ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES

OECD

Policies for Information Security & Privacy

…Internet Economy – Data Controller – Virus – Vulnerabilities – Passwords Sensor Networks – Cross-Border Enforcement Co-Operation – Identity Management…

Privacy & Data Protection – Security of Information Systems & Networks – Critical Information Infrastructures – Electronic Authentication Cryptography – RFID – Spam

…Transborder Flows – Personal Data – Cloud Computing – Cryptography Social Networks – Biometrics – Botnets – Phishing – PKI – Malware…

2009

OECD Policies for Information Security & Privacy

2009

Table of Contents

Preface

OECD's activities to generate trust in information and communications technologies (ICTs) pre-date the growth of the Internet. In the area of privacy, work began in the seventies arising out of concerns about the power of computing allied to the growth of telecommunications that might prejudice the individuals' personal information and have disruptive consequences for international data flows. At that time, the continuous exchange of information around the globe was still far off.

In the late 1990s, concerns focused on the Internet becoming the platform for e-commerce and the need for individuals and business to operate in a secure, predictable, and fair environment. The 1998 Ottawa Ministerial Conference on Electronic Commerce highlighted the need for bridges between different national approaches to enhance privacy protection across borders. In parallel, information security issues received heightened attention. OECD work between 1998 and 2007 elevated the importance of information security and privacy to the continued growth of the information society.

With the Internet becoming a critical information infrastructure supporting all kinds of economic and social activity, the 2008 Seoul Ministerial on the Future of the Internet Economy put an even greater emphasis on the need to strengthen confidence and security. While recognising the need for continued implementation of current policies and practices for information security and privacy, Ministers called for an assessment of the application of OECD instruments in light of changing technologies, markets and user behaviour and the growing importance of digital identities.

On the eve of the 30th Anniversary of the Privacy Guidelines, this compendium gathers current OECD Policies for Information Security and Privacy developed between 1980 and 2008 by the OECD Working Party on Information Security and Privacy (WPISP) and its parent body, the Committee for Information, Computer and Communications Policy. It includes Ministerial Declarations, Council Recommendations and Policy and Practical Guidance. Other work by the WPISP is available at: www.oecd.org/sti/security-privacy

OECD MINISTERIAL MEETING ON THE FUTURE OF THE INTERNET ECONOMY

(SEOUL, KOREA, 17-18 JUNE 2008)

DECLARATION FOR THE FUTURE OF THE INTERNET ECONOMY (THE SEOUL DECLARATION) (2008)

WE, the Ministers and representatives of Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Egypt, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, India, Indonesia, Ireland, Israel, Italy, Japan, Korea, Latvia, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, Senegal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom, the United States of America and the European Community, assembled in Seoul, Korea, on 17 and 18 June 2008 to discuss the future of the Internet Economy.

WE STATE our common desire to promote the Internet Economy and stimulate sustainable economic growth and prosperity by means of policy and regulatory environments that support innovation, investment, and competition in the information and communications technology (ICT) sector. We will work with the private sector, civil society and the Internet community to secure the ICT networks that underpin the Internet Economy as well as to take measures to protect the users of the Internet Economy, including the necessary cross-border co-operation.

WE ARE DETERMINED to work together to promote ubiquitous access to ICT networks and services enabling widespread participation in the Internet Economy. The further expansion of the Internet Economy will bolster the free flow of information, freedom of expression, and protection of individual liberties, as critical components of a democratic society and cultural diversity. We will also work to use the tools of the Internet Economy to address global challenges, such as climate change. In moving forward, we recognise the significant foundation that the 1998 *OECD Ministerial Conference on Electronic Commerce* provided to the nascent Internet Economy and take note of the outcomes of the 2003 and 2005 *World Summit on the Information Society* (WSIS).

WE SHARE a vision that the Internet Economy, which covers the full range of our economic, social and cultural activities supported by the Internet and related information and communications technologies (ICT), will strengthen our capacity to improve the quality of life for all our citizens by:

- Providing new opportunities for employment, productivity, education, health and public services as well as addressing environmental and demographic concerns.
- Acting as a key driver for the creation of enterprises and communities and stimulating closer global co-operation.
- Enabling new forms of civic engagement and participation that promote diversity of opinions and enhance transparency, accountability, privacy and trust.
- Empowering consumers and users in online transactions and exchanges.
- Reinforcing a culture of security which applies to information systems and networks, and their users.
- Developing an increasingly important platform for research, international science co-operation, creativity and innovation in many different sectors.
- Creating opportunities for new economic and social activities, applications and services through ubiquitous and seamless access to communication and information networks.
- Promoting a global information society based on fast, secure and ubiquitous networks which connect billions of people, machines and objects.

