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

OLIS : 24-Jul-1998
Dist. : 29-Jul-1998

Or. Eng.

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

DSTI/ICCP/REG(98)5/FINAL
Unclassified

Group of Experts on Information Security and Privacy

PRIVACY PROTECTION IN A GLOBAL NETWORKED SOCIETY

AN OECD INTERNATIONAL WORKSHOP WITH THE SUPPORT OF THE BUSINESS AND INDUSTRY ADVISORY COMMITTEE (BIAC)

OECD, Paris, 16-17 February 1998

67819

Or. Eng.

TABLE OF CONTENTS

NOTE BY THE SECRETARIAT....4

PREFACE....5

ORIENTATION REPORT....8

EXECUTIVE SUMMARY OF THE WORKSHOP....21

RAPPORTEUR'S REPORT....24

LIST OF PARTICIPANTS....44

NOTE BY THE SECRETARIAT

The Business and Industry Advisory Committee to the OECD (BIAC) was pleased to sponsor the OECD Workshop on Privacy Protection in a Global Networked Society (Paris, 16-17 February 1998), and would like to thank the companies and organisations which made this support possible:

America Online Incorporated
Citibank
International Federation of Direct Marketing Associations
IBM
Microsoft Europe
Shell Services International B.V

PREFACE

Privacy Protection in a Global Networked Society

Among the conclusions of the OECD Conference "Dismantling the Barriers to Global Electronic Commerce" held in Turku, Finland, on 19-21 November 1997, was that privacy protection is one of the critical elements of consumer and user trust in the online environment and a sine qua non for the development of electronic commerce.

The protection of privacy in the context of global information and communication networks will be one of the issues to be dealt with at the OECD Ministerial level Conference "A Borderless World: Realising the Potential of Global Electronic Commerce" to be held in Ottawa on 7-9 October 1998. The discussion of Ministers at the Conference could launch action in this area to be pursued over the next few years, along with activities in other key areas, such as taxation and consumer protection.

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 (GII/GIS), its history in developing the 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) outlined the concerns relating to privacy expressed by a number of network users and covered diverse initiatives undertaken by the private sector to develop privacy-enhancing technologies for global networks.

It proposed that OECD Member governments:

- reaffirm that the Privacy Guidelines are applicable with regard to any technology used for collecting and processing data;
- encourage those businesses who choose to expand their activities to information and communication networks to adopt policies and technical solutions which will guarantee the protection of the privacy of individuals on these networks, and particularly on the Internet; and
- foster public education on issues related to protection of privacy and the use of technology.

With that goal in mind, the report proposed to launch, among the OECD Member countries, a dialogue involving governments, industry and businesses, individual users and data protection authorities, to discuss trends, issues and policies in this area.

In that context, a workshop entitled "Privacy Protection in a Global Networked Society" was organised with the support of the BIAC on 16-17 February 1998. The workshop was intended to offer participants a balanced presentation of the issues linked to the protection of privacy and transborder flows of personal data in the developing global networked society. It brought together representatives of governments, the private sector, the user and consumer communities, and data protection authorities 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 an effective bridge between the type of policies for protection of personal data offered by the legislators in the European Union and the different policies of other Member countries. Furthermore an important focus was put on encouraging the private sector to provide meaningful protection for personal data on global networks by effective self-regulation.

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

- identifying and balancing the needs of the private sector and of those of users and consumers and formulating efficient strategies for "educating for privacy";
- developing "privacy enhancing technologies";
- implementing private sector-developed enforcement mechanisms for privacy codes of conduct and standards; and
- adopting model contractual solutions for transborder data flows.

The Workshop was chaired by **Michelle d'Auray**, Executive Director of the Electronic Commerce Task Force, Industry Canada. **Lord Williams of Mostyn**, Parliamentary Under-Secretary of State, Home Office, UK; **Guy Braibant**, Président de section honoraire au Conseil d'Etat, France; and **Mozelle W. Thompson**, Commissioner, Federal Trade Commission, US delivered keynote addresses. The four main sessions were chaired by **Professor Mads Bryde Andersen**, Copenhagen University, Denmark; **Roger Needham**, Pro-Vice-Chancellor and Professor of Computer Systems, University of Cambridge, UK; **Barbara Wellbery**, Special Counsel for Electronic Commerce, Department of Commerce, US; and **Philippe Lemoine**, Vice Président Directeur Général du Groupe Galeries Lafayette, France. Other Workshop participants included government representatives, European data protection authorities, industry experts, academics and consumer policy experts from OECD Member countries.

At the end of the Workshop, participants recognised that the growth of electronic commerce requires increased consumer confidence in privacy protection, and that the OECD Guidelines continue to provide a common set of fundamental principles for guiding efforts in this area. They affirmed the commitment to protect individual privacy in the increasingly networked environment, both to uphold human rights and to prevent interruptions in transborder data flows.

The Chair noted widespread consensus that the need to balance the benefits of free flow of information in the online medium with the need to protect 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 assess their practical application in a networked environment and their ability to meet the objectives of the OECD Guidelines (including effectiveness, enforceability, redress and coverage across jurisdictions.) Such a study would serve to identify gaps and barriers to interoperability, and suggest solutions to provide seamless privacy protection.

PRIVACY PROTECTION IN A GLOBAL NETWORKED SOCIETY

AN OECD INTERNATIONAL WORKSHOP WITH THE SUPPORT OF THE BUSINESS AND INDUSTRY ADVISORY COMMITTEE TO THE OECD

OECD, Paris, 16-17 February 1998

ORIENTATION REPORT

INTRODUCTION

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Privacy Guidelines) were adopted on 23 September 1980 as a Recommendation of the Council of the Organisation for Economic Co-operation and Development (OECD).

In adopting these Guidelines, the OECD Member countries clearly intended to "help to harmonise national privacy legislation and, while upholding such human rights, to prevent at the same time interruptions in international flows of data".

Since then, the Recommendation has proved to represent international consensus on general guidance concerning the collection and management of personal information. The principles contained in the OECD Privacy Guidelines are reflected in privacy legislation world-wide. Moreover these principles were designed in a technology-neutral way to accommodate future developments: they are still applicable with regard to any technology used for collecting and processing data, including network technologies.

In the context of the work of the OECD on the global information society and electronic commerce, the Group of Experts on Information Security and Privacy, under the auspices of the Committee for Information, Computer and Communications Policy, decided in October 1997 to organise this Workshop on the theme of "Privacy Protection in a Global Networked Society".

Convergence of technologies in global networks offers enormous social and economic benefits of all types and presents a number of challenges to traditional structures including the increased exchange of information by a growing number of entities, the ease of crossing national borders and the lack of centralised control mechanisms. As a result, national or regional policies and traditional methods for implementing them offer incomplete responses to the issues arising in the global information infrastructure. To enhance its success the new global information society requires the convergence of government policies, the transparency of rules and regulations and their effective implementation on information networks possibly through the use of new mechanisms and technological tools. These elements, of which important aspects deal with the protection of privacy and personal data, are essential for the establishment of a trustworthy global electronic environment and also crucial to prevent obstacles to transborder data flows.

Given its ongoing work in the area of the global information infrastructure and the global information society (GII/GIS), its history in developing the Privacy Guidelines and its continuing experience in issues related to privacy protection, the OECD has decided to consider the various solutions which would facilitate the implementation of the privacy principles in the context of international networks and contribute towards building a trustworthy environment for the development of electronic commerce.

The **objective** of this Workshop is to bring together representatives from the 29 OECD Member countries to engage in a dialogue among governments, the private sector, the user and consumer communities, and data protection authorities to focus on how the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data may be implemented in the context of global networks. In organising this Workshop, the OECD wishes to build on the various approaches adopted by its Member countries *and help to identify mechanisms and technological tools that could provide an effective bridge between* the level of protection of personal data guaranteed by the legislators in the European Union, and the *different policies* of other Member countries, of encouraging industry and commerce to provide meaningful protection for personal data by effective self-regulation.

With this goal in mind, the Workshop is designed to identify appropriate practical solutions for the protection of privacy and personal data which would be tailored to international networks and which could be implemented irrespective of the different cultural approaches. It intends to offer participants a balanced understanding of the issues linked to the protection of privacy and transborder flows of personal data in the developing global networked society.

Out of the various solutions which might assist with the implementation of the OECD Privacy Guidelines in the context of international networks, the following have been identified and will be discussed in separate sessions:

- identifying and balancing the needs of the private sector and of those of users and consumers and formulating efficient strategies to educate for privacy;
- developing privacy enhancing technologies;
- implementing private sector-developed mechanisms to enforce privacy codes of conduct and standards;
- adopting model contractual solutions for transborder data flows.

This orientation document is structured so as to present, for each session, the issues and main points to be examined. It also briefly introduces the presentations to be given in order to prepare and stimulate the discussion amongst participants. It proposes, at the end of each session, a provisional list of questions to be examined during the discussion. The role of this document is to provide food for thought, the essential task of the Workshop being the discussion between participants and the development of conclusions.

These conclusions will be presented to the Group of Experts on Information Security and Privacy and to the ICCP Committee. Based on these conclusions, OECD Member countries will consider options for future work in order to design a framework for international co-operation in the field of privacy protection in the global information society.

OPENING SESSION

Chair: Michelle d'Auray, Executive Director of the Electronic Commerce Task Force, Industry Canada

Keynote speakers

Lord Williams of Mostyn, Parliamentary Under-Secretary of State, Home Office, United Kingdom

Guy Braibant, Président de section honoraire au Conseil d'Etat, chargé par le Premier Ministre d'un rapport sur la transposition de la directive européenne de protection des données personnelles, France

Mozelle W. Thompson, Commissioner, Federal Trade Commission, United States

General legal context

Since 1980, considerable research and a range of initiatives, at both the national and international level, have been undertaken to explore and address issues related to the collection and use of personal data: in addition to the OECD Privacy Guidelines, two other international instruments -- prepared by the Council of Europe and the United Nations -- were adopted in 1981 and 1990, respectively.

Thirty-four countries world-wide have adopted legislation in this area, applicable, depending on the country, to the public and private sectors or to the public sector alone. Furthermore, in October 1998, a 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, is to be implemented in order to harmonise data protection laws within the European Union.

In countries that do not have special legislation intended to protect privacy and personal data, regulations which apply to specific industry sectors are nevertheless applicable as well as a number of industry-driven provisions. General principles or standards have also been established to serve as a reference in both the public and private sectors; and codes of good conduct have been adopted in many business communities.

Stefano Rodotà, President of the Data Protection Commission (Garante per la protezione dei dati personali), Italy will give an overview of the existing instruments in the field of privacy protection and highlight the consensus on the main privacy principles expressed in the OECD Privacy Guidelines.

General technological context

Advances in information and communication technologies have fostered the proliferation of private, industrial and commercial transborder electronic exchanges on a global scale which are bound to intensify among businesses and between businesses and consumers as electronic commerce develops. The volume and nature of personal data disclosed on networks during electronic transactions have increased and the temptation to capture this data to produce value-added information on customer and prospect profiles has increased as a result. New methods for processing the vast accumulation of data -- such as data mining techniques -- make it possible, on the basis of demographic data, credit information, details of on-line transactions, to identify new kinds of purchasing patterns or unusual relationships.

Johan Helsingius, Director of Product Development and Marketing, EUnet Intl. B. V. will describe network technologies and will highlight the fact that the international nature of networks offers numerous benefits but also requires new mechanisms to protect privacy.

SESSION 1: THE NEEDS OF THE PRIVATE SECTOR AND THOSE OF USERS AND CONSUMERS IN RELATION TO EDUCATION FOR PRIVACY IN A GLOBAL INFORMATION SOCIETY

Chair: Mads Bryde Andersen, Professor, Dr. Jur., Copenhagen University, Denmark

This session aims to highlight the premise that an active education strategy is one of the surest ways to help achieve online privacy protection and to give all actors the opportunity to understand their common interests.

The term "education" goes beyond mere information on the rights, responsibilities, institutions, technologies, and protection mechanisms with respect to privacy protection on line. It is a process of communication, the success of which strictly depends on taking into account the cultural diversity of the various actors on the networks. These cultural differences have a bearing on the concepts of risk, rights, obligations, and the role and use of technologies. Consequently, it is vital to know the needs and expectations of the principal actors present on the networks to help elaborate the framework of an efficient strategy for developing awareness of and education for privacy.

Indeed, the capabilities of network technologies provide an effective means of education for users, notably because of its interactive characteristics, by facilitating access to information and developing skills thus improving the practical ability to protect oneself.

Private sector needs

Jean-Marc Mosconi, délégué-général de l'association Mercatel, France will articulate the needs of the private sector in the context of electronic commerce and highlight the necessity of creating a trustworthy environment not only between companies and individuals but also between companies. He will describe under which circumstances and for what purposes businesses need to collect and process personal data. He will also give a private sector perspective in terms of the implementation of the OECD Privacy Guidelines, highlighting business issues related to particular principles of the Guidelines.

Peter Swire, Associate Professor, College of Law, Ohio State University, United States will identify specific examples of the kinds of transborder data flows which exist now and are likely to develop, especially in the area of electronic commerce, on the basis of evidence collected during extensive interviews, including many from the business community. He will describe electronic commerce as a "Market of one", the complex contractual relationships that it enables and will demonstrate the interest of market-driven experimentation. Finally, he will show how information about sales, perhaps including personally identifiable information, may be crucial ingredients in making the relationship mutually beneficial to customers and sellers.

User and consumer needs

Jim Murray, Director, Bureau Européen des Unions de Consommateurs (BEUC) will stress that electronic commerce has many potential benefits for consumers, but will concentrate on the potential privacy problems which can occur when a consumer browses commercial Internet sites. He will propose specific solutions and outline why agreement on common rules between countries will be helpful in resolving problems of jurisdiction. He will recommend that governments take into consideration the needs of consumers in other countries, as well as domestic consumers, and will call for practical steps to promote co-operation, enforcement and compliance in cross-border consumption and commerce.

Marc Rotenberg, Director, Electronic Privacy Information Center (EPIC), United States will describe the attitudes of on-line users in privacy matters, based on the findings of a Poll. He will demonstrate that privacy is the number one concern of Internet users and that users want control over their personal information online. He will then describe the implications for technology development, the implications for industry and for policy makers.

