2B disputes, the features of the dispute resolution mechanism are important. This discussion is to help to begin to identify key elements to be addressed for developing online mechanisms to resolve transborder C2B disputes.

Litigation

Litigation is always an option, but primarily in the B2B situation. The parties can agree that any dispute that may arise will be governed by the substantive law of a particular jurisdiction and submitted to the courts of a particular jurisdiction. Alternatively, if the parties have made no advance agreement, one party can, after a dispute has arisen, file a lawsuit in a particular jurisdiction. The parties could choose the forum where the contract was entered into, the forum where the contract was to be performed, or some other forum with a connection to the subject matter of the contract. In a B2B transaction there is a greater likelihood that such an agreement might be upheld by the relevant courts.

The situation changes, however, in a C2B transaction. The business entity may have a standard dispute resolution clause, which provides that any disputes must be resolved in the forum of the business entity. However, many jurisdictions are reluctant to impose a choice of jurisdiction provision against a consumer with less bargaining power. Many courts have invalidated a choice of forum selection, which compels a consumer to litigate in the forum of the business entity. There is therefore no guarantee that the courts of a given jurisdiction will uphold such a provision.

Advantages of litigation

A party may have the advantage of knowing that any dispute will be resolved in a forum with which it is familiar, and that the procedural and substantive law, which will be applied is one with which it has had experience. Unless the parties see a particular advantage to a particular forum, generally, only a party with a stronger bargaining position will be able to secure such an advance agreement.

The court will render a decision, which will set a precedent. To clarify a matter of law, it may be advantageous to proceed to litigation in order to have a final ruling on the matter. Other forms of dispute resolution generally do not provide the parties with a result that can set a precedent. Furthermore, litigation results in a final decision by a court, which the winning party will seek to enforce against the losing party. In most jurisdictions, the losing party has the right to appeal against an unfavourable decision. This right of appeal is not typically available in most other forms of dispute resolution

Disadvantages of litigation

There are also disadvantages. First, litigation can be lengthy: perhaps a period of years. In addition, litigation can be extremely costly. Furthermore, a losing party frequently has the right to appeal, thereby increasing both the cost and the length of the procedure. In most venues, litigation is not a confidential proceeding. Where a case is particularly sensitive, the public nature of litigation can be a deterrent. In addition, in cross border situations the winning party may still have to go to the losing party's jurisdiction to enforce the judgement.

Alternative dispute resolution

Parties to cross-border contracts can agree to submit disputes to alternative dispute resolution. The ADR mechanisms can be tailored to offer the parties maximum flexibility. Many ADR processes are consensual, rather than adjudicative. ADR combats certain disadvantages of litigation and arbitration, by being cheaper, faster, and broader in outlook and by allowing the parties more control over the process and the outcome. Below are presented some of the ADR options.

Arbitration

As with litigation, arbitration results in a binding decision, which can be enforced against the other party. In ad hoc arbitration the parties agree to arbitrate but do not choose one of the many arbitral institutions to administer the arbitration. While ad hoc arbitration may be less expensive than institutional arbitration, the parties will have to take on the organisational tasks normally carried out by the staff of the various institutional entities.

In "institutional" arbitration, the parties submit their dispute to one of the many recognised arbitral institutions, such as the International Chamber of Commerce ("ICC"), the American Arbitration Association ("AAA"), the World Intellectual Property Organisation ("WIPO") or the London Court of International Arbitration ("LCIA"). The parties can agree in their initial contract to submit any disputes to arbitration, or they can agree to do so after a particular dispute has arisen. If the parties agree to submit their dispute to institutional arbitration, they must follow the rules and procedures set forth by the respective institutions. Unless the parties have agreed, they are not bound by judicial rules of procedure and evidence, and frequently have more flexibility than they would in a court proceeding.

Advantages of arbitration

Arbitration has certain advantages: the parties are free to choose their respective arbitrators and the applicable law and procedure which will govern the arbitration; a party can chose an arbitrator with a particular expertise in a given field, and the parties can avoid litigating in the courts of their adversary. Generally, arbitration is less costly and faster than traditional litigation. The parties can provide for shortened time frames, which can speed up the arbitration and lower the cost.[10]

Arbitral awards are enforceable under the New York Convention on the Enforcement of Foreign Arbitral Awards.[11] Over 100 countries are signatories to this Convention. It requires the enforcement of a foreign arbitral award with limited exceptions. Enforcement of an arbitral award is frequently less complicated and costly than the enforcement of a foreign judgement, where one country may not necessarily recognise or allow for enforcement of a court judgement from a foreign jurisdiction.

Finally, with some exceptions,[12] arbitration is not a matter of public record, as with most litigation. The conduct of the proceedings and the decisions are typically not available to the public. This can be a significant advantage.

Disadvantages of arbitration

Arbitration is consensual. If a party does not consent to arbitration, it cannot be forced to. Arbitration can be time-consuming and expensive, and arbitral awards do not set a precedent, so the parties may end up arbitrating the same issue more than once with different parties.

Complex matters frequently arise where the rights of third parties must be adjudicated in order for a dispute to be finally resolved. Without the third party's consent to arbitration, the arbitral panel has no authority to make a decision binding the third party, and the proper recourse would be to litigation, assuming the courts had jurisdiction over the third party. So in a B2B contract where the issue in dispute was the rights of a third party (such as a data subject), arbitration may not be a practical method of dispute resolution.

Mediation

Mediation involves a structured procedure, facilitated by an independent third party. The authority of the mediator is consensual. The mediator assists the parties to the dispute to recognise each other's interests and to identify options for resolution, but has no power to give a view on an outcome or to impose a decision. Many organisations assist parties seeking to mediate. Typically, a party can withdraw from mediation at any time.