WE AGREE that our challenges are, through an appropriate balance of laws, policies, self-regulation, and consumer empowerment, to:

- Expand Internet access and use worldwide.
- Promote Internet-based innovation, competition, and user choice.
- Secure critical information infrastructures, and respond to new threats.
- Ensure the protection of personal information in the online environment.
- Ensure respect for intellectual property rights.
- Ensure a trusted Internet-based environment which offers protection to individuals, especially minors and other vulnerable groups.
- Promote the secure and responsible use of the Internet that respects international social and ethical norms and that increases transparency and accountability.
- Create a market-friendly environment for convergence that encourages infrastructure investment, higher levels of connectivity and innovative services and applications.

WE DECLARE that, to contribute to the development of the Internet Economy, we will:

a) Facilitate the convergence of digital networks, devices, applications and services, through policies that:

- Establish a regulatory environment that assures a level playing field for competition.
- Uphold the open, decentralised and dynamic nature of the Internet and the development of technical standards that enable its ongoing expansion and contribute to innovation, interoperability, participation and ease of access.
- Stimulate investment and competition in the development of high capacity information and communication infrastructures and the delivery of Internet-enabled services within and across borders.
- Ensure that broadband networks and services are developed to attain the greatest practical national coverage and use.
- Encourage a more efficient use of the radio frequency spectrum to facilitate access to the Internet and the introduction of new and innovative services, while taking into account public interest objectives.
- Encourage the adoption of the new version of the Internet protocol (IPv6), in particular through its timely adoption by governments as well as large private sector users of IPv4 addresses, in view of the ongoing IPv4 depletion.
- Ensure that convergence benefits consumers and businesses, providing them choices with respect to connectivity, access and use of Internet applications, terminal devices and content, as well as clear and accurate information about the quality and costs of services.

b) Foster creativity in the development, use and application of the Internet, through policies that:

- Maintain an open environment that supports the free flow of information, research, innovation, entrepreneurship and business transformation.
- Make public sector information and content, including scientific data, and works of cultural heritage more widely accessible in digital format.
- Encourage basic and applied research on the Internet and related ICTs.
- Encourage universities, governments, public research, users and business to work together in collaborative innovation networks and to make use of shared experimental Internet facilities.

- Combine efforts to combat digital piracy with innovative approaches which provide creators and rights holders with incentives to create and disseminate works in a manner that is beneficial to creators, users and our economies as a whole.
- Encourage new collaborative Internet-based models and social networks for the creation, distribution and use of digital content that fully recognise the rights of creators and the interests of users.
- Strengthen the development of human resources to take full advantage of the Internet and related ICTs, and further develop ICT skills and digital and media literacy.

c) Strengthen confidence and security, through policies that:

- Protect critical information infrastructures at national and international levels from security risks.
- Strengthen the resilience and security of the Internet and related networked ICT systems and devices to meet the increasing demands and needs of our economies and societies.
- Reduce malicious activity online through reinforced national and international co-operation among all stakeholder communities in their steps for effective prevention, protection, information sharing, response, business continuity and recovery.
- Ensure the protection of digital identities and personal data as well as the privacy of individuals online.
- Ensure that consumers benefit from effective consumer protection regimes and from meaningful access to fair, easy-to-use, and effective dispute resolution mechanisms, including appropriate redress for economic harm resulting from online transactions.
- Encourage collaboration between governments, the private sector, civil society and the Internet technical community in building an understanding of the impact of the Internet on minors in order to enhance their protection and support when using the Internet.
- Promote research to address emerging security threats.

d) Ensure that the Internet Economy is truly global, through policies that:

- Support expanded access to the Internet and related ICTs, especially for people in developing countries.
- Recognise the potential of the Internet and related technologies to provide enhanced services to people with disabilities and special needs.