Communicating with and educating business and consumers for understanding about privacy risks, rights, obligations and technologies

Perri 6, Research Director, Demos, United Kingdom will argue that "Privacy education" should be understood, not only as a process of providing information or giving instruction, but as a process of influencing how information is understood. He will explain why risk education should encourage individuals to take responsibility for protecting their personal data, either by taking *ex ante* measures for self-protection, filing complaints to other bodies for *ex post* compensation, or at least by assessing the risks to their privacy. He will also explain why this type of privacy risk education is neither politically neutral nor the simple and value-free presentation of "facts" on which people may form any opinion they wish.

Reactions of the panel and general discussion

- **Anne Line Grsstad, Special adviser, Ministry of Justice, Norway**
- **Hubert Bouchet, member of the CNIL (Commission nationale de l'informatique et des libertés), France**
- **Tetsuya Nishida, Director, Center for Financial Industry Information Systems (FISC), Japan**
- **Deirdre Mulligan, Staff Counsel, Center for Democracy and Technology (CDT), United States**

- What benefits can be obtained through transparency for all actors? (businesses and consumers)

- How important is the ability to exchange personal data for commercial purposes?

- What are the main points to focus upon in a dialogue between businesses and users or consumers?

- Who should be responsible for educating users? (businesses, NGOs, governments ...)

SESSION 2: TECHNOLOGICAL SOLUTIONS TO PROTECT PRIVACY ONLINE

Chair: Roger M. Needham, Pro-Vice-Chancellor & Professor of Computer Systems, University of Cambridge, United Kingdom

This session aims to point out that technological solutions can assist in implementing the OECD Privacy guidelines on global information networks. By empowering individuals to choose for themselves and to control their own personal data, technological solutions can help to establish a balance between the free flow of information and the right to privacy. Various privacy enhancing technologies able to meet these objectives will be presented during this session.

Privacy Enhancing Technologies (PETs) commonly refer to technological tools which aim to protect privacy. The various technologies put forward for protecting privacy range from tools that provide anonymity through those that offer a clear choice between anonymity and identification to those, more complex, that seek to provide openness about data practices and foster informed decisions by individuals. They therefore vary in their ability to respond to the different privacy concerns.

Any discussion on the effects of the use of PETs for the protection of individual privacy should take into account that these technologies reflect trade-offs to the extent that they are built on commercial choices or policies, as organisations seek to balance their other interests with their desire to protect privacy.

The 1995 Ontario/Dutch Report "Privacy Enhancing Technology (PET)" and an application in the health care environment

John Joseph Borking, Vice President, Data Protection Commission, Netherlands will present PETs as a system of technological measures that minimise or eliminate the collection of personal or identifiable data and therefore can safeguard the privacy of the user of any information system without damaging the system itself. He will present a recent PET-enriched hospital information system for preventing privacy intrusion which has been developed and successfully marketed in the Netherlands. He will suggest that PETs are vital for obtaining consumers trust and confidence, in particular in a global networked society.

5th Framework Programme on Research and technological development and privacy enhancing technology

Anne Troye-Walker, Lawyer, DG III - Industry, European Commission will present the Fifth Framework Programme on Technological Research & Development, which is currently being prepared and addresses requirements to enhance confidence and trust of consumers and businesses for electronic commerce and multi-media content and tools. Amongst these requirements the protection of information integrity and of privacy, notably through privacy enhancing technologies, will be considered. She will outline some of the key actions which are being prepared.

United States Council for International Business (USCIB) overview on privacy enhancing technology

Charles Prescott, Chairman of the USCIB Working Group on Privacy and Data Protection, United States will briefly introduce a number of privacy-enhancing technologies which are now being developed. He will point out that if business has a very active role in the development of these technologies, there is a need for interplay among the world of technology, the Internet, consumers, government and business in resolving the privacy issues in electronic commerce.

Technological aspects as preconditions for an effective protection of personal data

Stefan Engel-Flechsig, Senior Principal, Federal Ministry of Research and Technology, Germany will point out that new technologies contribute to broad acceptance of new services and at the same time set the stage for the development of guiding principles for international standards. He will explain how new technologies allow the user more freedom in protecting personal data and describe some of them at work in global information and communications networks today. He will recommend that modern data protection regulations take new technologies into account to safeguard the existing standards of privacy protection and to support their effectiveness.

Platform for Privacy Preferences (P3P)

Josef Dietl, Electronic Commerce Specialist, World Wide Web Consortium will describe the P3P project which results in the specification and demonstration of an interoperable way of expressing privacy practices and preferences by Web sites and users respectively. He will highlight the advantages of P3P for users and Web operators, including flexibility in making statements about privacy and preferences, ease of use and assurance of security. He will point out that a privacy policy statement can require a digital signature and will stress that the P3P project is closely linked to the W3C Digital Signature project.

Open Profiling Standard (OPS)

Sean Gaddis, Manager, Marketing Technology, Netscape Communication Corporation will present OPS, which is an Internet open standards solution designed to provide a structured technology to consumers, business, and developers. He will show that OPS offers the Internet user the ability to personalise applications and can provide a record of profile transactions. He will describe the benefits of OPS to Internet service providers and Internet developers. He will recall that OPS has been submitted to the P3P Working Group of the World Wide Web Consortium and that there has been an agreement to co-operate to build upon the previously proposed OPS standard within the P3P working group.

Anonymity and "electronic cash" applications

Jean-Pierre Camelot, Groupement des Cartes Bancaires, France will describe the concept of an electronic purse which provides anonymity while organising the tracability of the transactions. He will highlight the main characteristics of this concept which does not allow a "purse to purse" scheme, limits the tracability to the observation of global flows in order to detect fraud and makes it possible to know which bank account must be debited due to the use of electronic money.

Anonymous services

Lance Cottrell, Director, Infonex Internet Inc. will expose the general structure of anonymous services and deal with anonymity in high threat environments. He will give real examples of anonymous services such as anonymous accounts; anonymizers (anonymous Web surfing) and mixmaster anonymous remailers.

Reactions of the panel and general discussion

- **David Medine, Head, Credit Practices Division, Federal Trade Commission, United States**
- **Herbert Burkert, Institute for Media Communication, German National Research Center for Information Technology**
- **Yves Le Roux, Corporate Security Programme Office, Digital Equipment France**
- **Reid Watts, Vice President, Research and Advanced Technologies, NCR**

- How effectively do technological solutions allow the privacy protection principles to be implemented?

- Can users remain anonymous?

- Should a conflict between the privacy preferences of the user and those of the site be solved automatically or by the user action?

- To what extent can a dialogue between a Web site and a user concerning the privacy practices of the site and the privacy preferences of the user result in a refusal of access by the site? In such a case can refusal of access be construed as refusal of sale?

SESSION 3: PRIVATE SECTOR-DEVELOPED MECHANISMS, TO ENSURE EFFECTIVE IMPLEMENTATION OF CODES OF CONDUCT AND STANDARDS IN A GLOBAL ONLINE ENVIRONMENT

Chair: Barbara Wellbery, Special Counsel for Electronic Commerce, Department of Commerce, United States

There are primarily two approaches to address the issue of privacy protection -- government regulatory and legislative actions and market-based self-regulatory efforts. Government efforts offer predictable, enforceable legal protections and redress mechanisms yet they may lack the predictive skills and flexibility to adequately regulate at this early stage in the development of the online environment. Self-regulatory efforts enable organisations in different sectors to tailor detailed guidelines to work within specific circumstances. However, the resulting policy patchwork and divergent approaches may not provide the necessary transparency nor answer the often-heard question of enforceability. The harmonisation of effective self-regulatory efforts aimed at online privacy protection within a predictable global framework could both benefit business and increase consumer confidence in the online environment.

Keeping in mind the underlying principles for online privacy protection that will form part of this framework, this session is intended to examine and discuss a number of self-regulatory efforts to provide individual privacy protection in the global electronic environment. Indeed, it is important to consider the need to pursue a secure environment online that assures "adequate" protection for privacy.

This session is intended to look at recent practical implementation of codes of conduct and industry standards using enforceable mechanisms to ensure effective protection of personal information. A number of these may include the use of adequate and reputable labelling systems; privacy icons or symbols, trustmarks and authentication; trusted third-party auditing; effective redress mechanisms; digital certificates and proactive privacy commitments backed by government enforcement.

Government has a critical role in determining the policy framework that will encourage and promote private sector efforts in the implementation of privacy protection.

Mechanisms to ensure effective implementation of the Canadian privacy standard

Mona Goldstein, President, Wunderman Cato Johnson

Label and certification to implement the Japanese Privacy Guidelines

Yuji Yamadori, Director, Information Security Office, Japan Information Processing Development Center (JIPDEC) will explain that JIPDEC is planning to implement certification for protection of privacy in the private sector on April 1, 1998, based on the Ministry of International Trade and Industry (MITI) guidelines. The main objective is that any private organisation could be certified by labelling with a special mark noting protection of privacy whenever they handle personal data in an appropriate manner.

Yasuo Hasebe, Professor of Law, University of Tokyo, Japan will present various measures for the protection of privacy in the electronic environment, such as self-regulated guidelines of telecommunications industry and cyber business industry. He will also present possible governmental

measures now under discussion in a study group on Developing the Legal Environment for Advanced Information Communications Society.

Mechanisms to enforce US private sector codes of conduct

Ronald L. Plesser, Partner at Piper & Marbury LLP will present two models of industry self-regulation in the United States: the Individual Reference Services Group (IRS) and the Online Privacy Principles of the Direct Marketing Association. He will explain that the IRS Group, which is composed of leading companies in the business of providing information that assists users in identifying and locating individuals, has developed, in close consultation with the Federal Trade Commission (FTC), a comprehensive set of self-regulatory principles backed by audits and government enforcement. He will describe the Online Privacy Principles and the consequences of non-compliance.

William W. Burrington, Director, Law and Global Public Policy, Associate General Counsel, America Online Incorporated

Privacy Audits in the Private Sector - an Australian perspective

Steve Wolley, Partner, Price Waterhouse, will give the background to the developments of Privacy Codes in Australia and will consider a few of the interesting issues facing private sector organisations. He will examine the effectiveness, in terms of public confidence and value to the organisation, of the fact that some organisations have pre-empted the development of a national privacy code and have already established their own codes of practice supported by voluntary independent audits and public reporting. He will discuss how the lack of consumer redress mechanisms --which has long been the sticking point with the introduction of voluntary privacy codes -- is having an impact on those organisations already adhering to voluntary codes and will suggest the way forward.

TRUSTe: A global solution to privacy on the Internet

Susan Scott, Executive Director, TRUSTe, United States, will describe TRUSTe and TRUSTe's Principles. She will describe how TRUSTe performs audits and off-site reviews of privacy statements to ensure consistency and accuracy. She will also explain that TRUSTe gives expertise on how privacy statements can be strengthened and is able to ensure when a site has decided to adhere to the OECD Guidelines or to the European Union Directive, that they meet the terms of these instruments. She will also deal with prosecution, fraud and deceptive practices, trademark infringement and breach of contract. Finally, she will present TRUSTe branding campaigns which focus on education.

Privacy Icon

Alastair Tempest, **Director General, Public Affairs & Self-Regulation, Federation of European Direct Marketing Associations, International Federation of Direct Marketing Associations**, will describe the results of FEDMA research on codes of conduct and individual company privacy policy statements and describe the FEDMA proposal of an icon symbol for its members, which would help users identify whether a privacy policy exists and would provide ease of access. He will present the FEDMA guidelines on where to place this privacy icon and on what to include in a privacy policy notice. These

proposals, intended to encourage greater trust and confidence in Internet Marketing practices, should be agreed in 1998 at both the European and international levels by the Direct Marketing Associations.

Reactions of the panel and general discussion

- **Stephanie Perrin, Special Policy Advisor, Information Policy, Industry Canada**
- **Peter Ford, First Assistant Secretary, Information and Security Law Division, Attorney-General's Department, Australia**
- **Bart de Schutter, member of the Commission pour la protection de la vie privée, Belgium**
- **William R. Whitehurst, Director of Data Security Programs, IBM Corporation, United States**
- **Masao Horibe, Professor of Law, Faculty of Law, Chuo University, Japan**

- *What auditing mechanisms are possible (internal corporate certificate/ external independent)?*
- *Who can supply labels (different solutions according to different countries)?*
- *In terms of effectiveness and "enforcement" what are the consequences of failing to respect the codes of conduct or standards (with regard to individuals and with regard to businesses)?*
- *Does it matter if all organisations within a sector do not sign up to codes of conduct?*
- *What are effective dispute resolution and redress mechanisms?*
- *Who is ultimately accountable? Where does an aggrieved consumer go for redress?*

SESSION 4: TRANSBORDER DATA FLOWS AND THE COEXISTENCE OF DIFFERENT SYSTEMS FOUNDED ON LAW AND/OR SELF-REGULATION: EXAMINATION OF CONTRACTUAL SOLUTIONS

Chair: Philippe Lemoine, Vice Président Directeur Général du Groupe Galeries Lafayette, France

Among other legal techniques for assuring privacy of data in transborder data flows, contracts have their place in the context of international networks. In the absence of a statutory framework or effective self-regulation, contractual arrangements can, in some cases, provide a practical substitute. Contracts can also support compliance with a statutory regime.

This session aims at discussing the advantages and disadvantages of such contractual agreements in an online environment. For that purpose, it is intended to examine the nature of these contracts and their effects particularly for individuals. Contracts can be signed between two companies or between a company and an individual and in both cases, their conclusion raises important issues among which are the validity of consent being given online and the consequences of non-compliance (applicable law, sanctions and recourses available to data subjects).

This session will also examine the various measures which could foster the use of contractual solutions for transborder data flows such as adoption of model clauses or certification by independent trusted third parties.

The application of the European Data Protection Directive to international networks and the role of contracts

Susan M Binns, Director, DG XV (Internal Market), European Commission, will explain that co-existence of law-based and self-regulatory systems is manageable and stress that difficulties for transborder data flows only arise if the levels of protection delivered by different systems, regardless of whether they are law based or largely self-regulatory, differ too much. Contractual provisions can provide an *ad hoc* solution where general conditions to meet the requirement for "adequate protection" for data transferred to third countries do not exist. She will evoke the difficulties of the "data subject" to exercise his rights under a contract to which he is not a party and of performing effective independent control. She will also mention the difficulties that can arise even when personal data collected directly from the data subject are to some extent covered by "consent" exemption. More generally, she will underline the desirability of international data protection rules with global scope and will recall that the European Union would like to see legally binding rules. She will mention the World Trade Organisation as an obvious forum to deal with these issues.