Advantages of mediation

Mediation provides a less formal but disciplined method for the resolution of disputes. The parties are free to select a mediator knowledgeable in a particular field and to agree the applicable law or self-regulatory principles or code of conduct that will govern the mediation, with more latitude than parties involved in traditional litigation. Procedural flexibility permits the parties to reach creative and innovative solutions to their disputes.

In a mediation, the parties are free, if they choose, to introduce any piece of evidence or information which might assist in the settlement of their dispute, and they can often reach agreement faster and at less cost than in a more traditional dispute resolution forum. Mediation is generally less adversarial and can be an ideal method of settling a dispute where the parties wish to continue in their relationship.

Disadvantages of mediation

The procedure, if successful, results in a settlement. Many courts will enforce those agreements. However, in other jurisdictions, courts will not enforce mediation agreements.

Mediation does not necessarily result in an agreement. The parties can agree to mediate but if unsuccessful in reaching an agreement, they would have to resort to another form of dispute resolution, such as litigation or arbitration.[13]

It is also possible for mediation to achieve widely disparate results, even in substantively similar disputes.

Mediation-arbitration ("med/arb")

In "med/arb" procedure, the parties provide that in the event of a dispute they will attempt to resolve the dispute by mediation but, if the mediation is unsuccessful, the parties will agree to submit the dispute to arbitration.

This has the advantage of significant cost and time savings if the parties are successful in reaching a solution via mediation, but still preserves the parties' right to seek an arbitral award if the mediation is unsuccessful. Generally med/arb is most successful when the parties put a time limit on how long they are willing to mediate before resorting to arbitration.

Mini-trials and expert determinations

Two other forms of ADR, are mini-trials and expert determination. A mini-trial is a procedure where the parties meet in the presence of a "Neutral" and, after hearing presentations on the merits, the Neutral gives an opinion on how a court would be likely to rule, hopefully facilitating a voluntary settlement between the parties. Under expert determination or evaluation, the parties agree to submit

certain key issues to an expert for determination. The parties can then incorporate the expert's findings into either a subsequent process or into a binding agreement.[14] These two methods have the advantage of speed and cost-efficiency. They are voluntary and the outcome is non-binding unless the parties agree to incorporate the expert's findings into a binding agreement.

Enforcement mechanisms

Conventional enforcement mechanisms

Even if litigation may be the last resort option, there is still the issue of the enforcement of any judgement. Notwithstanding international agreements such as the Brussels Convention and domestic rules such as the US requirement to give "full faith and credit" to judgements of other states, the problem of enforcing a foreign judgement remains.

The enforcement of foreign arbitral awards is governed by the New York Convention, which strictly limits the grounds for non-enforcement of an award. Therefore, a party who obtains an arbitral award is likely to be able to enforce it as long as the enforcement country is a signatory to the Convention.

Online enforcement mechanisms

Various online dispute resolution mechanisms have been created in the last few years, a number of which are described below. Enforcement is being addressed by some of these projects providing an escalation process. For example, BBBonline provides for a third party arbitration/mediation programme if a dispute cannot be resolved with the Subscriber Company.

Examples of online dispute resolution mechanisms

TRUSTe

TRUSTe[15] is a well-known initiative under which consumers can resolve issues relating to their individual privacy rights (TRUSTe) and other consumer issues. Web site owners sign a one-year contract with TRUSTe, which binds the user to certain privacy principles, and provides for escalation procedures in the event a dispute cannot be resolved. TRUSTe reviews the Web site, to ensure that it complies with the TRUSTe privacy principles. There is a dispute resolution mechanism, which provides for TRUSTe's review and escalation of the dispute resolution process if necessary.

BBBonline

Similarly, BBBonline[16] was established to help foster consumer trust and confidence in e-commerce. The BBBonline Privacy program offers a comprehensive assessment process to measure a company's ability to stand behind the promises it has made in its online privacy statement, and provides for a dispute resolution process in the event a consumer has a concern over a privacy issue.

WIPO

The WIPO Arbitration and Mediation Center provides dispute resolution services for challenges related to abusive registration and use of Internet domain names, commonly known as "cybersquatting", on the basis of the Uniform Domain Name Dispute Resolution Policy adopted by the Internet Corporation for Assigned Names and Numbers (ICANN). The Procedure is largely

conducted online[17], with online direct submission of complaints also being available. Cases are decided over an average period of 45 days against a basic fee of USD 1 500.

CRDP

The *Centre de Recherche en Droit Public* (CRDP) of the University of Montreal developed an experimental project known as CyberTribunal.[18] It sought to assist parties in both the prevention and resolution of disputes arising in cyberspace. The service tried to address the needs of both businesses and consumers. This experimental projected concluded in December 1999, but the work is continuing via another joint project, the details of which can be found at www.eresolution.ca.

NCAIR

The National Centre for Automated Information Research (NCAIR) has developed the Virtual Magistrate Project and the Online Ombuds Office, to assist parties in the resolution of disputes online.

Virtual Magistrate

The Virtual Magistrate Project[19] offers arbitration between users of online systems that claim to be harmed by posted content and the systems operators. Both parties must consent to the procedure, but the types of complaints are limited to include such issues as copyright infringement, defamation and invasion of privacy.

Online Ombuds Office

The Online Ombuds Office[20] ("OOO") allows users to search their Web site to obtain information that is relevant to their particular dispute. Users can request the assistance of one of the online ombudspersons who do not provide legal advice, but can discuss strategies that a party might employ for the successful resolution of a dispute.

The need for tailored dispute resolution mechanisms for online C2B transfers

Prescribing the dispute resolution process in advance

In order to promote consumer confidence, the service provider, except when acting as consumer, should make clear to which codes of conduct and ADR mechanisms he subscribes, and how information upon these codes and mechanisms can be obtained.

Fostering pragmatism

In B2B contracts, the parties can address their relationship and contract to comply with a dispute resolution process. By contrast, the nature of Web browsing makes it unrealistic to treat dispute resolution as something that the average consumer would intend to address before interacting on the Web. However, in order to foster consumer trust, businesses might well wish to promote and abide by dispute resolution mechanisms.