- Recognise the importance of a competitive environment for the successful growth of the Internet Economy and the opportunities this can bring for development, particularly for people and regions with the most limited economic means.
- Promote use of Internet and related ICT networks by all communities as well as the creation of local content and multi-language translations to improve economic and social inclusion of people with different capabilities, education, and skills, and to preserve cultural and linguistic diversity.
- Facilitate the introduction of internationalised domain names (IDNs) while ensuring the integrity and stability of the Internet.
- Increase cross-border co-operation of governments and enforcement authorities in the areas of improving cyber-security, combating spam, as well as protecting privacy, consumers and minors.
- Harness the potential of the Internet to tackle global challenges such as improving energy efficiency and addressing climate change.

WE WELCOME the OECD report *Shaping Policies for the Future of the Internet Economy*, **RECOGNISE** its importance and **COMMEND** its consideration by OECD Member countries and non-member economies in developing their policies to support the Internet Economy.

WE COMMIT to working collectively with all stakeholders towards implementing and reviewing, as appropriate, the understanding that we have achieved in this Declaration in order to maintain its relevance to future challenges and opportunities confronting our economies and societies.

WE INVITE the OECD to further the objectives set out in this Declaration, through multi-stakeholder co-operation, by:

- Analysing the future development of the Internet Economy, namely: i) the important role and contribution of the Internet and related ICTs as a driver of innovation, productivity and economic growth; ii) the economic, social and cultural impacts of emerging Internet technologies, applications and services, including virtual worlds, sensor-based networks and social networking platforms.
- Based on this analysis, developing and promoting policy and regulatory principles, guidelines, other instruments and best practices for the future development of the Internet Economy.
- Researching the impacts of Internet and related ICTs in addressing climate change and improving energy efficiency.
- Examining the role of various actors, including intermediaries, in meeting policy goals for the Internet Economy in areas such as

combating threats to the security and stability of the Internet, enabling cross-border exchange, and broadening access to information;

- Improving statistical systems to measure the changing access and use of the Internet and related ICT networks by citizens, businesses and institutions in order to provide reliable measures of evolving uses and the impact of the Internet on economic performance and social well-being.
- Assessing the application of current OECD instruments addressing consumer protection and empowerment, privacy and security in light of changing technologies, markets and user behaviour and the growing importance of digital identities.
- Recommending the development of OECD instruments that provide guidance in the formulation of policies for the development and use of converged communication networks.
- Continuing multidisciplinary work looking at the challenges and good practices of e-government and public sector transformation.
- Supporting measures and mechanisms to implement more effective cross-border co-operation
- Conveying this Declaration and the OECD report Shaping policies for the Future of the Internet Economy to all relevant international bodies and organisations, including G8, the ITU, WIPO, and UNESCO.
- Reinforcing co-operative relationships and mutually beneficial collaboration with the Asia-Pacific Economic Co-operation, the Council of Europe as well as the Internet technical community, the private sector and civil society within fora such as the Internet Governance Forum.
- Reviewing within three years of its adoption, and thereafter as appropriate, the progress made at national and international levels in light of this Declaration.

PRIVACY

RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980)

THE COUNCIL,

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

RECOGNISING:

- That, although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information; that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices.
- That transborder flows of personal data contribute to economic and social development.
- That domestic legislation concerning privacy protection and trans-border flows of personal data may hinder such transborder flows.

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

RECOMMENDS:

1. That Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines contained in the Annex to this Recommendation, which is an integral part thereof.
2. That Member countries endeavour to remove, or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data;
3. That Member countries co-operate in the implementation of the Guidelines set forth in the Annex.
4. That Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines.

Annex
Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data

Part one: general

Definitions

1. For the purposes of these Guidelines:

a. "Data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf.
b. "Personal data" means any information relating to an identified or identifiable individual (data subject).
c. "Transborder flows of personal data" means movements of personal data across national borders.

Scope of guidelines

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

3. These Guidelines should not be interpreted as preventing:

1. The application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated:
   a. The exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or
   b. The application of the Guidelines only to automatic processing of personal data.

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

a. As few as possible, and
b. Made known to the public.

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

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

Part two: basic principles of national application

Collection limitation principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data quality principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose specification principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use limitation principle

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

a. With the consent of the data subject; or

b. By the authority of law.