The issue of contractual solutions for transborder data flows

Christopher J. Millard, Clifford Chance, United Kingdom will consider, in the context of transborder data flows, the legal, procedural and practical considerations which must be addressed for contractual solutions to be effective in terms of both a contract between two or more controllers and a contract between a controller and a data subject. In particular, he will address practical issues which are likely to arise in the context of online communications and transactions.

The Model Contract of the Council of Europe

Mr. Alexey Kozhemyakov, Deputy Director, Directorate for Legal Affairs, Council of Europe (invited) will present the "Model contract to ensure equivalent data protection in the context of data flows" which has been developed by the Council of Europe.

International Chamber of Commerce (ICC) model clauses for use in contracts involving transborder data flows

Heather Rowe, Chair of the ICC Working Party on Privacy and Data Protection will give an introduction to the draft model clauses being prepared by the ICC in the light of the provisions of article 26 of the European Union data protection directive.

A transborder data flow contract in Germany

H-J Garstka, Data Protection Commissioner of Berlin, Germany will present a practical answer to the question of whether, in the case of transborder data flows, data protection can adequately be guaranteed by contracts between the parties who exchange the data. He will describe the main features of a contract which has been concluded between the German Railway Company (Deutsche Bahn AG) and the German and American branches of the Citibank Corporation. He will show that such contractual solutions could

apply to data transmitted by the Internet or other networks in a way which could fulfil the requirements of an adequate data protection standard.

Microsoft's privacy compliance programme in Europe

Peter Fleischer, Corporate Attorney, Microsoft Europe

Challenge in the Private Sector: ECOM Guidelines and Model Homepage

Kouichi Sakusa, Electronic Commerce Promotion Council of Japan (ECOM) will give an overview of the ECOM Guidelines which comply with the eight principles of the OECD Privacy Guidelines and address characteristics of electronic commerce. He will present the ECOM model homepage developed with electronic commerce businesses in mind and will describe ECOM current activities.

Reactions of the Panel and general discussion

- **Charlotte-Marie Pitrat, Government representative, CNIL (Commission nationale de l'informatique et des libertés), France**
- **Beckwith Burr, Acting Associate Administrator, Office of International Affairs, NTIA, Department of Commerce, United States**
- **Francis Aldhouse, Deputy Data Protection Registrar, UK**
- **Christian Duvernoy, Attorney, Wilmer, Cutler and Pickering, Belgium**

- *What are some advantages and disadvantages of various contractual solutions to data transborder flows?*
- *Why use contracts?*
- *Should contracts be standardised?*
- *Can contracts be labelled or certified? By whom?*
- *If a contract is broken, what mechanisms are available to protect the contracting parties, particularly individuals?*

SESSION 5: MAIN CONCLUSIONS OF EACH SESSION AND OF THE WORKSHOP

Chair: Michelle d'Auray, Executive Director of the "Electronic Commerce Task Force", Industry Canada

Based on the various presentations and on the discussion among the panel and the participants, each session chair will draw the conclusions of his/her session. Each session chair may propose eventual future work related to the main issues which were discussed.

The Workshop chair will respond to these conclusions and propose the main conclusions of the Workshop to be presented to the Group of Experts on Information Security and Privacy and to the ICCP Committee.

EXECUTIVE SUMMARY OF THE WORKSHOP

by Francis Aldhouse, UK Deputy Data Protection Registrar

Introduction

OECD organised this workshop on privacy protection in a global networked society to focus on the implementation of its 1980 Privacy Guidelines and to look at practical measures to reconcile the different approaches of Member countries. A few main themes emerged. The 1980 Guidelines still provided the basis for legislative and self-regulatory privacy regulation even in global networks. It was important to promote the GIS and for that purpose privacy protection was needed which could be achieved by varied means, technological, legislative or self-regulatory. Bridges had to be built between countries relying on those different methods.

Opening Session

After the welcome to participants, the urgency of the work was emphasised. Privacy was critical for the success of global electronic commerce. Balances had to be struck between the privacy of individuals and the need for information flows. Those issues would be debated at the ministerial conference to be held in Ottawa in October 1998. The keynote speakers explained how data protection and e-commerce were seen in the United Kingdom, France and the United States. Data Protection was seen by the United Kingdom government as part of a package of human rights legislation. Personal privacy should be respected so that one could venture safely into cyberspace and balanced controls could be found to reconcile privacy with Internet use. The French viewpoint emphasised three main points: a trend towards privacy legislation; a technical trend to the dispersion of computing power; and the growth of data flows in global networks. Rights to privacy and to information and a free market had to be reconciled. Countries had to co-operate and OECD's work could develop the rules of the road for the information super-highway. The United States saw the need for global protection created by the expansion of the Internet. There were regulatory powers to protect personal data in some sectors, particularly credit reporting. Consumers were concerned about their privacy. Self-regulatory initiatives were being undertaken, but if they failed, then in some cases legal regulation might be needed. The legal and technical background to the Workshop was introduced. That background included the content of the 1980 Guidelines and the tensions between general principles of fundamental rights, detailed legislation, the self-regulatory approach, and the pressures to encourage data flows in the GIS. Technical solutions, often called privacy enhancing technologies, could be found to such legal problems as concerns about the ways in which individuals could be identified and profiled.

Session 1: The needs of the private sector and those of users and consumers in relation to education for privacy in a global information society

This session looked at the need for education. Even though education could not be a substitute for proper standards and might be an excuse for avoiding regulation, it could enable individuals to understand the capabilities of the technology and assert their rights. Surveys showed that customers were very concerned about their privacy on the Internet. Good privacy policies on Websites would set out an

individual's rights and the organisation's responsibilities. There were businesses who understood that consumer confidence was important and they should be encouraged to provide privacy protection. Formal education had a role, but it was important that consumers should be given greater transparency so that they understood what was happening to their personal data when engaged in e-commerce.

Session 2: Technological solutions to protect privacy online

This session made clear that technological solutions were available for privacy problems. Doubt was cast in some cases upon the appropriateness of anonymity, if consumers were to be properly protected. But anonymity, which individuals had increasingly been losing with the global increase in the collection of personal data, could, without loss of functionality in information systems, be restored to individuals by excluding or restricting the use of personal data. The session was told of a live example of a hospital system based on the principle of whether or not it was necessary to process personal data. Research was being encouraged in Europe to develop privacy enhancing technologies and speakers were confident that technological methods should and would be found to protect personal privacy in electronic commerce. Two further examples explained to the session were the Platform for Privacy Preferences Project (P3P) which would allow individuals to negotiate privacy agreements with Web sites, and the Anonymiser which acted as a trusted third party allowing users to browse Web sites anonymously. Notwithstanding the general optimism about technological solutions, the economic pressures to collect personal data and the need for political and social policy decisions to ensure privacy were both emphasised.

Session 3: Private sector-developed mechanisms to ensure effective implementation of codes of conduct and standards in a global environment

This session looked at the wide range of private and self-regulatory measures to deliver privacy protection. The debate started from the position that self-regulation could be just as effective as legislation, and it should not be assumed that compliance either with statutory or self regulation would be automatic, nor that one system would be more effective than another. The Canadian Direct Marketing Association had developed a compulsory code based on the OECD Guidelines and modified it for the Internet. The CDMA had moved from ignorance of privacy protection through self-regulation to calling for legislation. There were similar initiatives in Japan, both generally and for electronic commerce; guidelines had been published and systems of certification and awarding privacy marks were being developed. Icons could be used to indicate Web site privacy policies, and the enhanced TRUSTe system was explained in which the privacy policies of sites were independently audited. Presentations were given from Australia and the United States of other self-regulatory schemes which were also supported by independent audit. In those systems, compliance and consumer redress was assured by a public official or regulatory authority. If self-regulation were to succeed, then economic market pressure would be required to encourage good practice and discourage bad actors, but great concern was expressed about how consumers could secure redress in foreign jurisdictions, a problem heightened by global e-commerce.

Session 4: Transborder data flows and the coexistence of different systems founded on law and/or self-regulation: examination of contractual solutions

The last topic session looked especially at securing privacy protection in transborder data flows and especially the use of contractual solutions. The growth in international networks and the increase in personal data processing were noted by both the chair and the speakers. Similarly, they also pointed out

the importance of privacy as a fundamental right, its protection by legislation in Europe, and the possibility of permitting data flows to those countries which relied on self-regulation, if contractual or other guarantees of privacy were provided. Global e-commerce was changing the nature of retailing; there were great cultural and legal differences between countries affecting attitudes to the use of sensitive personal data; and the issue of applicable law in global transactions had to be resolved. OECD Member countries should require of each other compliance with the 1980 Guidelines; it would then not matter so much whether that standard was delivered by legislation or self-regulation. Contracts might bridge the gap between those with legislation and others, but the European Commission would prefer to negotiate a multilateral agreement with its international partners. Some doubt was cast upon the effectiveness of the contractual solution and particularly whether the well-known German Railways/Citicorp contract was applicable to cases affecting smaller numbers of customers. Contributors spoke warmly, however, of the previous work of the Council of Europe in developing a model contract together with the International Chamber of Commerce, which was already working on a revised model to satisfy the requirements of the EU Data Protection Directive. Although there was some discussion of alternative methods of privacy protection in transborder e-commerce, such as the Japanese ECOM model home page, the debate concentrated on contractual solutions. It was suggested that such contracts needed a legislative basis or at least a set of agreed principles; they were praised for being flexible, familiar to business and imposing no cost on the public purse.

Session 5: Main conclusions of each session and of the Workshop

In this final session the chairs of the four previous sessions presented their conclusions. The OECD Guidelines were acknowledged as an internationally accepted set of privacy principles. A role for education was seen in increasing the awareness of individuals of their rights and of the capabilities of the technology; and transparency was needed so that consumers could be aware of the privacy practices of e-commerce traders. Anonymity for users could be achieved by technological means, or if something less was thought appropriate, systems such as P3P would allow users and businesses to reach agreement on privacy practices. A variety of effective forms of self-regulation existed, commonly enforced by independent audit. Means of redress for individuals required examination, especially in regard to e-commerce transactions in foreign jurisdictions. Global e-commerce had to be reconciled with different legal and cultural traditions and a number of matters needed study, including the bases for contractual privacy protection and individual consent, and the problem of applicable law. At the end of the two-day session, the Chair of the Workshop reminded participants of the Ottawa Conference on electronic commerce in October 1998. Consumer confidence in privacy protection was a key issue for fostering the growth of global electronic commerce. A range of instruments had been created to implement the 1980 Guidelines which had stood the test of time. The Workshop had agreed on the need to give individuals control over personal data and on the key issues: on allowing free flow of data; on the flexibility of instruments; on the need for effectiveness; on the potential of technology; on the requirement for enforcement and redress; and on the need for better education. Ways had to be found to accommodate differences of approach in order to provide seamless protection for individuals, and the roles of all those providing education needed clarification. OECD should assess the variety of privacy instruments and their application in a networked environment against the 1980 Guidelines. The study should identify comparability, but also gaps in coverage and barriers to interoperability; it might also suggest standards for privacy instruments in a networked environment.

RAPPORTEUR'S REPORT

Objective

In October 1997, the Group of Experts on Information Security and Privacy, which works under the auspices of the Information, Computer and Communications Policy (ICCP) Committee, decided to organise a workshop on privacy protection in a global networked society. The convergence of technologies in global networks offers enormous social and economic benefits, but also presents a number of challenges. The global information society (GIS) requires the convergence of government policies, the transparency of regulation and effective implementation on global networks. An important aspect of these requirements is the need to establish the protection of privacy and personal data in order to ensure trust in global networks and prevent obstacles to transborder data flows.

In 1980, OECD published its Privacy Guidelines. It has taken a continuing interest in privacy protection since then, and has for some time been working in the area of the GIS. Consequently, it arranged the workshop to bring together representatives of its 29 Member countries to create a dialogue between governments, private business, privacy authorities and consumer bodies to focus on how the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data could be implemented in global networks.

The Workshop would seek to identify mechanisms and tools to build bridges between the approaches of those countries who relied primarily on legislation for privacy protection, and those who looked to self-regulation and other systems. The emphasis was to be on practical solutions for the protection of privacy capable of implementation irrespective of cultural differences.

Workshop Structure

The Workshop was organised in six Sessions as follows:

Opening Session - to introduce the Workshop, have the important themes set out by keynote speakers, and the general legal and technological context introduced;

Session 1 - to examine the needs of the private sector, consumers and users in relation to education for privacy in the GIS.

Session 2 - to examine technological solutions to protect privacy on-line.

Session 3 - to consider private sector mechanisms to ensure effective implementation of codes of conduct and standards in a global environment.

Session 4 - to consider the regulation of transborder data flows, law and self-regulatory approaches and particularly contractual solutions.

Session 5 - to consider the reports of Sessions 1 to 4 and reach conclusions for the consideration of the Group of experts and the ICCP Committee.

Main Themes

Although the sessions would seem to be quite distinct some themes re-emerged in each session. There was a general acceptance of the need to promote the GIS and the importance of protecting the privacy of individuals. The 1980 OECD Guidelines were acknowledged as the shared basis for many initiatives both legislative and self-regulatory. The Guidelines had stood the test of time and were accepted as still having value in the changed technological environment from that in which they were developed. The need to reconcile and balance the legitimate rights both of individuals to privacy and of businesses to use information was a recurrent topic. The differences between countries in their approaches to implementing the Guidelines became clear and speakers emphasised the importance of building bridges between countries with different approaches.

Other important themes arose out of the sessions. The need for an educated public and transparent systems emerged. There was particular optimism over the private sector technological initiatives to secure privacy protection. Self-regulatory initiatives could be effective and properly enforced and were therefore seen as legitimate and valuable. Contractual agreements were seen as one of the ways to bridge the different approaches in Member countries.