Considering options

From the earlier discussion of the advantages and disadvantages of dispute resolution mechanisms it seems that litigation, and possibly formal arbitration[21], are "last resort" options, whose effectiveness and adaptability may be limited in respect of online C2B interactions. However,

arbitration, modified to look more like the use of a third party arbiter with a simplified set of rules, could have direct application to online C2B dispute resolution.

The other options worth exploring are mediation, med/arb, independent expert evaluation (or expert determination) and conciliation. The latter category is a hybrid of a number of other mechanisms. The exact structure and operation of a conciliation process varies depending on the model and reflects particular types of dispute. The conciliator has the powers of both a mediator and an arbiter. This is distinct from processes such as mediation, which is then escalated to arbitration (med/arb).

Suggestions for developing C2B online alternative dispute resolution mechanisms

Developing dispute resolution for online C2B disputes requires consideration of factors, and the particular characteristics of C2B transfers. Below are some suggestions provided as food for thought.

Use of Privacy Policy Statements

A starting point could be to encourage businesses to inform the consumer of the complaints referral and investigation process they recommend, and to provide guidance on how to invoke these procedures.

Where a business has submitted to a verification process or applied for certification, its adherence to any described dispute resolution mechanism could be one of the matters to be assessed and verified. Verification would have to provide tangible value; it should not be unnecessarily costly or burdensome.

Requirement to exhaust prior remedies

Disputants could be required to exhaust their remedies under the prescribed process, before having recourse to litigation.

There are useful precedents such as industry specific dispute procedures in some jurisdictions, in the areas of insurance, telecommunications, banking and health services. Only after this avenue has been exhausted can the dispute proceed to litigation. Some data protection regimes (such as under the New Zealand privacy law) provide that all complaints must first be referred to the data protection authority for investigation and/or conciliation before they can proceed to the next tier in the dispute resolution process.

Alternatively, encouragement could be given to refer disputes to a dispute resolution service, but not to make this mandatory. Recourse to the court would occur where it is necessary for the data subject or consumer to obtain urgent interlocutory or injunctive relief, such as to prevent a proposed or continuing disclosure of personal data.

Choice of underlying philosophy

A key issue to be discussed is whether alternative C2B dispute resolution mechanisms should be consensual, as in most ADR mechanisms, or provide for a decision-maker with the power to impose a decision. Some options already available are:

- ***Independent expert evaluation (determination)****:* The parties could nominate an independent third party expert, or else there could be a panel of experts on which to draw.

- ***Conciliation***: This is a blend of mediation techniques and adjudicative. The process can draw on an independent expert. The conciliator can issue a recommendation, and sometimes issue an outcome. Alternatively, if the conciliator's recommendation is not followed, the matter is then automatically referred to some other process.

- ***A stepped or two-tier process:*** The dispute resolution process may commence as mediation but if there is no settlement, the process then converts to arbitration.

- ***Online arbitration.***

Other issues to be considered

Many other issues may also need to be considered. Some of those may include:

- The process to log or notify disputes.
- The notification of the parties, including the information to be forwarded to them and the rules governing communications; defining applicable criteria to "hear" the dispute.
- The appointment of any panel of experts.
- The appointment of the Neutral (arbiter/arbitrator/mediator/conciliator/expert).
- The protocols for identifying the information exchanges and any documentary or evidentiary requirements for dealing with the dispute.
- The protocols for establishing a record of the proceedings.
- Confidentiality.
- The security of the communications, and which transmissions must be encrypted.
- Possibilities to co-opt or involve third parties, such as:

    (a) Any data protection authority.
    (b) Any verification agent, inspector or auditor.

- The interface with any self-regulatory action or redress available under a governing industry code or rules.
- The ability or desirability of publishing: binding decisions; anonymized case notes; information providing particular guidance or insights; statistics; reports; the evidence in the proceedings.
- Any power to notify any applicable sector or industry body if the dispute affects a class of individuals or reveals a widespread practice (privacy violation).
- Any limits on the availability of sanctions (such as limits on financial compensation or particular powers of decision-making for the Neutral).
- Where there is no settlement, the advice to the data subject of other avenues of recourse and rights.
- Rules on the enforcement process in respect of any settlement agreement or a final decision or award.
- Self-assessment of the Service. There should be periodic reviews of the statistics for the Service, such as dispute types, resolution outcomes and the reason why some procedures are

preferred over others. The results of these reviews should be used to improve the design of the dispute system.

- The volume of disputes which any procedure could handle.
- The simplicity or complexity of the procedure, its timeliness, and cost.
- The possible need for several stages in a procedure between complaints handling and arbitration.

Other questions such as funding, control, oversight, accountability and quality should also be addressed.

Conclusions on dispute resolution mechanisms

Both businesses and consumers need to be able to have confidence in the use of global networks. Both will benefit from an effective mechanism for the resolution of disputes including privacy issues arising in online B-B and B-C transfers. The issues of dispute resolution are critical to improving the level of global privacy protection and development of tailored C2B online dispute resolution mechanisms has to be stimulated.

While some of the traditional mechanisms may be adapted to the resolution of online disputes, it is likely that new mechanisms will need to be developed. Especially in B2C and SME transactions, the cost, speed and enforceability of dispute resolution mechanisms are important considerations.

VI. Future initiatives

Summary of conclusions

It arises from the conclusions in this report that there is a role for contractual privacy solutions for transborder data flows occurring in the use of global networks. In particular, the potential of B2B contracts to satisfy the privacy protection expectations as measured against various privacy instruments, must be recognised. However, the report has identified various constraints on the use of B2B contracts. These limitations are not sufficient to negate the validity of privacy contractual solutions as a positive measure, the cumulative effect of which should improve fair information-handling practices and ensure transborder data flows. This is particularly so given the availability of a range of supplementary privacy protection measures.