Security safeguards principle

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

Openness principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be

readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual participation principle

13. An individual should have the right:

a. To obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him.

b. To have communicated to him, data relating to him:

- Within a reasonable time.
- At a charge, if any, that is not excessive.
- In a reasonable manner; and
- In a form that is readily intelligible to him.

c. To be given reasons if a request made under sub-paragraphs a) and b) is denied, and to be able to challenge such denial; and

d. To challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability principle

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

Part three: basic principles of international application: free flow and legitimate restrictions

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

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

17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

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

Part four: national implementation

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

a. Adopt appropriate domestic legislation.

b. Encourage and support self-regulation, whether in the form of codes of conduct or otherwise.

c. Provide for reasonable means for individuals to exercise their rights.

d. Provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and

e. Ensure that there is no unfair discrimination against data subjects.

Part five: international co-operation

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

21. Member countries should establish procedures to facilitate:

a. Information exchange related to these Guidelines, and

b. Mutual assistance in the procedural and investigative matters involved.

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

Explanatory Memorandum

Introduction

A feature of OECD Member countries over the past decade has been the development of laws for the protection of privacy. These laws have tended to assume different forms in different countries, and in many countries are still in the process of being developed. The disparities in legislation may create obstacles to the free flow of information between countries. Such flows have greatly increased in recent years and are bound to continue to grow as a result of the introduction of new computer and communication technology.

The OECD, which had been active in this field for some years past, decided to address the problems of diverging national legislation and in 1978 instructed a Group of Experts to develop Guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, in order to facilitate the harmonization of national legislation. The Group has now completed its work.

The Guidelines are broad in nature and reflect the debate and legislative work which has been going on for several years in Member countries. The Expert Group which prepared the Guidelines has considered it essential to issue an accompanying Explanatory Memorandum. Its purpose is to explain and elaborate the Guidelines and the basic problems of protection of privacy and individual liberties. It draws attention to key issues that have emerged in the discussion of the Guidelines and spells out the reasons for the choice of particular solutions.

The first part of the Memorandum provides general background information on the area of concern as perceived in Member countries. It explains the need for international action and summarises the work carried out so far by the OECD and certain other international organisations. It concludes with a list of the main problems encountered by the Expert Group in its work.

Part Two has two subsections. The first contains comments on certain general features of the Guidelines, the second detailed comments on individual paragraphs.

This Memorandum is an information document, prepared to explain and describe generally the work of the Expert Group. It is subordinate to the

Guidelines themselves. It cannot vary the meaning of the Guidelines but is supplied to help in their interpretation and application.

I. General background

The Problems

1. The 1970s may be described as a period of intensified investigative and legislative activities concerning the protection of privacy with respect to the collection and use of personal data. Numerous official reports show that the problems are taken seriously at the political level and at the same time that the task of balancing opposing interests is delicate and unlikely to be accomplished once and for all. Public interest has tended to focus on the risks and implications associated with the computerised processing of personal data and some countries have chosen to enact statutes which deal exclusively with computers and computer-supported activities. Other countries have preferred a more general approach to privacy protection issues irrespective of the particular data processing technology involved.

2. The remedies under discussion are principally safeguards for the individual which will prevent an invasion of privacy in the classical sense, *i.e.* abuse or disclosure of intimate personal data; but other, more or less closely related needs for protection have become apparent. Obligations of record-keepers to inform the general public about activities concerned with the processing of data, and rights of data subjects to have data relating to them supplemented or amended, are two random examples. Generally speaking, there has been a tendency to broaden the traditional concept of privacy ("the right to be left alone") and to identify a more complex synthesis of interests which can perhaps more correctly be termed privacy and individual liberties.

3. As far as the legal problems of automatic data processing (ADP) are concerned, the protection of privacy and individual liberties constitutes perhaps the most widely debated aspect. Among the reasons for such widespread concern are the ubiquitous use of computers for the processing of personal data, vastly expanded possibilities of storing, comparing, linking, selecting and accessing personal data, and the combination of computers and telecommunications technology which may place personal data simultaneously at the disposal of thousands of users at geographically dispersed locations and enables the pooling of data and the creation of complex national and international data networks. Certain problems require particularly urgent attention, *e.g.* those relating to emerging international data networks, and to the need of balancing competing interests of privacy on the one hand and freedom of information on the other, in order to allow a full exploitation of the potentialities of modern data processing technologies in so far as this is desirable.