Opening Session

This session was an opportunity to welcome participants to the workshop, explain its background and objective and set the tone with leading keynote speakers. In opening the workshop, **Risaburo Nezu** explained the background of OECD involvement in the GIS and privacy issues. He emphasised the work of the Organisation and particularly the ICCP Committee in striving to ensure that electronic commerce was not hampered by technical, legal or institutional barriers. He recalled that in the previous November, the OECD had hosted jointly with the government of Finland a conference (the Turku Conference) to discuss a variety of specific barriers to the development of GII-GIS and that it had concluded that adequate protection of privacy was one of the prerequisites for the full exploitation of the potential of electronic commerce (e-commerce). He said that the OECD was fully aware of the different approaches in the field of privacy but that the level of maturity of discussion and readiness to take decisions was not uniform, making international agreement difficult in the near future. However, highlighting the fact that the policy of one country would have immediate impact on the whole global community, he stressed the necessity to look at privacy from a global perspective and the urgent need to make progress. The best use should be made of the forthcoming ministerial conference in Ottawa in the autumn of 1998 organised jointly by OECD and the Government of Canada to lay down key principles for establishing a coherent global system of e-commerce.

Michelle d'Auray, the overall chair of the Workshop, emphasised its timeliness, the preparatory role for the Ottawa conference and the value of OECD as an appropriate forum. She mentioned several of the difficult aspects of global electronic commerce: digital signatures, certification, authentication, taxation and consumer protection. Also among these -- and most critical -- was privacy. The 1980 Guidelines had stood the test of time, but one had to look at how to implement them in the GIS by a variety of technical, legal and self-regulatory means. She explained the structure of the workshop sessions, emphasised that consumers would not use global commerce unless satisfied of privacy protection, and re-affirmed the common ground and objective of the need to build bridges and find

compatibilities between self-regulation and legislation. She concluded, before introducing the keynote speakers, by noting, on the one hand, that data protection was a fundamental right, but that on the other hand, consumers and businesses also had a right to information flows. A balance had to be struck, and OECD had met the challenge previously.

The first keynote speaker, **Lord Williams of Mostyn**, started by explaining how data protection fitted into a package of rights legislation in the United Kingdom, including Freedom of Information and the incorporation of the European Convention on Human Rights. He was reassured to see OECD looking for practical measures in a world in which information about individuals was increasingly widely available. Individual privacy is important to all; there is no one about whom some organisation does not hold information. This often surprised individuals who fear technology. Education for ordinary people was required, as well as technical solutions, so that individuals understood what was being done with their information.

He went on to explain how a new Data Protection Bill had been introduced to implement the EU Directive 95/46/EC on data protection, and he gave details of the new legislation. It aimed to strengthen protection for individuals and strike a workable and fair balance between the rights of individuals to privacy and the need for data users, including business, government and voluntary bodies, to deliver services by handling personal data efficiently and effectively. There would be individual enforceable rights in the new law, because there could be no effective right without easy enforcement. He saw the right of subject access as important because personal data was the "property" of the individuals to whom it related. He referred to the requirement for adequate protection in countries outside the European Union, and the difficulties which would arise in cases of inadequacy. The European Commission had enormous powers which had to be handled sensitively. There was a good deal of concern outside Europe, but there was no sinister intention and one had to make sure that balanced, thoughtful controls were put in place and solutions produced to problems which were apparently intractable, but which could not be allowed to remain so.

Lord Williams commented that although national laws applied to the Internet and other technologies, it was very difficult to police the Internet, and not only in the context of data protection. It should be possible to access the Internet as anonymously as one could go shopping. Personal information -- the property of individuals -- should be respected so that one could venture safely into cyberspace. Consumer education could ensure that individuals could give properly informed consent. Technological means -- such as the applications of cryptography -- could help to maintain privacy. There might be a need to rethink the relationship between what was properly private and what could properly be used by government and business. Countries had different legal and cultural backgrounds, but it should be possible to strike the right balances.

The second keynote speech was given by **Guy Braibant** who explained that he was chairman of the commission studying how to transpose the EU Data Protection Directive into French law on which matter he was due to report in early March 1998. He welcomed the timely decision of OECD to organise the Workshop. In the 20 years since the passing of the existing French data protection law there had been important developments and new challenges. There might need to be changes or adaptations to the OECD Guidelines, but in the last 20 years more than 30 countries within and outside Europe had taken those Guidelines into account in the course of their legislation.

He stressed three main points. First, there was a legal and political trend in the direction of protective legislation exemplified by the EU harmonising Directive. Secondly, he pointed out that there had been a significant technical trend in the same period: a move from macro-computing concentrated in the hands of governments and large corporations to micro-computing with a great dispersion of computing

power and consequent impact on individuals. A third trend was the growth of global networks such as the Internet which had led to a great growth in transborder flows of data.

One had to reconcile different fundamental rights -- rights to information and a free market with rights to privacy. There was also the general public interest of states to be taken into account, such as the need for information for fighting crime.

There were generally accepted international principles such as the fairness of data processing, the right of individuals to oppose processing and the need for individual consent to the use of sensitive data. Those who had the need to process data also had the means and skills to protect that data. Two ways of implementing those principles existed: legislation supported by a data protection authority, and self-regulation in which trade organisations applied rules to their own members. Those methods corresponded to different legal traditions which had to be accepted, and ways should be found to co-operate. Perhaps negotiation might establish the equivalence of different systems, or one could consider an international convention.

The Internet ought to be trustworthy in its use of personal data. The protection of personal data should keep pace with technical developments, in order to give individuals the assurance of privacy. The objective of privacy protection was not to stop the processing of data but to signpost the correct route. Traffic regulation had to be developed for the information super-highway as it had been for the roads in order to prevent accidents, and OECD's work would help to develop the rules of the road for the super-highway.

Mozelle Thompson, a Federal Trade Commissioner, pointed out in the third keynote speech that Internet expansion had created the need for global protection and OECD provided a good forum to examine experience and explore ways to protect individuals. He explained that in the United States the Federal Trade Commission (FTC) had enforcement authority under a number of regulations including the Fair Credit Reporting Act. There were restrictions on the use of information for credit purposes which had led to an effective credit market. Generally, the United States had a sectoral approach to privacy protection issues.

Three years ago the FTC had started to focus on electronic commerce. The extra personal information arising in on-line transactions posed a threat to personal privacy and polls showed that this was of real concern to individuals. If that concern were addressed, electronic commerce could grow; thus all had an interest in solving the problems. The Consumer Privacy Initiative showed that industry understood the concerns. He preferred self-regulation: it was flexible, least disruptive to the technology and least burdensome on business. It must, however, be real and not cosmetic. He mentioned the Individual Reference Services self-regulatory code supported by independent audit. Such approaches should be given a chance to work before considering legislation.

In March 1998, the FTC would review the privacy policies of 12 000 Web sites to determine how easy they were to find and what they contained. Children's privacy on the Internet was a particular concern. There was strong parental opposition to the collection of information about children. The FTC hoped that self-regulation would succeed, but collection from children could in some cases violate the Federal Trade Act. Section 5 of that Act prohibited unfair or deceptive trade practices. The FTC expected to use its powers to protect the rights of children and adults in relation to the collection of information. The Internet should be market driven but the FTC was a law enforcement agency charged with enforcing the prohibition on unfair and deceptive practices.

After the three keynote speakers, Professor Rodota and Johan Helsingius respectively explained the general legal and technical context of the workshop.

Stefano Rodota pointed out the risk of conflict between states with legal regulation and those relying on self-regulation. The Guidelines could take us beyond that ideological conflict. It was still possible to find the necessary balance, even if it had become more difficult. He explained the content of the Principles in the OECD Guidelines. There was not a legal vacuum. Legislation was a realistic alternative to self-regulation and technical solutions. Privacy protection was essential to electronic citizenship.

There was a tendency for legislation to move from general principles to detailed provisions. Privacy, however, was seen as a fundamental right and general principles therefore still had an appropriate place. He referred particularly to the German notion of a right of informational self-determination, the development of European Union legislation and the Latin American Principles.

Personal data had become an essential good in the Information Society; there was a need for information to circulate. There were also the rights of human dignity, individual choice and to construct one's own private sphere. There should be rules to allow individuals to decide on their own level of protection. He mentioned the guidelines promulgated in Japan. Protection of private life also had a constitutional aspect as well as an interface with freedom of expression.

Privacy needed subordinate laws on access and control. Data varied from the publicly available to the highly sensitive. There was a need for adequate protection which could be provided by a move to "clean" technology. There were changes in the notion of privacy. Pluralistic structures integrating law and other techniques could provide individuals with the required autonomy. There could be a hierarchy of means: contractual rules, self-regulatory codes and formal law. The means could include privacy enhancing technologies, and the use of one method need not exclude the use of another.

Johan Helsingius explained that he was a technology-based businessman. He found it hard to separate business, legal and technical issues relating to privacy. Technical solutions could be found to what some saw as legal problems, and it was important to avoid premature regulation.

He raised the issue of identity, pointing out that a variety of different partial identifiers might exist and that data mining might put together extensive amounts of information. One could produce a profile of an individual, but still not know who he really was. Some have proposed the use of hard biometric identifiers, but he doubted the need. Profiling could be very precise and its development from the use of transaction logs was a worrying trend. If we only needed to be paid by a customer, we did not need the full background on that person.

Cryptographic means could give individuals protection, but their use required great know-how and sophistication. There were privacy invasive tools, but also privacy enhancing technologies. Policy decisions could not determine how technology would develop.

This opening session effectively raised all the main themes which were examined in the later sessions: the differences between those countries with formal law and others relying on various degrees of self-regulation; the risk of conflict and the need to build bridges; the importance of global electronic commerce; the concerns expressed by individuals and the importance of privacy protection; the dangers posed by technical developments and equally the protection which other developments could bring. All speakers were conscious of a degree of urgency in the work, the value of the existing 1980 Guidelines, the

problem of applying those Guidelines in global networks, and the appropriateness of OECD as a forum for seeking to identify solutions.

Session 1: The needs of the private sector and those of users and consumers in relation to education for privacy in a global information society

Mads Bryde Andersen introduced this session which, as the Orientation Paper put it, aimed "to highlight the premise that an active education strategy is one of the surest ways to achieve on-line privacy protection and to give all actors the opportunity to understand their common interests." He pointed out that the 1980 Guidelines set out principles. They were not legally binding, but a number of jurisdictions had adopted them or used them as a guide to legislation. They were technically neutral, but it was not clear how they would work in global networks. He used the analogy of pharmaceutical drugs to explain why education was required: it was important to know both how drugs worked and how to lead a healthy life and do without them. There were also different cultural attitudes to drug use which needed to be understood.

Before introducing the session contributors, he explained that Perri 6 could not be present. He would have spoken of privacy in the context of risk and the cultural differences that dictated how people perceived risks differently. Risk education should encourage the taking of individual responsibility. Risk literacy was usually acquired as a side-effect of other activities and learning. Privacy risk communication to children should be part of a widespread preparation for adult life. It was not politically neutral, but a deliberate cultural strategy to enable dialogue with other privacy risk cultures.

Peter Swire suggested that if the Principles had a narrower focus, they would have a more binding effect and receive greater enforcement by private sector self-regulation. He suggested that we expected to have access to some name-linked information -- such as that about an employee, a borrower or a consumer -- and that information should be within the scope of the Principles. Other information we did not expect to be given access to -- even if name-linked -- and it should really be seen as information about a business rather than an individual. There had not been general recognition of the private sector need to exclude from data protection passing references that did not lead to decisions about individuals.

Jim Murray, the Director of BEUC, told the Workshop that he did not expect to be tracked by camera as he went round a store; nor did he expect to be treated in a similar way on the Internet by the analysis and profiling of his clickstream. He doubted whether Web sites conformed either to data protection laws in Europe or to the OECD Guidelines. Generally, consumers were not told what was happening to their data, nor could they exercise any choice. Education as a policy instrument had limited value. It was often used as an excuse for avoiding regulation. Customers were compelled to provide information by standard contractual clauses. Education did not give individuals the power of choice, nor did it substitute for restrictions on abuse. Systems should be user friendly and not require lengthy education for individuals to deal with them. He was sceptical about self-regulation which was often a pretence. There needed to be a measure of the outcomes and of the content of self-regulatory codes. There had to be independent redress for individuals. A formal law was not essential, but it was for governments to vindicate the rights of individuals. They could delegate but not abdicate. He asked whether industry had ever suggested self-regulation to deal with the problems of intellectual property. There should be tests of consumer privacy protection related to the knowledge of the consumer, the information provided, the opportunity for subject access, and the right to correct errors.

Jean-Marc Mosconi of Mercatel explained the market pressures on businesses in mature markets to devise more sophisticated and appealing products. For that they needed extensive information

about actual and potential customers. This collection and analysis of customer information was a major trend to which limits must be set in order to exclude invasions of privacy and loss of consumer confidence. Many companies behaved responsibly for example those who had signed the mail order charter and did not collect specially sensitive data. The Internet provided the opportunity to collect information secretly. Consumer confidence and a loyal customer base were business assets. Businesses should make their policies clear thereby helping to educate the public. Those businesses which adopted good practices should be publicly acknowledged and encouraged.

Marc Rotenberg, the Director of EPIC, told the Workshop of the results of two surveys. EPIC had looked at the privacy practices of 49 Web sites which collected personally identifiable information. Only 17 had privacy statements, and they were not easy to find; only eight had restrictions on secondary use. A good policy would set out the rights of individuals and the responsibilities of the organisation. He emphasised that cookies were a problem and that the ability to be anonymous was important. There was no assurance of independent audit on the sites studied. In his view, notice and consent did not produce a market solution. The second study by the Georgia Institute of Technology showed that privacy was the principal concern of users and that concern was highest in the United States: 83 per cent of respondents favoured anonymous use of the Internet; 72 per cent supported privacy laws. The level of concern in the US had risen not fallen, which rather indicated that self-regulation had not worked. Users wanted anonymity and so privacy protection was vital.

The panel for this session responded to the contributions and a discussion followed. Many of the points made reinforced elements of the contributors' presentations. Doubt was cast on the proposal that a distinction could be drawn between named information held in relation to decisions about the person and about a business. Support was given to the role of education to allow individuals to defend themselves. The Workshop was reminded of the importance of personal information for business purposes particularly in credit granting. Lack of transparency on the Web created a different situation from conventional shopping. Consumers needed to know with whom they were dealing and what rules applied. Education could be like signs warning of a damaged highway, but the road still needed to be repaired. Education was not a substitute for good policy, but it was a valuable element. How would education be delivered and by whom? The need of business for good privacy protection and understanding of what was required were mentioned. In a global system one could not expect perfect compliance, and the more clear and explicit the privacy promise, the easier it would be to enforce.