Many of the B2B contractual issues are relevant to C2B transfers. However, the pressures and characteristics of the GII have significant implications for the use of contractual privacy solutions.

There are a number of initiatives, which have been identified as meriting further consideration. There are four themes, which emerge from the conclusions:

- The importance of promoting privacy awareness and providing educational tools.
- How to develop enforceable privacy commitments for online C2B transfers.
- The various international developments which require monitoring and further collaboration.
- The need to develop online alternative dispute resolution mechanisms for online C2B transfers.

Promoting privacy awareness and educational tools

In accordance with the Openness Principle of the OECD Privacy Guidelines, there should be continued emphasis on systemic measures to improve privacy procedures offering knowledge and/or consent where appropriate to ensure transparency and accountability. Data subjects need to be informed of the purposes of collection and processing of their data. This is a pre-requisite to their ability to challenge the accuracy and use of their data and to being able to pursue their rights, such as seeking redress.

In that respect, the OECD Privacy Policy Statement Generator is a practical measure to provide businesses with the tools to improve their level of awareness of their privacy responsibilities. It also provides the means for businesses (data controllers) to articulate their privacy policy. This educational function should continue to be encouraged; in particular, the correlation between improving consumer confidence and trust in the online environment and ensuring that those responsible for processing personal data act in accordance with the OECD privacy principles.

On the theme of data subject awareness, there may be an opportunity for a dedicated information page resource, made available through the technology (Web site) to inform data subjects of resources regarding laws and/or self-regulatory mechanisms.

Enforceable privacy commitments for online C2B transfers

Much of the data collection occurs prior to the time of formation of any contract. It is very difficult to establish a binding intention to contract, between a consumer browsing a Web site and the data controller of that Web site, until such time as the consumer engages the various prompts to select the goods or services advertised on the Web site, or by providing payment details.

In this context, privacy statements provide an opportunity for data controllers (Web site owners) to put the consumer on notice as to the applicable privacy obligations and as to a number of other matters which support privacy compliance. These may include any verification measures or certification processes applying to the Web site, any submission to the jurisdiction and governing law of a particular country, and the ability to stipulate in advance how complaints will be handled, especially the dispute resolution process.

Attempts to design privacy protection measures within the constraints of a contractual framework may pose difficulties due to the timing issues inherent in, and the nature of, C2B transfers. Even if a privacy statement were held to be a contract, there should be means for the consumer to obtain redress under that contract. There are many difficulties facing any individual consumer or data subject who takes legal action against an online business for breach of privacy through conventional litigation. With the aim of protecting privacy, it may be more efficient to focus less on contractual solutions, and more on dispute resolution measures, in particular on developing creative self-regulatory options in this regard.

Monitoring and collaboration

There are many international developments, which would need to be monitored in order to learn from these experiences when implementing contractual privacy solutions and ancillary measures. The areas to keep under review would include:

- Electronic commerce developments on the contractual requirements for acceptance, non-repudiation and authentication.

- Actual experiences with different forms of verification and certification measures, to assess their practicality, efficacy and benefits.
- Any further work based on the ICC Model Clauses.
- Any work rationalising the rules on conflicts of laws to address the borderless characteristics of the Internet and the difficulty to define territoriality in geographical or physical terms.
- The trend for countries to enact laws to recognise third party beneficiary rights under a contract (to avoid concerns over the lack of privity of contract).
- Any movement towards international co-operation on the legal recognition of statements, declarations or other forms of privacy policies, which would prescribe the dispute resolution processes to be followed.
- The various projects around the world to develop online dispute resolution measures.

Potential framework for encouraging the development of tailored online C2B pilot dispute resolution mechanisms

The importance of individual redress for a privacy breach appears to be a recurring theme. Irrespective of whether or not it is possible to apply a contractual framework to data collection via the Web, the "bottom line" is a pressing need to provide an effective level of privacy protection for consumers in C2B transfers. This includes fostering the opportunity for a consumer or data subject to file a complaint and to have that matter investigated and resolved, without resorting to a very expensive, time-consuming and complex process of issuing court proceedings. There would be corresponding benefits for business in terms of costs and time savings, possibly greater control over the procedure of dispute resolution, and in increasing credibility and certainty. All of these factors militate in favour of developing self-regulatory alternative dispute resolution mechanisms which could cater for high volume disputes arising out of online C2B transfers.

The development of the Privacy Policy Statement could provide an opportunity to describe how consumer complaints would be handled and any outstanding dispute resolved. A number of mechanisms could be adapted, ranging from mediation (a consensual process) to arbitration (an adjudicative measure).

To conclude, the very nature and scope of the medium in C2B transfers challenges the proposition that a "contract" could solve all the issues. Rather, it should be considered to take a macro approach and develop responses suited to a global privacy protection strategy. The OECD might usefully contribute to future work in this respect by taking forward some of the issues discussed in this report and in particular the study of online dispute resolution mechanisms.

NOTES

1. The eight Principles are: Collection Limitation Principle; Data Quality Principle; Purpose Specification Principle; Use Limitation Principle; Security Safeguards Principle; Openness Principle; Individual Participation Principle; Accountability Principle.

2. "Preliminary Views on the Use of Contractual Provisions in the Context of Transfers of Personal Data to Third Countries", 22 April 1998.

3. www.ntia.doc.gov/reports/privacydraft/198dftprin.htm.

4. Accountability Principle 14 "A data controller should be accountable for complying with measures which give effect to the principles stated above" OECD Privacy Guidelines.

5. Paras. 37-39; clause 4 Model Contract.

6. FIAT case (1989) and Deutsche Bahn (AG)/Citibank (1995).

7. Clause 4.

8. "Preliminary Views on the Use of Contractual Provisions in the Context of Transfers of Personal Data to Third Countries", 22 April 1998.

9. Brussels Convention 1968 on jurisdiction and the enforcement of judgements in civil and commercial matters. Rome Convention 80/934/CEE 19 June 1980 on the law applicable to contractual obligations 1980.