Activities at national level

4. Of the OECD Member countries more than one-third have so far enacted one or several laws which, among other things, are intended to protect individuals against abuse of data relating to them and to give them the right of access to data with a view to checking their accuracy and appropriateness. In federal states, laws of this kind may be found both at the national and at the state or provincial level. Such laws are referred to differently in different countries. Thus, it is common practice in continental Europe to talk about "data laws" or "data protection laws" (lois sur la protection des données), whereas in English speaking countries they are usually known as "privacy protection laws". Most of the statutes were enacted after 1973 and the present period may be described as one of continued or even widened legislative activity. Countries which already have statutes in force are turning to new areas of protection or are engaged in revising or complementing existing statutes. Several other countries are entering the area and have bills pending or are studying the problems with a view to preparing legislation. These national efforts, and not least the extensive reports and research papers prepared by public committees or similar bodies, help to clarify the problems and the advantages and implications of various solutions. At the present stage, they provide a solid basis for international action.

5. The approaches to protection of privacy and individual liberties adopted by the various countries have many common features. Thus, it is possible to identify certain basic interests or values which are commonly considered to be elementary components of the area of protection. Some core principles of this type are: setting limits to the collection of personal data in accordance with the objectives of the data collector and similar criteria; restricting the usage of data to conform with openly specified purposes; creating facilities for individuals to learn of the existence and contents of data and have data corrected; and the identification of parties who are responsible for compliance with the relevant privacy protection rules and decisions. Generally speaking, statutes to protect privacy and individual liberties in relation to personal data attempt to cover the successive stages of the cycle, beginning with the initial collection of data and ending with erasure or similar measures, and to ensure to the greatest possible extent individual awareness, participation and control.

6. Differences between national approaches as apparent at present in laws, bills or proposals for legislation, refer to aspects such as the scope of legislation, the emphasis placed on different elements of protection, the detailed implementation of the broad principles indicated above, and the machinery of enforcement. Thus, opinions vary with respect to licensing requirements and control mechanisms in the form of special supervisory bodies ("data inspection authorities"). Categories of sensitive data are defined differently, the means of ensuring openness and individual participation vary, to give just a few instances. Of course, existing

traditional differences between legal systems are a cause of disparity, both with respect to legislative approaches and the detailed formulation of the regulatory framework for personal data protection.

International aspects of privacy and data banks

7. For a number of reasons the problems of developing safeguards for the individual in respect of the handling of personal data cannot be solved exclusively at the national level. The tremendous increase in data flows across national borders and the creation of international data banks (collections of data intended for retrieval and other purposes) have highlighted the need for concerted national action and at the same time support arguments in favour of free flows of information which must often be balanced against requirements for data protection and for restrictions on their collection, processing and dissemination.

8. One basic concern at the international level is for consensus on the fundamental principles on which protection of the individual must be based. Such a consensus would obviate or diminish reasons for regulating the export of data and facilitate resolving problems of conflict of laws. Moreover, it could constitute a first step towards the development of more detailed, binding international agreements.

9. There are other reasons why the regulation of the processing of personal data should be considered in an international context: the principles involved concern values which many nations are anxious to uphold and see generally accepted; they may help to save costs in international data traffic; countries have a common interest in preventing the creation of locations where national regulations on data processing can easily be circumvented; indeed, in view of the international mobility of people, goods and commercial and scientific activities, commonly accepted practices with regard to the processing of data may be advantageous even where no transborder data traffic is directly involved.

Relevant international activities

10. There are several international agreements on various aspects of telecommunications which, while facilitating relations and cooperation between countries, recognise the sovereign right of each country to regulate its own telecommunications (The International Telecommunications Convention of 1973). The protection of computer data and programmes has been investigated by, among others, the World Intellectual Property Organisation which has developed draft model provisions for national laws on the protection of computer software. Specialised agreements aiming at informational co-operation may be found in a number of areas, such as law enforcement, health services, statistics and judicial services (*e.g.* with regard to the taking of evidence).

11. A number of international agreements deal in a more general way with the issues which are at present under discussion, *viz.* the protection of privacy and the free dissemination of information. They include the European Convention on Human Rights of 4th November, 1950 and the International Covenant on Civil and Political Rights (United Nations, 19th December, 1966).