The conclusions of the session were presented by the chair during Session 5.

Session 2: Technological solutions to protect privacy online

The Orientation Paper explained that this session, which was chaired by **Roger Needham**, aimed "to point out that technological solutions can assist in implementing the OECD Privacy Guidelines on global information networks." He asked the participants to bear in mind that technical solutions were often available if users were aware of the need and capability; that it was easy to design a solution for the wrong problem; and that the effectiveness of technical solutions depended on the environment for which they were designed and in which they would work He suggested that governments often prevented the environment from being sufficiently universal for a technical solution to be effective.

John Borking from the Dutch data protection authority explained their thinking about privacy enhancing technologies. These were technical measures to safeguard personal privacy by minimising or eliminating the collection of identifiable data. There was a global trend to more collection and processing of personal information with a consequent loss of anonymity. To restore anonymity they had asked

whether personal data could not be excluded from systems without loss of functionality and the necessary authentication and non-repudiation elements. Could technology translate social and legal requirements into hard specification, the object of which would be to enable the individual to keep control? They had developed the idea of an identity protector on the communication lines between separate modules of an information system. The ID protector would create pseudo-identities and there would be separate domains in one of which one was known and in others unknown. A live example was a hospital information system developed as a response to an audit of a psychiatric hospital. Sub-modules of the information system were created so that only the essential carers knew the true identity of the individual. The system worked without loss of functionality and was based on the principle of whether or not it was necessary to process personal data.

Anne Troye-Walker, from the European Commission (DGXV) explained what steps the Commission was taking to encourage the development of privacy enhancing technologies. She mentioned the requirements of Directive 95/46/EC and the Commission's Electronic Commerce Initiative of April 1997 which aimed to create confidence for consumers by securing compliance with the data protection directive and minimising the use of personal data. She spoke of the work already undertaken in the Fourth Framework Programme to commission research which would address the legal constraints on the use of personal data collection and profiling systems. She spoke particularly of the E-Clip project to give legal support and analysis to other projects in order to find technological solutions to legal problems. The Fifth Framework Programme which was in preparation would include a specific programme aimed at the creation of a user-friendly information society. The programme would address the requirements for the enhancement of consumer and business confidence in electronic commerce; it would examine technologies to support legal compliance; and it would specifically consider privacy enhancing technologies to secure information integrity and privacy.

Charles Prescott of the US Council for International Business briefly explained the work of USCIB. He commended the OECD Guidelines as a technologically neutral useful guide. He believed that much anxiety was caused by the fear of new technologies. Citizens would have to learn to use new tools in the same way that they had come to be comfortable with the benefits of electricity. Information would lead to empowerment of the citizen. Businesses had a duty to educate, but individuals had a duty to understand and take steps for themselves. Tools were being developed to tame the "wild west" of the Information Society. Some might prove ineffective, but at least one would be found to succeed.

Stefan Engel-Flechsig of the German Federal Ministry of Research and Technology told participants of the German multimedia law of August 1997. Protection of personal data in global networks posed new challenges, including the difficulty of individuals' establishing control. There were new opportunities not only for improved services, but also for technological protection of personal privacy. Some business sectors lagged far behind in using privacy enhancing technology. Technology had to be an integral part of data protection and the legal environment had to match the new technologies. The principles of data avoidance, of anonymity or pseudonimity, and secure electronic consent should be adopted. New legal concepts should allow for flexibility and the use of different tools. Multilateral security and inter-operability should be guaranteed. Data protection auditing would provide a quality guarantee.

Josef Dietl of the World Wide Web Consortium introduced W3C and explained the Platform for Privacy Preferences Project (P3P). The principles behind P3P were that there should be personal choice with informed consent, commitment by Web publishers, an opportunity to form agreements on privacy practices, and digital signatures to aid enforcement. Users would set generic preferences in their Web browsers, so that the browsers would scan sites visited. If a site complied with those preferences, no action would be apparent to the user. Exceptional sites would be alerted to the user, and there should then

be an opportunity for dialogue to establish whether or not and on what basis a user would proceed to visit a site. Whilst a user should be able to download standard preferences from trusted sites, publishers should provide a clear statement of privacy practice, and the technology would thereafter facilitate negotiation and agreement between the user and the publisher. Digital signatures would aid enforcement of privacy statements by guaranteeing their integrity and authenticity. The technology would prevent data transfers not authorised by an individual; and whereas the market would provide trust and auditing services, regulation should ensure that there were no deceptive or fraudulent uses of privacy statements. The P3 Project had started in June 1997 and was coming to the end of its second phase at the time of the Workshop.

Jean-Pierre Camelot of Groupement des Cartes Bancaires spoke of the French approach to electronic cash. On consumer protection grounds, he doubted whether anonymity ought to be provided. Confidentiality should be guaranteed, but transactions should be traceable to secure consumer redress, to settle disputes between consumer and merchant, to detect fraud, and to prevent tax evasion. There was no full anonymity in current card systems, but the use of card information was restricted. There was extensive use of payment cards in France; there was no difference from the shopkeeper's point of view between a credit and a debit card. The same systems would support an electronic purse, but he doubted whether it should be described as cash. There would be restrictions on issuing cards and anonymity would depend on whether cards were linked to bank accounts. In France, he expected cash cards to comply with the EMV standard and to be introduced for low value transactions in the transport sector. Bank payment cards would probably be used for Internet transactions. Payment and purse functions could be on the same card. He expected that initially with an electronic purse there would be little aggregation of transactions for consumer protection reasons; when, with experience, confidence grew in the system, greater aggregation of transactions might be introduced with a consequently greater degree of anonymity.

Lance Cottrell from Infonex Internet Inc explained the need for anonymity and the success of anonymous services such as The Anonymiser. The service worked at a profit on the Internet including non-Web functions such as internet telephony. Net activity was logged as distinct from the relative anonymity of ordinary life. The Anonymiser was a trusted third party (TTP) and an identity protector. Access to the Internet via an Anoymiser server stripped out identifiers. Pseudonymity available through strong cryptography would be useful. There was a demand for the service to avoid censorship, to be able to express opinions which were unpopular or sometimes even dangerous for the individual, to avoid association with an employer, to avoid profiling, to avoid traffic analysis, and to avoid research. The system worked in real time and for store and forward services such as e-mail. His company knew who the customers really were and therefore had a TTP function. They deleted the traffic information collected. The system did not need the co-operation of data collectors; there was no dependence on a helpful legal jurisdiction; and there was no invasive monitoring of businesses. Separate identities could be created with different businesses, but in some cases such as dealing with government a real name was required. Identification was not the same as identity. There were difficult issues of liability, but despite criticisms of encouraging irresponsible and illegal behaviour, they were not aware of the use of the system for illegal purposes. Law breakers would always find systems to abuse. Anonymity could probably not be stopped because of the ease of moving to different legal jurisdictions.

Sean Gaddis was unable to join the Workshop to deliver his presentation on the Open Profiling Standard (OPS) which was intended to provide a standard technological framework for consumers and businesses to overcome the lack of trust on the Internet. OPS had been submitted to W3C for incorporation in P3P.

The panel responded to the presentations and a discussion took place. It was suggested that anonymity might not be desirable: a patient might be placed at risk by identity protection. It was said that

technology might be a surrogate for government action. It could give individuals market power, but would individuals feel protected? How easy would systems be to use, and what would the system default settings be? How could a consumer know that a Web site was trustworthy? Government intervention would be needed to take action against fraudulent policy practices. The Workshop was reminded of the overhead costs of the widespread use of encryption, but it was told that the privacy enhancing costs of the hospital example were perhaps less than 1 per cent of the cost of building the system. It was, in any case, doubted whether the hospital example would work effectively outside a closed environment. The cultural and national differences in privacy preferences were raised. The problem of Internet libel using anonymity was discussed without any clear solution. One panelist was a sceptical believer in privacy enhancing technologies: privacy was more than anonymity and there were strong economic pressures to hand over information. It was a political and social policy issue, not a technical problem. The discussion emphasised the importance of personal choice and the use of technology to deliver such choice; there might be a trade-off between anonymity and consumer protection and other considerations, such as helping individuals and their families in cases of emergency. Some support was expressed for distinguishing anonymity from confidentiality. The view was expressed that the correct policy was that on-line matters should be treated in the same way as off-line information, and the comment was made that technical and policy issues tended to become confused.

The Chair presented the results of the session during Session 5.

Session 3: Private sector-developed mechanisms to ensure effective implementation of codes of conduct and standards in a global environment

This session chaired by **Barbara Wellbery** from the United States Department of Commerce was, as explained by the Orientation Paper, "intended to look at recent practical implementation of codes of conduct and industry standards using enforceable mechanisms to ensure effective protection of personal information." The Chair asked participants to bear in mind several considerations: the need to find ways to bridge the different approaches to privacy protection; the lack of omnibus privacy laws in most countries; the fact that the lack of such laws did not mean that privacy was not regarded in those countries; compliance with privacy protection rules was not automatically guaranteed by law; flexible self-regulation unrestricted by jurisdictional borders might deliver effective compliance; restriction of information flows could have severe economic consequences; and the individual should get the privacy he chose.

The first contributor was **Mona Goldstein** from the Canadian Direct Marketing Association (CDMA). She explained how the Association was the predominant marketing association in Canada and that it had moved from relative ignorance of privacy protection through the development of a self-regulatory code to a recent call for legislation. A seven point compulsory privacy code, based on the OECD Guidelines, was adopted in 1993. The code set out principles because specific rules tended to create loopholes. In 1996 the Canadian Standards Association (CSA) published its Model Code of ten principles and the CDMA Code had been reviewed in the light of the CSA Model Code and a collection principle added. The CDMA had called for legislation based on the CSA Model Code to establish a level playing field, to establish consumer confidence, and to facilitate international trade. The CDMA had developed on-line marketing rules because of the unique nature of the Internet. Consent would be required for marketing by e-mail. Spamming was not permitted. A reply mechanism would be required for all e-mails and members had to maintain suppression lists. Members were required to disclose any marrying of clickstream data to individual identity. The CDMA had lost no members as a result of their code and had become advocates for legislation.

Yuji Yamadori from the Japan Information Processing Development Center (JIPDEC) presented to the Workshop the system for granting privacy marks which JIPDEC would trial from 1 April 1998. He explained that MITI had published private sector privacy guidelines in 1985 which had been reviewed in the light of the EU Directive resulting in the publication of new Guidelines in March 1997. A committee was looking at how to implement them. It was proposed to establish a system to certify those complying with the MITI Guidelines; that would help to secure implementation, increase awareness and enhance the Guidelines. A system had been established by which trade bodies could grant marks to member companies. JIPDEC would also grant marks directly to and certify companies. There was a reporting procedure and MITI would supervise the whole process. JIPDEC would consider complaints from individuals. It was hoped that the system could be launched after a year's trial on 1 April 1999.

Yasuo Hasebe remarked that there had been a great increase in the flow of personal data, leading to consumer concern. Consequently in September 1991, the Japanese Ministry of Posts and Telecommunications had published guidelines for the communications sector based largely on the OECD Guidelines. They dealt with the collection, use and disclosure of personal data and with the right of subject access. There had been more recent Guidelines on calling line identification and in September 1996 Pay TV Guidelines dealing with the use of subscriber data. Many nodes give rise to a risk of access to communications data, and information could be collected from access logs. There were privacy risks in electronic trading. In December 1997 the Privacy Working Group of the Cyber Business Association had produced self-regulatory guidelines. Individuals should be told how their data would be used and if access logs would be cross-referenced to other information. The demand for protection would grow with the growth of Internet trading. Data subjects did not know what data were collected nor how they were used; they could not, therefore, judge the propriety of information handling. Data subjects must be informed, perhaps by the display of a privacy mark. The Ministry of Posts could register those companies following a privacy policy and award a mark. Some municipalities had already adopted that practice. If self-regulation failed legislation might be needed. He expected the cost of privacy regulation to increase with deregulation of telecommunications. Regulation might be required for the whole sector or for each industry.

William Burrington of America Online claimed the Internet as the communications and e-commerce medium for the 21st century. It would be a global medium for democracy and trade; it would encourage economic growth and the expansion of employment. The digital economy gave added value and power to individuals. The problem was that the vast majority were concerned about threats to privacy as a result of media exaggeration and misunderstanding of technology. In reality, very few using on-line services or the Internet had suffered invasions of privacy. The majority supported profiling for marketing purposes. In short, consumers were concerned, but there was little evidence of abuse. Government must not add to the privacy invasion hysteria. Clear? meaningful privacy policies should be adopted and bad actors discouraged. There was a real opportunity to provide the benefits of the "one to one" medium for all, and privacy should be protected by business in co-operation with government. A new self-regulatory model was required for the digital age. The catalysts would be government and consumer market pressure. Companies must feel the economic pain of non-compliance.

Ronald Plesser of Piper and Marbury wished to tell the Workshop about self-regulation by the US Individual Reference Services Group (IRSG) and by the US Direct Marketing Association (USDMA). The members of IRSG provided information to assist in identifying individuals. As a consequence of a political dispute over the service about a year previously, the industry had acted to prevent legislation. The system was not truly self-regulatory. Fourteen companies had individually signed a Code. They committed themselves not to make available information given for marketing, not to distribute generally information such as social security numbers, nor to permit searching by social security number, to educate the public, to give subject access, to enable individuals to prohibit the general distribution of non-public

information, and not usually to distribute information about children. Those principles were enforced by independent audit, by contractual ties on those who bought information from IRSG members, and by the risk of prosecution for deceptive trade practices if IRSG members failed to comply with the Code they had adopted. The DMA had adopted on-line privacy principles which the speaker briefly outlined. It would be a condition of DMA membership that members should give prominent notice of their information practices to consumers, that they should enable consumers to opt out of their information being rented, sold, or exchanged and that they should comply with the rules of the Mail Preference Service. These rules were enforced by the DMA's Committee on Ethical Business Practice. The DMA also had rules about the use of e-mail for marketing and the collection of information from or about children.