10. For example, the ICC Rules of Arbitration provide that the parties "may agree to shorten the various time limits set out in these rules". Rule 32.1, The ICC Rules of Arbitration (in force as of 1 January 1998). Several other arbitral institutions provide for similar procedures with respect to time-frames.

11. Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York Convention), 10 June 1958, entered into force 7 June 1959.

12. In the United States, arbitration decisions can be reviewed by the court to some extent and, as a result, are a matter of public record.

13. Many organisations, both international and domestic, offer mediation services, and different jurisdictions have laws governing mediation, which can vary widely. To combat the widely disparate body of law on mediation, many entities are seeking to draft model mediation codes or statutes. In the United States, for example, the American Bar Association, in conjunction with the National Conference of Commissioners on Uniform State Laws, drafted a Uniform Mediation Act, which is designed to replace the current mix of state laws on mediation (www.abanet.org/dispute). In Australasia, organisations such as Lawyers Engaged in Alternative Dispute Resolution (LEADR), and governing bodies of the law profession, have promoted uniformity through codes of ethics.

14. The International Chamber of Commerce offers this service through the ICC International Centre for Expertise. This Centre was created in 1976 and offers the parties the services of a wide variety of experts to assist them in various ways, including assistance in the resolution of disputes.

15. www.truste.org.

16. www.bbbonline.org.

17. http://arbiter.wipo.int/domains/rules/.

18. www.cybertribunal.org.

19. www.vmag.org.

20. www.ombuds.org/center/ombuds.html.

21. This conclusion assumes that the arbitration model involves the complex and formal procedures of submission to an appropriate arbitration forum.

ANNEX

WHERE TO FIND INFORMATION ON PRIVACY

CONTACT DETAILS FOR INTERNATIONAL AND REGIONAL ORGANISATIONS, NATIONAL GOVERNMENTAL AUTHORITIES, NON-GOVERNMENTAL ORGANISATIONS AND PRIVATE SECTOR ORGANISATIONS[1]

INTERNATIONAL AND EUROPEAN ORGANISATIONS

COUNCIL OF EUROPE
Data Protection Unit
Public Law Department
Directorate General of Legal Affairs
Secretariat General
67075 Strasbourg Cedex
France
Tel: 33 3 88 41 3174
Fax: 33 88 41 2764
E-mail: data.protection@coe.int
www.coe.int/dataprotection

Convention 108 - Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data: www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/International_legal_instruments/1Treaties.asp#TopOfPage

EUROPEAN COMMISSION
European Commission Legal Advisory Board
Directorate General XV-E1 (Free Movement of Information and Data Protection)
Rue de la loi 200 (C 107)
B 1049 Brussels
Belgium
Tel: +32 2 296 2264
Fax: +32 2 296 8010
Web site: http://europa.eu.int/comm/internal_market/en/dataprot/

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:
http://europa.eu.int/comm/internal_market/en/dataprot/law/index.htm

INTERNATIONAL CHAMBER OF COMMERCE
International Secretariat
38, Cours Albert 1er
75008 Paris
France
Tel: +33 1 49 53 28 28
Fax: +33 1 49 53 29 42
E-mail: icc@iccwbo.org
Web site:www.iccwbo.org/home/news_archives/2001/dataflow.asp

1. Please note that this list is not exhaustive.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT
Information, Computer and Communications Policy Committee
2 rue André-Pascal
75775 Paris Cedex 16
France
Tel: +33 1 45 24 82 00
Fax: +33 1 45 24 93 32
Web site: www.oecd.org/sti/security-privacy

Guidelines on the Protection Of Privacy and Transborder Flows of Personal Data:
www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

Guidelines for the Security of Information Systems: www.oecd.org/dataoecd/59/0/1946946.pdf

UNITED NATIONS
United Nations Centre for Human Rights
8-14 Avenue de la Paix
1211 Geneva 10
Switzerland
Tel: +41 22 917 3924
Fax: +41 22 917 0213
Web site: www.unhchr.ch/hchr_un.htm

Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly Resolution 45/95 of 14 December 1990: www.unhchr.ch/html/menu3/b/71.htm

WORLD TRADE ORGANISATION
World Trade Organisation
154 Rue de Lausanne
1211 Geneva 21
Switzerland
E-mail : enquiries@wto.org
Web site: www.wto.org/english/tratop_e/serv_e/gatsqa_e.htm
www.wto.org/english/tratop_e/serv_e/_derived/sourcecontrol_gats_factfiction10_e.htm

NATIONAL PRIVACY AND DATA PROTECTION AUTHORITIES

AUSTRIA
Büro der Datenschutzkommission und des Datenschutzrates
Bundeskanzleramt
Ballhausplatz 1
1014 Vienna
Tel: +43 1 531 15 25 28
Fax: +43 1 531 15 26 90
E-mail: georg.lechner@bka.gv.at
Web site: www.ris.bka.gv.at/

AUSTRALIA
Federal Privacy Commissioner
GPO Box 5218
Sydney NSW 2001
Tel: +61 2 9284 9800
Fax: +61 2 9284 96 66
E-mail: privacy@privacy.gov.au
Web site: www.privacy.gov.au

BELGIUM
Commission de la Protection de la vie privée
Boulevard de Waterloo 115 / Avenue de la Porte de Hal 5 - 8
Bruxelles 1060
Tel: +32 2 542 72 00
Fax: +32 2 542 72 12 / 7201
E-mail : privacy@euronet.be
Web site: www.privacy.fgov.be

CANADA[3]
Federal Privacy Commissioner
112 Kent Street
Ottawa Ontario K1A 1HR
Tel: +1 613 995 24 10
Fax: +1 613 947 68 50
E-mail: mai@magi.com
Web site: www.privcom.gc.ca