12. However, in view of the inadequacy of existing international instruments relating to the processing of data and individual rights, a number of international organisations have carried out detailed studies of the problems involved in order to find more satisfactory solutions.

13. In 1973 and 1974 the Committee of Ministers of the Council of Europe adopted two resolutions concerning the protection of the privacy of individuals vis-à-vis electronic data banks in the private and public sectors respectively. Both resolutions recommend that the governments of the Member states of the Council of Europe take steps to give effect to a number of basic principles of protection relating to the obtaining of data, the quality of data, and the rights of individuals to be informed about data and data processing activities.

14. Subsequently the Council of Europe, on the instructions of its Committee of Ministers, began to prepare an international Convention on privacy protection in relation to data processing abroad and transfrontier data processing. It also initiated work on model regulations for medical data banks and rules of conduct for data processing professionals. According to present plans, work on the Convention is to be completed before 30th June, 1980. The draft Convention seeks to establish basic principles of data protection to be enforced by Member countries, to reduce restrictions on transborder data flows between the Contracting Parties on the basis of reciprocity, to bring about co-operation between national data protection authorities, and to set up a Consultative Committee for the application and continuing development of the convention.

15. The European Community has carried out studies concerning the problems of harmonization of national legislations within the Community in relation to transborder data flows and possible distortions of competition, the problems of data security and confidentiality, and the nature of transborder data flows. A sub-committee of the European Parliament held a public hearing on data processing and the rights of the individual in early 1978. Its work has resulted in a report to the European Parliament in Spring 1979. The report, which was adopted by the European Parliament in May 1979, contains a resolution on the protection of the rights of the individual in the face of technical developments in data processing.

Activities of the OECD

16. The OECD programme on transborder data flows derives from computer utilisation studies in the public sector which were initiated in 1969. A Group of Experts, the Data Bank Panel, analysed and studied different aspects of the privacy issue, *e.g.* in relation to digital information, public administration, transborder data flows, and policy implications in general. In order to obtain evidence on the nature of the problems, the Data Bank Panel organised a Symposium in Vienna in 1977 which provided opinions and experience from a diversity of interests, including government, industry, users of international data communication networks, processing services, and interested intergovernmental organisations.

17. A number of guiding principles were elaborated in a general framework for possible international action. These principles recognised:

a. The need for generally continuous and uninterrupted flows of information between countries.

b. The legitimate interests of countries in preventing transfers of data which are dangerous to their security or contrary to their laws on public order and decency or which violate the rights of their citizens.

c. The economic value of information and the importance of protecting "data trade" by accepted rules of fair competition.

d. The needs for security safeguards to minimise violations of proprietary data and misuse of personal information, and

e. The significance of a commitment of countries to a set of core principles for the protection of personal information.

18. Early in 1978 a new ad hoc Group of Experts on Transborder Data Barriers and Privacy Protection was set up within the OECD which was instructed to develop guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, in order to facilitate a harmonization of national legislations, without this precluding at a later date the establishment of an International Convention. This work was to be carried out in close co-operation with the Council of Europe and the European Community and to be completed by 1st July, 1979.

19. The Expert Group, under the chairmanship of the Honourable Mr. Justice Kirby, Australia, and with the assistance of Dr. Peter Seipel (Consultant), produced several drafts and discussed various reports containing, for instance, comparative analyses of different approaches to legislation in this field. It was particularly concerned with a number of key issues set out below.

a. The specific, sensitive facts issue

The question arises as to whether the Guidelines should be of a general nature or whether they should be structured to deal with different types of data or activities (*e.g.* credit reporting). Indeed, it is probably not possible to identify a set of data which are universally regarded as being sensitive.

b. The ADP issue

The argument that ADP is the main cause for concern is doubtful and, indeed, contested.

c. The legal persons issue

Some, but by no means all, national laws protect data relating to legal persons in a similar manner to data related to physical persons.

d. The remedies and sanctions issue

The approaches to control mechanisms vary considerably; for instance, schemes involving supervision and licensing by specially constituted authorities might be compared to schemes involving voluntary compliance by record-keepers and reliance on traditional judicial remedies in the Courts.