Stephen Wooley, a partner in Price Waterhouse, told the Workshop of his experience as a private sector privacy auditor in Australia. The Privacy Act 1988 based on the OECD Guidelines applied to Commonwealth Agencies and Federal Departments. Although the government had planned to extend legislation to the private sector, that proposal had been abandoned in favour of the development of industry self-regulatory codes. Legislation was, however, proceeding both at a State level and also to apply to suppliers of outsourced services to the federal government. The costs of codes were the cost of development, the process re-engineering costs and the cost of monitoring and compliance. Guidance and support for codes could be found in national and state legislation and external instruments such as the EU Directive. Complaint mechanisms were a problem: should they be internal or external, and how should consumers be given redress? The speaker used as an example Telstra, the previously state-owned national telecommunications carrier. The internal company code demonstrated social responsibility, was part of the company risk management strategy, helped to facilitate transborder data flows, and gave a competitive advantage by increasing consumer confidence which had previously been lacking. The Telstra Code had 12 principles and the Canadian model code had been looked at in its development. It was enforced by an independent compliance audit programme resulting in a published annual report. In the first audit, a lack of awareness and a need for internal education had been apparent. There had been considerable improvement with the adoption of privacy impact statements and the appointment of privacy co-ordinators. Consumer redress was both internal and by appeal to the Telecommunications Ombudsman. Guidelines were to be produced for caller identification. Telstra was seen as a market leader. The privacy auditor was, however, not always popular for slowing down product development.

Susan Scott, the Executive Director of TRUSTe, described the service offered by the organisation. The TRUSTe system was intended to implement information privacy practices through effective self-regulation. It would increase the acceptance of electronic commerce, give users control, give Web publishers a means of compliance, and regulators an assurance. The site would contract with TRUSTe to adopt a privacy policy, to disclose and adhere to that policy, to display the TRUSTe mark and to co-operate with TRUSTe in conducting audits. Clicking on the mark would display the privacy policy. TRUSTe would work with a site to develop a policy, but it was for the site to determine what it would be willing to do. There would be initial and periodic site reviews. Seeding was used to track activities and independent auditors were used. TRUSTe would consider consumer complaints; the site could be re-audited and would have to pay the cost if found not to be complying with its stated policy. Malicious and fraudulent cases would be referred to the FTC. Contractual and intellectual property remedies were also available. This was a flexible programme with effective enforcement, helping many companies who were responding to US government pressure for self-regulation.

Alastair Tempest of FEDMA spoke of a study of on-line codes of practice and privacy statements. There were great differences in the presentation of codes. The codes were easy to access, but that was not always true of on-line privacy statements. If a Web site did not wish to use someone such as TRUSTe, it could display a privacy icon which would indicate the existence of a privacy policy and give access to it. Important issues were the collection of data, child protection, and the clarity of publicity.

Privacy rights should give the right to opt-out of marketing uses, the right to know the uses to which information was being put and rights to access and rectification. Existing legislation and codes gave all the guidance needed. They together with technological measures could provide consumer privacy protection in order to build consumer confidence. A good starting place was the OECD Guidelines.

As in the case of the other sessions, a panel responded to the presentations and a discussion ensued. The fear was expressed that the proliferation of marks might lead to increasing confusion about what was meant by privacy. Large companies could develop quality codes, but small organisations would increase in number in electronic commerce. The OECD Guidelines called for international co-operation and co-ordination on implementation and that was still required. In further comment, doubt was expressed about how co-operation could be achieved between those with legislation and those who preferred self-regulation. A diversity of approaches was possible and legislation was not necessarily superior. Auditing and labelling were possible routes to enforcement, but alternative dispute resolution procedures (ADR) should also be considered. The question was asked whether codes of conduct could be truly effective and whether they were just a step on the way to legislation. There was the problem of codes applying only to the members of a trade association and also the problem of competing codes. Concern was expressed about the difficulty of an individual obtaining redress in a foreign jurisdiction. On this matter there was an extended discussion including the suggestion that the problem was made worse by the small size of Internet transactions which meant that it was uneconomic for an individual to seek to defend his rights. It was pointed out that the problem of consumer redress in foreign jurisdictions went beyond privacy matters. Several contributors expressed optimism for self-regulatory means based on the OECD Guidelines; self-regulation did not mean the absence of law. Participants were reminded of the concern expressed by individuals about privacy matters and the different solutions to the problem, including the Japanese government sponsored guidelines for the private sector. Doubt was cast on the effectiveness of the CDMA prohibition on spamming.

The Chair presented the conclusions of the session during Session 5.

Session 4: Transborder data flows and the coexistence of different systems founded on law and/or self-regulation: examination of contractual solutions

For this session the Orientation Paper told the participants that, “Among other legal techniques for assuring privacy of data in transborder data flows, contracts have their place in the context of international networks.” The session aimed “at discussing the advantages and disadvantages of such contractual arrangements in an online environment.” The chair was taken by Philippe Lemoine of Groupe Galeries Lafayette who recalled that he had participated in the process of setting up the ICCP Committee which had prepared the OECD privacy Guidelines. There were two main themes to be borne in mind: on the one hand, the internationalisation and interconnection of networks, and on the other, the growth in the diversity and universality of processing personal information, with an accompanying growth in the technical resources available for that purpose. It was in this context that the question of protecting individual data, which for 20 years had been subjected to a variety of approaches based on law or self-regulation, had to be addressed today.

The EU Directive had harmonised law within the European Union and permitted free transfer outside the EU provided that the protection afforded by the Directive was respected. The chair explained the requirement of Article 25 of the EU Directive for adequate protection in third countries and the exceptions available including contractual protection under Article 26(2) and where transfers are made in a contractual context under Article 26(1). Contracts could allow for the coexistence of systems based both on law and on self-regulation. The use of contracts raised questions relating to their content,

standardisation and their legal impact (particularly, the consequences arising from failure to observe contract terms or more fundamental breaches of contract). The scope of these legal questions had become more wide-ranging as a result of the development of the Internet and electronic commerce.

It was a highly topical subject: the Internet symbolised global commerce; faced with a rapid expansion in the number of transactions there was a need to define a stable lasting framework for business; the Internet brought profound change to markets; and adjusting contracts to that reality was a complex problem.

Three points were inescapable. First, the increase in business to consumer transactions was reorganising the intermediation process: a consumer might deal with a business located in another country; new intermediaries would appear and enlarge the number of suppliers; consequently, questions had to be answered about the means of protecting personal data, and adapting contracts to "consumer zapping" and to the shared access to customers. Secondly, the great difference in social and legal policy between countries had to be faced; so for example, consent might not be sufficient in some countries to permit the processing of sensitive data. Accordingly, one had to address the issues of consumer consent mechanisms, methods of controlling personal data flows, and the implementation of different public policies. Thirdly, there was the issue of applicable law: the question was whose jurisdiction would apply to a transaction, that of the provider or the consumer. The chair left us with an example: the problem of credit information the use of which was subject to strict legal control in some European jurisdictions. It was not clear how those restrictions could apply to a globally operating credit reference agency.

Susan Binns, a Director of DGXV of the European Commission, noted that 15 Member countries had gone beyond the non-binding OECD Guidelines with the adoption of the EU Directive. Fundamental rights had to be protected in the same way as physical safety. Rules of limited geographical application caused problems and the European Commission wished to see a wider agreement on data protection through GATS or the WTO. The variety of law, guidelines and private sector self-regulation should not create an unmanageable problem. The difficulty would be the existence of inadequate standards. Reliance on contracts might be one solution. All OECD Member countries should require of each other adherence to the 1980 Guidelines; where they were not implemented there must remain the possibility of blocking personal data transfers. That was recognised by Article 14 of GATS. The European Commission would prefer to be working with its international partners to find agreed protective arrangements. The speaker dealt with the application of the EU Directive in global systems. It was technologically neutral and applied to EU based Web site operators; the EU looked to independent supervisory authorities to secure compliance. It was not possible or desirable to apply the Directive to services on the Internet delivered from outside the EU and in that context the consent of individuals was important. This was a pragmatic rather than a legal analysis and Article 25 might apply to an internet service provider in a third country regularly inviting European content and then misusing personal data. The Directive relied on the principle of home country control and perhaps an elaboration of Article 14 of GATS could achieve a level of assurance relying on the same principle at an international level. Contracts could support or substitute for law. They could bind data controllers to assure protection. The contract must satisfactorily compensate for the lack of law. It must be detailed, specify the purpose of the processing and prohibit further disclosure. Where control remained with a data controller within the EU, no legal difficulty would arise. Confidence could be boosted by audit, perhaps in the manner agreed by the Berlin Data Protection Commissioner. Self-regulation was encouraging; but the problem of enforcement remained. Contracts would have an important role, but the European Commission wished first to look at more general solutions.

Christopher Millard, a partner in Clifford Chance, then spoke of the massively networked technical environment and the problem of the mainframe assumptions of the 1980 Guidelines, the Council

of Europe Data Protection Convention (European Treaty Series No. 108) and the EU Directive 95/46/EC, all of which relied on the notion of an identifiable data controller. SMEs were increasingly dependent on cross-border data communications. One hundred million people had Internet access, but most without any data protection. Internet routings were not predictable. Millions of Web pages were cached in multiple jurisdictions; and "push" technologies would also have an impact. In all, large quantities of personal data were being transferred into and out of the EU. From 24 October 1998, the adequate protection rule would apply, but only 35 jurisdictions had a data protection law. Article 26(1) of the EU Directive provided exemptions and 26(2) permitted transfers where safeguards were provided which might be by contractual means. Contracts might be between controllers, or between controllers and processors. Article 26(2), however, gave rise to a cumbersome procedure of notifying the Commission and other member states and an opportunity for objection to the transfer. That procedure might be protracted. Other problems existed, particularly the difficulty of assuring the rights of individuals in those common law jurisdictions which still applied the privacy of contract rule. There were examples of effective contracts; but he believed that the Citibank/German Railway case, which applied to large numbers of customers, was not sufficiently scaleable. He also noted that the Commission was not giving prominence to the possibility of approving model contracts under Article 26(4). In conclusion, contracts would not provide enough help, and reliance would have to be placed on individual consent which might, indeed, be achieved contractually. The vast majority of transfers would escape Articles 25 and 26; neither business nor regulators had the resources to achieve full compliance.

Alexey Kozhemyakov, from the Directorate of Legal Affairs of the Council of Europe, spoke of the work of the Council and the model contract conditions which it had promoted. Use of the 1992 Model Contract could help to resolve the problem of inadequate data protection in some jurisdictions and the lack of global protection. Data Protection was an essential part of the right to private life assured by Article 8 of the European Convention on Human Rights. The Council which was established to promote pluralist democracy and individual rights and freedoms had forty member states. Its Data Protection Convention (Treaty 108) was open to non-members of the Council. Twenty States had ratified the Convention and another 23 had signed it. The Council had produced Recommendations to apply Treaty 108 which referred to transborder data flows and the use of the model contract. The objective of the model contract was to promote the free flow of data and guarantee data protection. The contract conditions regulated disclosure to third parties; they required data protection obligations to be respected; there had to be appropriate guarantees for the processing of sensitive data; and in case of dispute, the contract could be cancelled. Arbitration and applicable law were provided for. The Council had not left matters with the contract conditions; the Data Protection Project Group favoured codes of practice and was working on guidelines for the Internet.

Heather Rowe, a partner in Lovell White Durrant and Chair of the Working Party on Privacy and Data Protection of the International Chamber of Commerce, then spoke about the work of ICC in developing model contract conditions. ICC had developed the 1992 conditions which were endorsed by the Council of Europe, the European Commission and OECD. Under Article 26(2) of the EU Directive, EU member states could approve overseas data transfers guaranteed by contracts. The 1992 conditions were a little jaded and efforts were being made to update them in the light of the work of the Article 29 Working Party. The work would be technologically neutral; it would try to reflect the conditions which the European Commission would expect to see; and it was going through the ICC approval process. It was hoped that the contract would help SMEs. Under the contract, the exporter warranted compliance with its national law and undertook to make arrangements with its national regulator. The importer warranted compliance with the local law. the provision of security measures, home country control, compliance with the exporter's rules, purpose restriction, and constraint on third party disclosure. The risk of legal action in the home country would secure enforcement of the contract. The data subject had a

contractual relationship with the data exporter. The ICC conditions were an updating of the 1992 model contract and somewhat more onerous.

Next **Hans-Jurgen Garstka**, the Berlin Data Protection Commissioner, explained the background and content of the contract with Citicorp which dealt with the problem which arose when the German Railway Discount Card was co-branded by Citicorp to provide a VISA card facility. In July 1995 all new customers and those renewing their discount cards were required to accept the VISA facility and to provide information for credit scoring. The credit card data was to be processed in Nevada and South Dakota. Under German law, foreign processing would only be legal with the consent of individual data subjects and with measures taken to guarantee data protection. There were fears of secondary use of the data abroad and customers complained to the Berlin Data Protection Commissioner. As a consequence German Railways and Citicorp re-negotiated their agreement to the satisfaction of the Berlin Commissioner. The old discount card was reinstated, and customers were allowed to choose whether or not to take the VISA card facility. The Application Forms were changed. Citicorp agreed to the German restrictions on secondary use, so that the personal data were only to be used by Citicorp for card issuing and credit scoring purposes, and the parties agreed to apply German data protection law. There was to be no cross-selling of the two products from data collected for the separate cards. Citicorp would appoint data protection officials; data subjects were given the rights against Citicorp which they would have had under German law; and the Berlin Commissioner was granted the right to carry out inspections in the United States. The Berlin Commissioner was satisfied that this agreement satisfied German data protection law. The agreement was made before the EU Directive was adopted, and because it applied to between 3 and 5 million customers it might not be applicable to smaller scale transfers. Dr Gartska asked whether such a contract would work in a network environment, and whether the restrictive conditions could be implemented. He thought the general availability of strong cryptography would be helpful in protecting data during transmission through global networks.

Peter Fleischer of Microsoft Europe then spoke of Microsoft's privacy compliance programme in Europe. He explained that although the company had 20 000 employees, it was only one tenth the size of IBM. Microsoft had provided support for P3P in its Internet Explorer browser; a cookie warning function had been added together with support for encryption and security measures. Microsoft privacy policies included requirements for notice to users, individual consent, and the rights to opt out and to correct data. Microsoft had been prompted to undertake its Data Protection Compliance Project by consumer concerns, risks to the company's reputation, the threat of enforcement action, and by a desire to promote electronic commerce. Users needed education in what was available to them. Microsoft believed that Codes of Practice required co-operative effort, whereas contracts which were a routine business activity could easily be entered into to secure adequate data protection. In that light, legislation was not needed.