Provincial / Territorial Privacy Laws, Oversight Offices and Government Organisations
www.privcom.gc.ca/information/comms_e.asp

CZECH REPUBLIC[2]
Office for Personal Data Protection
Havelkova 22,
130 00 Praha 3
Tel: + 48 22 827 88 10
Fax: + 48 22 827 88 11
E-mail: info@uoou.cz
Web site: www.uoou.cz

DENMARK
Registertilsynet
Christians Brygge 28 - 4
1559 Copenhagen V
Tel: +45 33 14 38 44
Fax: +45 33 13 38 43
E-mail: sekretariatet@registertilsynet.dk
Web site: www.registertilsynet.dk

ESTONIA[2]
Estonia Inspection of Data Protection
Pikk 61
EE 10133 – Tallinn
Tel : +372 627 4135
Fax: +372 627 4137
E-mail : info@dp.gov.ee
Web site : www.dp.gov.ee

FINLAND
Office of the Data Protection Ombudsman
Albertinkatu 25 A, P.O. Box 315
00181 Helsinki
Tel: +358 9 259 8771
Fax: +358 9 259 87735
E-mail: tietosuoja@om.fi
Web site: www.tietosuoja.fi

---

2. Links to the national institutions responsible for personal data protection policy in the following countries: Czech republic; Estonia; Hungary; Lithuania; Latvia republic; Poland; Slovak Republic www.ceecprivacy.org (Central and Eastern Europe Data Protection Authorities Web Site).

FINLAND
Finnish Communications Regulatory Authority
Itämerenkatu 3 A, P.O. Box 800
00181 Helsinki
Tel: +358 9 69 661
Fax: +358 9 6966 410
E-mail: info@ficora.fi
Web site: www.ficora.fi

FRANCE
Commission Nationale de l'Informatique et des Libertés
21, rue Saint -Guillaume
75340 Paris Cedex 7
Tel: +33 1 53 73 22 22
Fax: +33 1 53 73 22 00
Minitel: 36-15 code CNIL
Web site: www.cnil.fr

GERMANY[3]
Der Bundesbeauftragte für den Datenschutz
Postfach 20 01 12
53131 Bonn (Bad Godesberg)
Tel: +49 228 - 819 950 or 01888 - 7799 - 0
Fax: +49 228 819 95 50
E-mail: poststelle@bfd.bund400.de
Web site: www.bfd.bund.de

German regional Privacy Commissioners
www.datenschutz.de/partner/

GREECE
Data Protection Commission
Omirou 8
105 64 Athens
Tel: +30 1 33 52 601-5
Fax: +30 1 33 52 617
E-mail: pdonos@dpa.gr
Web site: www.dpa.gr

GUERNSEY
Peter R Harris C. Eng, MA, PhD, FBCS
Data Protection Commission
PO Box 642
Frances House
Sir William Place
St. Peter Port
GY1 1JE
Tel: +44 (0) 1481 742074
Fax: +44 (0) 1481 742077
E-mail: dataprotection@gov.gg
Web site: www.dataprotection.gov.gg

3. Virtual Privacy Office: A common service of privacy protection institutions from the following countries: Canada; Germany; the Netherlands; Poland; the Slovak Republic and Switzerland: www.datenschutz.de.

HAWAII
Director
Office of Information Practices
Department of the Attorney General
Leiopapa a Kamehameha
Room 304
235 South Beretania Street
Honolulu
96813-2437.
Tel: +1 808 586 1400
Fax: +1 808 586 1412
Web site: www.state.hi.us/oip/rules_home_page.htm

HONG KONG
Privacy Commissioner
Office of the Privacy Commissioner for Personal Data (PCO)
Unit 2001, 20/F Office Tower, Convention Plaza
1 Harbour Road
Hong Kong – Wanchai
Tel: +852 2877 7168
Fax: +852 2877 7026
E-mail: hkpcpd@pco.org.hk
Web site: www.pco.org.hk

HUNGARY[2]
The Parliamentary Commissioner for Data Protection and Freedom of Information
1051 Budapest
Nádor u. 22.
Tel: +36 1 475 7186
Fax: +36 1 269 3541

ICELAND
Data Protection Commission
Ministry of Justice
Arnarvholl
150 Reykjavik
Tel: +354 560 90 10
Fax: +354 552 73 40
E-mail: afgreidsla@dkm.stjr.is

IRELAND
Data Protection Commissioner
Block 4 Irish Life Centre
Talbot Street
Dublin 1
Tel: +353 1 874 85 44
Fax: +353 1 874 54 05
E-mail: info@dataprivacy.ie
Web site: www.irlgov.ie/justice/Publications/publications.htm

ISLE OF MAN
Isle of Man Data Protection Registrar
Office of the Data Protection Registrar
PO Box 69
Douglas
Isle of Man IM99 1EQ
Tel: +1624 661030
Fax: +1624 661088
Web site: www.gov.im/odpr/

ISRAEL
Registrar of Data Bases
Ministry of Justice
6 Hillel Street
P.O. Box 2808
Israel - Jerusalem 91027
Tel: +972 2 625 56 50
Fax: +972 2 622 27 80

ITALY
Garante per la protezione dei dati personali
Largo del Teatro Valle, 6
00186 Roma
Tel: +39 06 - 68 18 61
Fax: +39 6 681 86 50
Web site: www.privacy.it/normativ.html

JAPAN
Ministry of Public Management, Home Affairs, Post and Telecommunications
2-1-2 Kasumigaseki
Chiyoda-ku Tokyo 100 – 8926
Tel: +81 3 5253 5359
Fax: +81 3 5253 5345
E-mail: opinions-2002@soumu.go.jp
Web site: www.soumu.go.jp

JERSEY
Data Protection Registrar
Data Protection Registry
Morier House
Halkett Place
St Helier
JE1 1DD
Channel Islands
Tel: +1534 5023255
Fax: +1534 502399