e. The basic machinery or implementation issue

The choice of core principles and their appropriate level of detail presents difficulties. For instance, the extent to which data security questions (protection of data against unauthorised interference, fire, and similar occurrences) should be regarded as part of the privacy protection complex is debatable; opinions may differ with regard to time limits for the retention, or requirements for the erasure, of data, and the same applies to requirements that data be relevant to specific purposes. In particular, it is difficult to draw a clear dividing line between the level of basic principles or objectives and lower level "machinery" questions which should be left to domestic implementation.

f. The choice of law issue

The problems of choice of jurisdiction, choice of applicable law and recognition of foreign judgements have proved to be complex in the context of transborder data flows. The question arises, however, whether and to what extent it should be attempted at this stage to put forward solutions in Guidelines of a non-binding nature.

g. The exceptions issue

Similarly, opinions may vary on the question of exceptions. Are they required at all? If so, should particular categories of exceptions be provided for or should general limits to exceptions be formulated?

h. The bias issue

Finally, there is an inherent conflict between the protection and the free transborder flow of personal data. Emphasis may be placed on one or the other, and interests in privacy protection may be difficult to distinguish from other interests relating to trade, culture, national sovereignty, and so forth.

20. During its work the Expert Group has maintained close contacts with corresponding organs of the Council of Europe. Every effort has been made to avoid unnecessary differences between the texts produced by the two organisations; thus, the set of basic principles of protection are in many respects similar. On the other hand, a number of differences do occur. To begin with, the OECD Guidelines are not legally binding, whereas the Council of Europe has produced a Convention which, if adopted, would be legally binding among those countries which ratify it. This in turn means that the question of exceptions has been dealt with in greater detail by the Council of Europe. As for the area of application, the Council of Europe Convention deals primarily with the automatic processing of personal data whereas the OECD Guidelines apply to personal data which involve dangers to privacy and individual liberties, irrespective of the methods and machinery used in their handling. At the level of details, the basic principles of protection proposed by the two organisations are not identical and the terminology employed differs in some respects. The institutional framework for continued co-operation is treated in greater detail in the Council of Europe Convention than in the OECD Guidelines.

21. The Expert Group also maintained co-operation with the Commission of the European Communities as required by its mandate.

II. The guidelines

A. Purpose and scope

General

22. The Preamble of the Recommendation expresses the basic concerns calling for action. The Recommendation affirms the commitment of Member countries to protect privacy and individual liberties and to respect the transborder flows of personal data.

23. The Guidelines set out in the Annex to the Recommendation consist of five parts. Part One contains a number of definitions and specifies the scope of the Guidelines, indicating that they represent minimum standards. Part Two contains eight basic principles (Paragraphs 7-14) relating to the protection of privacy and individual liberties at the national level. Part Three deals with principles of international application, *i.e.* principles which are chiefly concerned with relationships between Member countries.

24. Part Four deals, in general terms, with means of implementing the basic principles set out in the preceding parts and specifies that these principles should be applied in a non-discriminatory manner. Part Five concerns matters of mutual assistance between Member countries, chiefly through the exchange of information and by avoiding incompatible national procedures for the protection of personal data. It concludes with a reference to issues of applicable law which may arise when flows of personal data involve several Member countries.

Objectives

25. The core of the Guidelines consists of the principles set out in Part Two of the Annex. It is recommended to Member countries that they adhere to these principles with a view to:

a. Achieving acceptance by Member countries of certain minimum standards of protection of privacy and individual liberties with regard to personal data.

b. Reducing differences between relevant domestic rules and practices of Member countries to a minimum.

c. Ensuring that in protecting personal data they take into consideration the interests of other Member countries and the need to avoid undue interference with flows of personal data between Member countries; and

d. Eliminating, as far as possible, reasons which might induce Member countries to restrict transborder flows of personal data because of the possible risks associated with such flows. As stated in the Preamble, two essential basic values are involved: the protection of privacy and individual liberties and the advancement of free flows of personal data. The Guidelines attempt to balance the two values against one another; while accepting certain restrictions to free transborder flows of personal data, they seek to reduce the need for such restrictions and thereby strengthen the notion of free information flows between countries.

26. Finally, Parts Four and Five of the Guidelines contain principles seeking to ensure:

a. Effective national measures for the protection of privacy and individual liberties.

b. Avoidance of practices involving unfair discrimination between individuals; and

c. Bases for continued international co-operation and compatible procedures in any regulation of transborder flows of personal data.