Kouichi Sakusa of the Electronic Commerce Promotion Council of Japan (ECOM) was the last of the principal speakers in Session 4. He described the work of ECOM in producing guidelines and a model home page. If consumers knew about cryptographic protection, they would embrace e-commerce. Effective methods had to be found for legitimate businesses and legitimate customers to do business together. Accordingly ECOM had adopted guidelines on the use of personal data and promulgated a model home page in order to implement the guidelines. Techniques to ensure secure information exchange were set out in the guidelines which also included rules on informing customers, and the use of data. Customers could opt out of marketing uses of personal data. The model home page incorporated the rules and gave access to the guidelines. The data protection screens were accessible from the purchase acceptance screen, and the intention was that consumers should learn about the data protection measures available before confirming a purchase.

This session also concluded with reactions from a panel and a discussion. It was suggested that contracts could not replace codes or laws, but they were a legally robust method of providing a bridge between the different systems of law. A body of principles such as the OECD Guidelines was required as a basis for a contract. New guarantees of anonymity must be provided and mechanisms for individual redress had to be found. The work of ICC on a model contract was valuable pioneering work. The view was expressed that there was a consensus on the need to achieve adherence to a high standard of fair information practice. There was a need for consumer confidence. The mechanism to reach that goal was not important and one would expect sectoral variation. One should seek to cover the widest range of transactions with the least regulation. The view was expressed that data protection was an issue of fundamental human rights and that perhaps it should not be negotiated in the context of international trade bodies. The reality for an EU data protector was that there would not be world-wide adequacy of data protection to the EU standard by October 1998 and a practical way had to be found of allowing responsible companies to continue trading on an international basis. Contractual solutions were an attractive flexible option for providing privacy protection. There was also the possibility that contracts might be formed between individuals and data controllers and not just between importers and exporters. Contracts might be a means of repatriating remedies and jurisdiction to the country of the consumer. This contributor did have doubts about how the contractual solution could be made to work in a global network environment. The view was expressed that for the banking industry there were great advantages to the contractual solution. The flexibility allowed gaps in legal protection to be filled at no cost to public resources. The protection offered by the Citicorp contract was emphasised and the panellist doubted whether there was a practical problem relating to the scale of the operation; but it was suggested that there was a difficulty created by the tension between the principles of home country and host country control. In the course of the general discussion which followed, the point was made that in some circumstances the only means of delivering privacy protection would be the use of contractual guarantees. Contracts had so far only been used in closed systems rather than in open networks. It was thought that there was scope for contractual agreements between consumers and providers. Doubt was cast on the validity of a consent given merely by clicking on a box; on the other hand, it was explained that users were often asked to do more than that: for example, to type in their name. There was a discussion about the need for a legislative basis to provide an accepted body of principles to be enforced by contractual arrangements. Concern was expressed about contracts being used to seek the waiver of rights of individuals. Emphasis was placed on the value of contracts for securing effective enforcement of the OECD Privacy Principles.

BIAC took the opportunity of this session to make clear its reaction to the Workshop. BIAC applauded the efforts of OECD to highlight the relevance and applicability of the 1980 Guidelines to Internet related privacy concerns. Many businesses and trade bodies had used the Guidelines as a basis for privacy codes and practices. Business had responded to consumer privacy concerns. BIAC continued to support the Guidelines and believed that, notwithstanding their age, they were applicable to the Internet without revision. They continued to be the basis for industry self-regulation and OECD could promote their implementation by surveying the mechanisms that had been developed in the OECD Member countries for privacy protection. OECD should also monitor the development of privacy enhancing technologies and their ability to further the 1980 Principles. BIAC also joined in the call for consumer education in both privacy and new technologies and suggested that policy makers should consider technological development in the creation, evaluation and oversight of privacy codes and practices.

The conclusions of this session were also reported by the chair in the final session.

Session 5: Main conclusions of each session and of the Workshop

This last session of the Workshop was an opportunity for the session chairs to report their assessment of the work of each session and to put forward conclusions and suggestions for further work. The chair of the plenary Workshop then took the opportunity to summarise its work and look forward to the Ottawa ministerial conference.

Mads Bryde Andersen spoke for the first session which had discussed issues relating to education. He started from the point that the OECD Privacy Guidelines provided a globally accepted set of privacy principles. They could provide a basis for the protection of users of global electronic networks. There was a need for education and transparency: two concepts which he wished to differentiate. Users of global networks required more transparency. It was a question of applying the openness principle, Principle 12, of the 1980 Guidelines. A user should know what privacy policy a site applied in relation to data collection, its use of cookies, the uses it made of data, and similar matters. More generally users should be aware of their rights and of the capabilities of the technology in relation to matters such as the preferences which could be selected when using Web browsers. The session had not focused on the roles of governments, NGOs, business and consumers and international bodies such as OECD in relation to general education, but it would be welcome if the formal education system were to take up the general task of educating users in the technology and their rights. The session had dealt largely with providing transparency through self-regulation. The consumer advocates had argued for consumer redress mechanisms of a formal nature. Business and consumers clearly needed to talk and exchange views to reach a consensus on transparency in global networks. OECD could facilitate that dialogue by providing a forum, conducting studies and generating proposals.

Roger Needham presented the conclusions of the second session. Technology should be the servant of policy; one had to decide as a matter of policy how people should be able to behave in networked systems. Some things could be done anonymously and in those cases users needed to have no concern about other measures -- such as legal restrictions -- for their privacy protection. The session had considered a successful Dutch application of anonymous use in a closed system, but it was not clear to what extent transactions could in general be conducted anonymously or to what degree the technology could provide that protection of anonymity in open systems. Further study was required of the extent to which the technical capability of providing anonymity could be used as the means to deliver privacy protection. If anonymity were thought to be too strong a level of protection, then systems such as P3P could provide for the identification of sufficient trust and confidence to reassure users and permit transactions to proceed. A system such as P3P was not a perfect solution and further study was required both of the extent to which such technical applications could assist privacy protection and also on methods of enforcing compliance with privacy policies in a global environment. There was a spectrum of measures from anonymity, through schemes such as P3P to contractual guarantees, but no technical measure could provide a perfect solution. Further study was required of the policy questions which the technical measures were designed to answer.

The chair of the third session, **Barbara Wellbery**, spoke of the three themes and the areas for further study which had emerged from that session. First, a variety of self-regulatory means for delivering private sector privacy protection had been identified. Examples had been provided from Japan, Australia, Canada and the United States which had been prompted by a range of forces from market pressure to fear of legislation. Secondly, the session had considered the variety of methods of enforcing codes and privacy statements ranging from labelling and certification through third-party audit to formal enforcement by a regulatory body. This was an area that warranted further study. Thirdly, the session had looked at the question of individual redress. Internal dispute machinery was important, but the session had also heard of the value of an external appeal mechanism. Two further areas of study identified were the need for

international co-operation to achieve effective self-regulation in e-commerce, and the ways in which consumer redress could be provided for customers trading in foreign jurisdictions.

Philippe Lemoine, the chair of session 4, presented the findings of that session. Two matters had been agreed: first, that instruments had to be found to reconcile the world-wide character of the Web with the different legal approaches of Member countries; and secondly, that the 1980 OECD Guidelines were an important starting point. He identified five areas for further study. Work needed to be done on the scope for and the legal basis of contractual solutions to privacy protection. It would be especially valuable to look at case studies in addition to the German Railway example. Secondly there was the issue of consent and how that might properly be given by a Web-surfer. Thirdly there were questions of public and legal policy (*ordre public*), for example, where a state wished to make it impossible for individuals to give a valid consent to the use of sensitive personal data and how that policy could be made effective in a global context. Fourthly, there were questions of applicable law, typically whether the law of the user or the provider should apply to a transaction. Fifth were issues of methodology, for a cross-roads had been reached between the legal and technological agenda. An open mind should be kept, for it was not possible to forecast technical progress accurately. The way forward should be an approach which did not impede the consideration of the questions, especially in the United States, because those questions reflected the concerns of consumers. At the same time, further questioning should not be avoided in Europe, where there was already legislation, and new relations should be put in place between public authorities, consumers and the private sector.

The two days were brought to a conclusion by **Michelle d'Auray**. She first thanked the OECD and BIAC for having arranged the workshop, the session chairs, speakers and panellists for their contributions, and the Secretariat, particularly Anne Carblanc, for the excellence of the result. She reminded participants that in opening the Workshop, she had referred to the importance of the work because privacy issues were integral to the work of the Ottawa Conference on electronic commerce in October 1998. Consumer confidence in privacy protection was one of a number of key issues which she mentioned for fostering the growth of electronic commerce. The Workshop had clearly highlighted the importance of the issue especially in a globally networked environment. The Workshop had confirmed the view that the 1980 Guidelines had stood the test of time. Since 1980 there had been two major developments, the creation of an extensive range of instruments to implement the Guidelines, and secondly, the growth of pervasive networked communications with their impact on business, citizens, governments and privacy authorities. The first development was a cause for optimism, but the second posed challenges. Both had been central to the session discussions. Without attempting to review the whole Workshop, she recalled some particular points and two themes which had been identified during the sessions. The wide range of instruments for giving effect to the Guidelines and also the issues of the security and global nature of networks had been pointed out; and the Workshop had learnt of the scope of the tools, the aims of the different actors and the points of convergence. There was convergence on privacy objectives to give individual control over personal data. There was also convergence on the key issues: allowing free flow of data; on the flexibility of instruments; on the need for effectiveness; on the potential of technology; on the requirement for enforcement and redress; and on the need for better education. Citizens, business, government, privacy bodies and international organisations all had to address the key questions in the light of the range of privacy instruments and the impact of networked communications. There was a need to clarify how the instruments would ensure global protection of privacy that satisfied the criteria of effectiveness, enforceability, efficiency, and intelligibility, but which also gave individuals control, permitted information sharing, made sense for business, and was also technologically innovative. Ways had to be found to accommodate differences of approach and to provide seamless protection for individuals. The roles of all actors in providing education needed to be clarified. Further study was required and she proposed that OECD form a group of experts to develop a matrix assessing the variety of privacy instruments and their application in a networked environment against the

OECD Guidelines, and to assess whether those instruments gave comparable privacy protection to individuals, whilst giving businesses comparable access to information across jurisdictions. Perhaps case studies would be an interesting approach to the study. The study should identify comparability and bridges between different approaches, but also gaps in coverage and specific barriers to interoperability. Preferably it would suggest solutions, perhaps in the form of standards for privacy instruments as they applied in a networked environment. It would be helpful for that report to be available by June 1998 for consideration by Member countries with a view to debate in Ottawa in October 1998. But at the least there would be a report of the Workshop which would show the importance which all attached to privacy protection. She concluded with repeated thanks to OECD, BIAC and the Secretariat, and hoped that all participants would, like herself, take back to their countries food for thought and interesting ideas for the development of national policies.

LIST OF PARTICIPANTS

Mr. Perri 6	Research Director Demos United Kingdom
Mr. Marty ABRAMS	Vice President, Information Policy and Privacy, Experian United States
Mr. Nezih AGAN	Expert UnderSecretariat of Treasury Turkey
Ms. Andrée AHANO	Director, European Government Affairs Business The Dun & Bradstreet Corporation Belgium
Mr. Joseph ALHADEFF	Director, Electronic Commerce US Council for International Business United States
Mr. Francis ALDHOUSE	Deputy Registrar Data Protection United Kingdom
Ms. Michelle d'AURAY	Executive Director of the Electronic Commerce Task Force Industry Canada Canada
Ms. Mari BO HAUGSTAD	Ministry of Justice Norway
Mr Alain BAILLIART	Consultant Séléction du Reader's Digest ICC
Ms. Fabrizia BENINI	Administrator European Commission Belgium

Ms. Susan BINNS	Director DG XV, Internal Market European Commission Belgium
Mr. John BORKING	Vice President of the Data Protection Commission Netherlands
M. Hubert BOUCHET	Secrétaire Général de l'Union des Cadres et Ingénieurs - Force ouvrière (UCIFO) France
M. Claude BOULLE	Groupe Bull - European Cooperation France
M. Guy BRAIBANT	Président de section honoraire au Conseil d'Etat Mission d'Etude sur le Traitement des Données Personnelles France
Ms. Paula BRUENING	Attorney Advisor, National Telecommunications and Information Administration U.S. Department of Commerce United States
Ms. Helena R. BRUS	Director, Economic and Health Care Policy Merck & Co. Inc. Human Health Division United States
Mr. Mads BRYDE ANDERSEN	Professor Københavns Universited Denmark
Ms. Ingeborg BUCHALIK	Permanent Delegation of Norway to the OECD
Counsellor Gianni BUONOMO	Authority for Information Technology in Public Administration Italy
M. Didier BUREAU	Directeur adjoint, Ministère de l'industrie France
Mr. Herbert BURKERT	Institute for Media Communication German National Research Centre for Information Technology Germany

Mr. William W. BURRINGTON	Director Law and Global Public Policy Associate General Counsel America Online, Inc United States
Ms. J. Beckwith BURR	Acting Associate Administrator Office of International Affairs National Telecommunications and Information Administration U.S. Department of Commerce United States
Ms. Mireille BUSSON	European Regulatory Affairs Adviser British Telecom United Kingdom
M. Jean-Pierre CAMELOT	Groupement des Cartes Bancaires France
Ms. Anne CARBLANC	Consultant ICCP Division Directorate for Science, Technology and Industry OECD
Dr. Seung Hee CHOI	Senior Researcher Electronics and Telecommunications Research Institute Korea
Ms. Jean CANTRELL	Director, Government Affairs The Dun & Bradstreet Corporation United States
Mr. Philippe COEN	Counsel The Walt Disney Company France
Ms. Jane COFFIN	Telecommunications Policy Analyst National Telecommunications and Information Administration Office of International Affairs U.S. Department of Commerce United States
Mr. Lance COTTRELL	Infonex Inc. United States