LATVIA REPUBLIC[2]
Data State Inspection
Kr.Barona iela 5-4,
Riga, Latvia, LV 1050
Tel: +371 7223131
Fax: +371 7223556

LITHUANIA[2]
State Data Protection Inspectorate
under the Ministry of Public Administration Reforms and Local Authorities
Gedimino Str. 27/2
2600, Vilnius
Tel: +370 5 212 75 32
Fax: +370 2 61 94 94
E–mail: jakstaite@is.lt
Web site: www.is.lt/dsinsp

LUXEMBOURG
Commission à la Protection des Données Nominatives
Ministère de la Justice
Boulevard Royal , 15
Tel: +352 478 45 46
Fax: +352 22 76 61

NETHERLANDS[3]
College Bescherming Persoonsgegevens (CBP)
Prins Clauslaan 20
P.O. Box 93374
2509 AJ The Hague
Tel: +31 70 381 13 00
Fax: +31 70 381 13 01
E-mail: info@cbpweb.nl
Web site: www.cbpweb.nl

NEW ZEALAND
The Office of the Privacy Commissioner
P.O. Box 466
Auckland
Tel: +64 9 302 21 60
Fax: +64 9 302 23 05
E-mail: privacy@iprolink.co.nz
Web site: www.privacy.org.nz

NORWAY
Datatilsynet / The Data Inspectorate
P.O. Box 8177 Dep
0034 Oslo
Tel: +47 22 39 69 00
Fax: +47 22 42 23 50
E-mail: postkasse@datatilsynet.no
Web site: www.datatilsynet.no

POLAND[2, 3]
The Office of the General Inspector of Data Protection
PL. Powstancow Warsawy 1
00 030 Warsawa
Tel : +48 22 827 88 10
Fax: +48 22 827 88 11
E-mail : sekretariat@giodo.gov.pl or dif@giodo.gov.pl
Web site: www.giodo.gov.pl

PORTUGAL
Commissao Nacional de Proteccao de Dados Pessoais Informatizados
Rua de Sao Bento 148
1200 Lisboa
Tel: +351 1 392 84 00
Fax: +351 1 397 68 32
E-mail: cnpdpi@mail.telepac.pt
Web site: www.cnpdpi.pt or www.cnpd.pt

SLOVAK REPUBLIC[2, 3]
Office for Personal Data Protection
Mr Pavol Husar - President
Odborárske nám. 3
817 60 Bratislava
Tel: +421 2 5023 9418
Fax: +421 2 5023 9441
E-mail: statny.dozor@pdp.gov.sk or pavol.husar@pdp.gov.sk
Web site: www.dataprotection.gov.sk

SLOVAK REPUBLIC[2, 3]
National Security Authority
Budatínska 30
850 07 Bratislava
Tel: +421 2 6869 9519
Fax: +421 2 6382 4005
E-mail: info@nbusr.sk
Web site: www.nbusr.sk

SLOVENIA
Ministry of Justice
Zupanciceva 3
1000 Lubjana
Tel : +386 61 17 85 549
Fax: +386 61 12 61 050
E-mail : Joze.Santavec@gov.si

SPAIN
Agencia de Protección de Datos
Paseo de la Castellana 41, 5a planta
Madrid 28046
Tel: +34 1 308 40 17
Fax: +34 1 308 46 92
E-mail: rel.internacionales@agenciaprotecciondatos.org
Web site: www.ag-protecciondatos.es

SWEDEN
Datainspektionen
Fleminggatan, 14, 9th Floor
Box 8114
104 20 Stockholm
Tel: +46 8 - 657 61 00
Fax: +46 8 652 86 52
E-mail: Datainspektionen@din.se
Web site: www.din.se/index.html

SWITZERLAND[3]
Préposé fédéral à la protection des données / Data Protection Commissioner
Feldeggweg 1
3003 Berne
Tel: +41 31 322 43 95
Fax: +41 31 325 99 96
E-mail: info@edsb.ch
Web site: www.edsb.ch

TAIWAN
Prosecutor, Bureau of Legal Affairs
The Ministry of Justice
130 Sec 1 Chung Ching
South Road
Taipei 100 ROC 100
Tel: +886 2 381 39 39
Fax: +886 2 311 49 00

UNITED KINGDOM
The Office of the Data Protection Registrar
Water Lane
Wycliffe House
Wilmslow
Cheshire SK9 5AF
Tel: +44 (0) 1625 - 53 57 11
Fax: +44 (0) 1625 524 510
E-mail: data@wycliffe.demon.co.uk
Web site: www.dataprotection.gov.uk

UNITED STATES
National Telecommunications & Information Adm.
US Department of Commerce - Room 4713
14th & Constitution Avenue NW
Washington DC 20230
Tel: +1 202 48 21 816
Fax: +1 202 50 18 013
E-mail: privacy@ntia.doc.gov

Federal Trade Commission
6th & Pennsylvania Avenue, N.W.
Washington, DC 20580
Tel: +1 202 FTC-HELP (382-4357)
Fax: +1 202 326-2012 attn: CRC
Web site: www.ftc.gov/index.html

Department of Commerce
International Trade Administration
Office of Information Technologies & Electronic Commerce
14th & Constitution Avenue, N.W.
Washington, DC 20230
Tel: +1 202 482-0216
Fax: +1 202 482-5522
Web site: http://export.gov/infotech

Office of Management and Budget
Executive Office of the President
725 17th Street, NW
Washington, DC 20503
TeleTel : 1 202 395 3080
Fax: 1 202 395 3888
Web : www.whitehouse.gov/omb/

Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554
Tel: +1 202 418 0200
Fax: +1 202 418 0232
Web site: www.fcc.gov/

Department of the Treasury
1500 Pennsylvania Avenue, NW
Washington, DC 20220
Tel: +1 202 622 2000
Fax: +1 200 622 6415
Web : www.ustreas.gov/