Mr. Piper COLE	Director of Global Public Policy Deputy General Counsel Sun Microsystems, Inc. United States
Ms. Pamela DEACON	Counsellor Permanent Delegation of Canada to the OECD
Ms. Heleen DE BRABANDER-YPES	Ministry of Economic Affairs The Hague Netherlands
Mr. Edgar DE LANGE	Ministry of Transport, Public Works and Water Management, Telecommunication and Post Department Policy Affairs Directorate Netherlands
Mme Anne DE LA PRESLE	Secrétariat général du gouvernement France
Mme Pascale DE SAINTE-AGATHE	Ministère de l'industrie France
M. Bart DE SCHUTTER	Membre de la Commission pour la protection de la vie privée VUB-CIRT Belgium
Mr. Carlo Sarzana DI S. IPPOLITO	Président Adjoint de la Chambre des Juges des Enquêtes Preliminaires - Tribunal de Rome Italy
Mr. Allan DIXON	European Legal Counsel Business Software, Alliance United States
M. Robert DIETCHI	Office Fédéral de Communications (OFCOM) Département fédéral des transports, des communications et de l'énergie Switzerland
Mr. Josef DIETL	Electronic Commerce Specialist W3C - INRIA France

Mr. Bohumil DOLEJŠÍ	Counsellor, Permanent Delegation of the Czech Republic to the OECD
Mr. John DRYDEN	Head of ICCP Division Directorate for Science, Technology and Industry OECD
Mr. Christian DUVERNOY	Wilmer Cutler and Pickering Belgium
Mr. Stefan ENGEL-FLECHSIG	Senior Principal Federal Ministry of Research and Technology Germany
Mr. Deniz ERÖCAL	Manager Business and Industry Advisory Committee to the OECD
Mme Isabelle FALQUE-PIERROTIN	Maître des requêtes au Conseil d'Etat France
M. Pierre FIORINI	DGSI/Serics France
Mr. Peter FLEISCHER	Corporate Attorney Microsoft Europe France
Mr. Peter FORD	First Assistant Secretary Information Law Branch of the Australian Attorney-General's Department Australia
Ms. Joëlle FREUNDLICH	Cegetel France
Mr. Sean GADDIS	Manager of Marketing Technology Netscape Communications Corporation United States
Mr. Luigi GAMBARDELLA	Direzione Affari Generali Istitvzionali e Regolamentari Olivetti Italy
Mr. Hansjürgen GARSTKA	Data Protection Commissionner Germany

M. Dominique GEORGE	Managing Director G.P. Morgan France
Ms. Mona GOLDSTEIN	President Wunderman Cato Johnson Canada
Mme Suzanne GROSSMANN	Office Fédéral des Affaires Economiques Extérieures Département fédéral de l'économie Switzerland
Ms. Anne Line GRSSTAD	Special Adviser Ministry of Justice and Police Civil Department Norway
Mr. Yonca GUNDUZ-OZCERI	Permanent Delegation of Turkey to the OECD
Mr. Lauren HALL	Chief Technologist Software Publishers Association United States
Dr. Péter HANÀK	Director General National Committee for Technological Development Hungary
Mr. Jostein HÅØY	Research Department IT policy coordination unit Ministry of Trade and Industry Norway
Mr. Yasuo HASEBE	Professor of Law Tokyo University Japan
Mr. Johan HELSINGIUS	Director of Product Development and Marketing EUNet International BV Netherlands
Mr. David HECNAR	Director, International Policy Canadian Council for International Business Canada
Mr. Nigel HICKSON	Head, Information Security Policy Group Department of Trade and Industry United Kingdom

Ms Heidi HIJIKATA	Director, Software Division, International Trade Administration U.S. Department of Commerce United States
Mr. Masao HORIBE	Professor of Law Faculty of Law Hitotsubashi University Japan
Mr. Zoltàn HORVÀTH	Energy Advisor Permanent Delegation of Hungary to the OECD
Ms. Axelle HOVINE	SJTIC France
Mr. P.J. HUSTINX	Data Protection Registrar Netherlands
Ms. Marie-Therese HUPPERTZ	Corporate Attorney Microsoft Belguim
Mr. Klaus-Dietmar JACOBY	Counsellor Science, Technology, Information, and Nuclear Energy Permanent Delegation of Germany to the OECD
Mr. Eivind JAHREN	Ministry of Trade and Industry Norway
M. Michel JAOUL	Président d'Honneur Fondation franco-américaine France
Ms. Hiroko KAMATA	Principal Administrator ICCP Division Directorate for Science, Technology and Industry OECD
Mr. Keiichi KAWAKAMI	First Secretary Permanent Delegation of Japan to the OECD
Ms. Joanna KEMPKERS	Second Secretary Permanent Delegation of New Zealand to the OECD

Mr. Michael KEPLINGER	Senior Councellor US Patent and Trade Office United States
Mr. Mannuel KOHNSTAMM	Vice President Public Affairs Time Warner Europe Belguim
Mr. Masaaki KOBASHI	Director Office of Information Technology Security Policy Machinery and Information Industries Bureau Ministry of International Trade and Industry Japan
Mr. Manuel KOHNSTAMM	Vice President, Public Affairs Time Warner Europe Belgium
Mr. Alexey KOZHEMYAKOV	Direction des Affaires juridiques Conseil de l'Europe France
Dr. Katharina KOPP	Senior Policy Analyst Center for Media Education United States
Ms. Waltraut KOTSCHY	Chancellerie Fédérale Austria
Mr. Christopher KUNER	Gleiss Lutz Hootz Hirsch Germany
Ms. Laurie LABUDA	Consultant ICCP Division Directorate for Science, Technology and Industry OECD
Mme Isabelle LAFONTAINE	DPT France
Mr. Stefano LAMBORGHINI	Segretario Generale AIIP Associazione Italiana Internet Providers Italy
Ms. Laurentia LARACY	Longworth Associates Level 7, Royal Sun Alliance Building United States

Ms. Margrit LEEMHUIS	Permanent Delegation of Netherlands to the OECD
Mr. Philippe LEMOINE	Vice Président Directeur Général du Groupe Galeries Lafayette
Mr. Yves LE ROUX	DIGITAL Equipment
Mr. Alexandros LEVENTIDIS	Head, Directorate for Operational Infrastructure, Ministry of Internal Affairs, Public Management and Decentralisation Greece
Mr. Erich LINKE	Principal Administrator ICCP Division Directorate for Science, Technology and Industry OECD
Mr. Evripidis LOUKIS	Staff expert Service for the Development of Informatics of the Ministry of Internal Affairs, Public Management and Decentralisation Greece
M. Jacques LOUVIER	SJTIC France
Dr. Willliam H. LOWRANCE	Consultant in Health Policy Switzerland
Dr. Steven LUCAS	Vice President, Matchlogic United States
Ms. Linda LUSBY	Canada
Ms. Elizabeth LYNCH	Consultant ICCP Division Directorate for Science, Technology and Industry OECD
Mme Annie MARI	Ministère des affaires étrangères France
M. Hubert MARTY-VRAYANCE	SCSSI France

Mr. Michael McCABE	Director for APEC and OECD International Communications and Information Policy Bureau of Economic and Business Affairs Department of State United States
Ms. Helen McDONALD	Canada
Mr. Willian McFADDEN	Senior Policy Advisor International Finance and Monetary Policy U.S. Department of Treasury United States
Ms. Kate McGEE	Vice President, Corporate Affairs Oracle United States
Mr. David MEDINE	Head Credit Practices Division Federal Trade Commission United States
Dr. Alicia MIGNONE	Scientific Attaché Permanent Delegation of Italy to OECD
Mr. Kazuhiro MIHASHI	Assistant Manager KDD France
Mr. Christopher J. MILLARD	Clifford Chance United Kingdom
Ms. Harris MILLER	President Information Technology Association of America United States
Ms. Suzanne MORIN	Canada
Ms. Evangelia MITROU	Advisor to the Prime Minister Greece
M. Jean-Marc MOSCONI	Délégué-Général de l'Association Mercatel
Lord Williams of MOSTYN	Parliamentary Under-Secretary of State Home Office United Kingdom

Ms. Deirdre MULLIGAN	Staff Counsel Center for Democracy and Technology (CDT) United States
Mr. Jim MURRAY	Director Bureau Européen des Unions de Consommateurs BEUC/395/97 Belgium
Mr. Roger NEEDHAM	Pro-Vice-Chancellor & Professor of Computer Systems University of Cambridge United Kingdom
Mr. Risaburo NEZU	Director Directorate for Science, Technology and Industry OECD
Mr. Tetsuya NISHIDA	Director General Research Department The Center for Financial Industry Information Systems (FISC) Japan
Mr. Pekka NURMI	Director at Ministry of Justice and Chairman of Data Protection Board Finland
Mr. Michael OBORNE	Deputy Director Directorate for Science, Technology and Industry OECD
Mr. Nagaaki OYAMA	Professor Tokyo Institute of Technology Japan
M. Michel PACHE	Division politique V Département fédéral des affaires étrangères Switzerland
Dr. Mària PÀNCZÉL	Second Counsellor Embassy of Hungary France

Ms. Inci PEKGULEC-APAYDIN	Head of Division General Directorate of Economic Research UnderSecretariat of Treasury Turkey
Ms. Stephanie PERRIN	Special Policy Advisor Information Policy Industry Canada Canada
Ms. Teresa PETERS	Administrator ICCP Division Directorate for Science, Technology and Industry OECD
Mr. Roger PETTERSSON	Ministry of Justice Sweden
Dr. Iimari PIETARINEN	Finance Counsellor Ministry of Finance Finland
Mme Charlotte-Marie PITRAT	Commissaire du Gouvernement auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL) France
Mr. Ronald L. PLESSER	Partner Piper & Marbury LLP United States
Mr. Bill POULOS	Director, Electronic Commerce Policy EDS Office of Government Affairs United States
Mr. Charles PRESCOTT	Chairman of the USCIB Working Group on Privacy and Data Protection United States Council for International Business United States
Mr. Ivan PROCHÀZKA	Director Office for the State Information System Czech Republic
Mr. Bob PUBLICOVER	Canada

M. Philippe RAILLON	ART France
Mr. Bong-Ha RHA	First Secretary Permanent Delegation of Korea to the OECD
M. Luc RIFFLET	Conseiller Délegation Permenante de la Belgique auprès de l'OCDE
Prof. Stefano RODOTA	Garante per la Tutela dei Dati Personali Italy
Mr. Marc ROTENBERG	Director Electronic Privacy Information Centre (EPIC) United States
Mr. John ROTHCHILD	Federal Trade Commission United States
Ms. Heather ROWE	ICC Lovell White Durrant United Kingdom
M. Joseph ROYEN	Conseiller adjoint à l'administration de la politique commerciale Ministère des Affaires économiques Belgium
Mr. Hiroaki SAITO	Deputy Director Tariff Division, Telecommunications Business Department, Telecommunications Bureau Ministry of Posts and Telecommunications Japan
Mr. Kouichi SAKUSA	Electronic Commerce Promotion Council of Japan (ECOM) Japan
Counsellor Carlo SARZANA	Tribunale Penale di Roma Italy
Ms. Alden SCHACHER	Manager Government affairs, the Dun and Bradstreet Corporation United States

Mr. Herman SCHIPPER	International and European affairs Netherlands Standardisation Institute Netherlands
Ms. Susan SCOTT	Executive Director TRUSTe United States
Mr. Mitsugu SEKIMOTO	Director of Research and Information Security of Japan Information Processiong Development Center (JIPDEC) Japan
Mr. Dimitris SERRELIS	First Secretary, Permanent Delegation of Greece to the OECD
Ms. Joanna SHELTON	Deputy Secretary-General OECD
Mr. Milos ŠNYTRE	Vice-president Office for the State Information System Czech Republic
Dr. Alain SOMMER	Co-Chair of the BIAC Working Group on Health Care Policy France
M. SORNAT	Ministère de la Défense France
Mr. John STEPHENS	European Affairs Adviser Reuters Ltd.
M. Pierre STRUMELLE	Conseiller adjoint, Ministère des Affaires Economiques Administration de l'Information économique Rue de l'Industrie Belgium
Mr. Richard M. SAWCHUK	Senior Advisor, Public Policy & Government Affairs TELUS Corporation United States
Mr. Jun SOFUE	Senior Vice President Strategic Planning Dynastrat, Inc. United States

Mr. Peter P. SWIRE	Associate Professor Ohio State University College of Law United States
Mr. Iván SZÉKELY	Chief Counsellor Office of the Parliament Commissioner for Data Protection and Freedom of Information Hungary
Ms. Jennifer TALLARICO	Electronic Commerce Task Force International Trade Administration Department of Commerce United States
Mr. Alastair C. TEMPEST	Director General Public Affairs & Self-Regulation International Federation of Direct Marketing Federation of Direct Marketing Belgium
M. THIERCELIN	SCSSI France
Mr. Mozelle W. THOMPSON	Commissioner Federal Trade Commission United States
M. Kosmas TSIRAKTSOPULOS	Secrétariat du Préposé à la protection des données Département fédéral de justice et police Switzerland
Ms. Anne TROYE-WALKER	DG III - Industry European Commission Belgium
Ms. Anne-Marie TURCOTTE	Canada
Mr. Christiaan VAN DER VALK	Policy Manager Telecoms and Electronic Commerce Coordinator of Commission Projects ICC
Mr. J. Robert VASTINE	President Coalition of Service Industries United States
Mr. L. VERHEY	Ministry of Justice Netherlands

M. Philippe VERNET	Cullen International SA Belgium
Dr. Armgard VON REDEN	Manager, Government Programmes IBM Europe, Middle East, Africa Belguim
Mr. Reid WATTS	National Cash Register - NCR United States
Mr. Kernaghan WEBB	Canada
Ms. Barbara WELLBERY	Special Counsel for Electronic Commerce Department of Commerce United States
Mr. William R. WHITEHURST	Director of Data Security Programs IBM Corporation United States
Mr. Steingrim WOLLAN	Advokatkollegiet A/S Norway
Mr. Stephen WOOLLEY	Partner Privacy and Information Systems Risk Management Price Waterhouse Australia
Mr. Yuji YAMADORI	Director, Information Security Office Japan Information Processiong Development Center (JIPDEC) Japan
Mr. Mabito YOSHIDA	First Secretary Permanent Delegation of Japan to the OECD
Mr. Ioannis ZANNETOPOULOS	Head EDP Directorate of the Ministry of Internal Affairs, Public Management and Decentralisation Greece
Mr. Vasilis ZORKADIS	Staff expert, Ministry of Internal Affairs, Public Management and Decentralisation Greece