UNITED STATES
United States Department of Health and Human Services
200 Independence Avenue, SW
Washington DC 20201
Tel: +1 202 619 0257
E-mail: hhsmail@os.dhhs.gov
Web site: www.os.dhhs.gov/

NON-GOVERNMENTAL ORGANISATIONS

CENTER FOR DEMOCRACY AND TECHNOLOGY
1634 Eye Street NW
Suite 1100
Washington DC 20006
Tel: +1 202 637 9800
Fax: +1 202 637 0968
Web site: www.cdt.org/

ELECTRONIC FRONTIER FOUNDATION
1550 Bryant Street, Suite 725
San Francisco CA 94103-4832
Tel: +1 415 436 9333
Fax: +1 415 436 9993
Web site: www.eff.org/

ELECTRONIC PRIVACY INFORMATION CENTER
666 Pennsylvania Ave SE
Suite 301
Washington, DC 20003
Tel: +1 202 544 9240
Fax: +1 202 547 5482
E-mail: info@epic.org
Web site: www.epic.org/

FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION
B.C. Freedom of Information and Privacy Association
#204-1929 West Broadway
Vancouver, B.C.
V6J 1Z3
Tel: +1 604 739-9788
Fax: +1 604 739-9148
Web site: griffin.multimedia.edu/~fipa/

GLOBAL WEB SITE LIBERTY CAMPAIGN
Web site: www.gilc.org/index.htm

INFORMATION TECHNOLOGY INDUSTRY COUNCIL
1250 Eye Street NW Suite 200
Washington, DC 20005
Tel: +1 202 737 8888
Fax: +1 202 638 4922
Web site: www.itic.org

THE NATIONAL BUSINESS COALITION ON E-COMMERCE AND PRIVACY
601 Pennsylvania Avenue NW, North Building 11th Floor
Washington, DC 20004-2601
Tel: +1 202 756 3385
Fax: +1 202 756 3333
E-mail: jschall@practicalprivacy.org
Web site: www.practicalprivacy.org/nbcpe/index.htm

ONLINE PRIVACY ALLIANCE
c/o Christine Varney
Hogan and Hartson
555 13th Street NW
Washington, DC 20004
Tel: +1 202 637 5600
E-mail: webmaster@privacyalliance.org
Web site: www.privacyalliance.org/

PRIVACY AND AMERICAN BUSINESS
2 University Plaza
Hackensack, NJ 07601
Tel: +1 201 996 1154
Fax: +1 201 996 1883
E-mail: pab@idt.net or ctrslr@aol.com
Web site: www.pandab.org/

PRIVACY COUNCIL
1300 East Arapaho, Suite #300
Richardson, Texas 75081
Tel: +1 972 997 4001, or 866 P-Council (866.726.8624)
Fax: +1 972 997 4450
E-mail: info@privacycouncil.com
Web site: www.privacycouncil.com/

PRIVACYEXCHANGE.ORG
C/o Centre for Social and Legal Research
2 University Plaza, Suite 414
Hackensack, NJ 07601
Tel: +1 201 996 1154
Fax: +1 201 996 1883
E-mail: ctrslr@aol.com or admin@privacyexchange.org
Web site: www.privacyexchange.org/

PRIVACY FORUM
Vortex Technology
Woodland Hills
California
Tel: +1 818 225 2800
Fax: +1 818 225 7203
Web site: www.vortex.com/privacy.html

PRIVACY INTERNATIONAL
Privacy International Washington Office
666 Pennsylvania Ave, SE, Suite 301
Washington, DC 20003
Tel: +1 202 544 9240
Fax: +1 202 547 5482
Web site: www.privacy.org/pi

PRIVACY RIGHTS CLEARING HOUSE
3100 - 5th Ave., Suite B
San Diego CA 92101
Tel: +1 619 298 3396
Fax: +1 619 298 5681
E-mail: prc@privacyrights.org
Web site: www.privacyrights.org

WORLD WIDE WEB CONSORTIUM
Web site: www.w3.org/

PRIVATE SECTOR ORGANISATIONS

AT&T
AT&T Corp.
The Platform for Privacy Preferences (P3P) Project
295 North Maple Avenue
Basking Ridge, NJ 07920
United States
Tel: +1 973 360 8607
E-mail: lorrie@research.att.com
Web site: www.research.att.com/projects/p3p/

BBBOnLine, Inc.
4200 Wilson Boulevard
8th Floor
Arlington, VA 22203
United States
Tel: (Reliability Seal Program) +1 703 247 9370
Tel: (Privacy Seal Program) +1 703 247 9336
Tel: (Online Privacy Dispute Resolution Intake Center) +1 888 679-3353
Fax: +1 703 276-8112
Web site: www.bbbonline.org/about/contactinfo.html

DIRECT MARKETING ASSOCIATION
Direct Marketing Association
1120 Avenue of the Americas
New York, NY 10036-6700
Tel: +1 212 768 7277
Fax: +1 212 302 6714
Web site: www.the-dma.org/

JAPAN INFORMATION PROCESSING DEVELOPMENT CENTRE
Kikai Shinko Bldg, 3-5-8, Shibakoen, Minato-ku,
Tokyo, 105-0011
Japan
Tel: +81 3 3432 9387
Fax: +81 3 3432 9419
Web site: www.jipdec.orjp/security/privacy

PRIVACY TIMES
P.O. Box 21501
Washington DC 20009
Tel: +1 301 229 7002
E-mail evan@privacytimes.com
Web site: www.privacytimes.com/

TRUSTe
685 Market Street, Suite 560
San Francisco, CA 94105
United States
Tel: +1 415 618 3400
Fax: +1 415 618 3420.
E-mail: inquiries@truste.org
Web site : www.truste.org

OECD PUBLICATIONS, 2, rue André-Pascal, 75775 PARIS CEDEX 16
PRINTED IN FRANCE
(93 2003 05 1 P) ISBN 92-64-10162-4 – No. 53251 2003