Level of detail

27. The level of detail of the Guidelines varies depending upon two main factors, *viz. a*) the extent of consensus reached concerning the solutions put forward, and *b*) available knowledge and experience pointing to solutions to be adopted at this stage. For instance, the Individual Participation Principle (Paragraph 13) deals specifically with various aspects of protecting an individual's interest, whereas the provision on problems of choice of law and related matters (Paragraph 22) merely states a starting-point for a gradual development of detailed common approaches and international agreements. On the whole, the Guidelines constitute a general framework for concerted actions by Member countries: objectives put forward by the Guidelines may be pursued in different ways, depending on the legal instruments and strategies preferred by Member countries for their implementation. To conclude, there is a need for a continuing review of the Guidelines, both by Member countries and the OECD. As and when experience is gained, it may prove desirable to develop and adjust the Guidelines accordingly.

Non-member countries

28. The Recommendation is addressed to Member countries and this is reflected in several provisions which are expressly restricted to relationships between Member countries (see Paragraphs 15, 17 and 20 of the Guidelines). Widespread recognition of the Guidelines is, however, desirable and nothing in them should be interpreted as preventing the application of relevant provisions by Member countries to non-member countries. In view of the increase in transborder data flows and the need to ensure concerted solutions, efforts will be made to bring the Guidelines to the attention of non-member countries and appropriate international organisations.

The broader regulatory perspective

29. It has been pointed out earlier that the protection of privacy and individual liberties constitutes one of many overlapping legal aspects involved in the processing of data. The Guidelines constitute a new instrument, in addition to other, related international instruments

governing such issues as human rights, telecommunications, international trade, copyright, and various information services. If the need arises, the principles set out in the Guidelines could be further developed within the framework of activities undertaken by the OECD in the area of information, computer and communications policies.

30. Some Member countries have emphasized the advantages of a binding international Convention with a broad coverage. The Mandate of the Expert Group required it to develop guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, without this precluding at a later stage the establishment of an international Convention of a binding nature. The Guidelines could serve as a starting-point for the development of an international Convention when the need arises.

Legal persons, groups and similar entities

31. Some countries consider that the protection required for data relating to individuals may be similar in nature to the protection required for data relating to business enterprises, associations and groups which may or may not possess legal personality. The experience of a number of countries also shows that it is difficult to define clearly the dividing line between personal and non-personal data. For example, data relating to a small company may also concern its owner or owners and provide personal information of a more or less sensitive nature. In such instances it may be advisable to extend to corporate entities the protection offered by rules relating primarily to personal data.

32. Similarly, it is debatable to what extent people belonging to a particular group (*e.g.* mentally disabled persons, immigrants, ethnic minorities) need additional protection against the dissemination of information relating to that group.

33. On the other hand, the Guidelines reflect the view that the notions of individual integrity and privacy are in many respects particular and should not be treated in the same way as the integrity of a group of persons, or corporate security and confidentiality. The needs for protection are different and so are the policy frameworks within which solutions have to be formulated and interests balanced against one another. Some members of the Expert Group suggested that the possibility of extending the Guidelines to legal persons (corporations, associations) should be provided for. This suggestion has not secured a sufficient consensus. The scope of the Guidelines is therefore confined to data relating to individuals and it is left to Member countries to draw dividing lines and decide policies with regard to corporations, groups and similar bodies (cf. paragraph 49 below).

Automated and non-automated data

34. In the past, OECD activities in privacy protection and related fields have focused on automatic data processing and computer networks. The Expert Group has devoted special attention to the issue of whether or not these Guidelines should be restricted to the automatic and computer-assisted processing of personal data. Such an approach may be defended on a number of grounds, such as the particular dangers to individual privacy raised by automation and computerised data banks, and increasing dominance of automatic data processing methods, especially in transborder data flows, and the particular framework of information, computer and communications policies within which the Expert Group has set out to fulfil its Mandate.

35. On the other hand, it is the conclusion of the Expert Group that limiting the Guidelines to the automatic processing of personal data would have considerable drawbacks. To begin with, it is difficult, at the level of definitions, to make a clear distinction between the automatic and non-automatic handling of data. There are, for instance, "mixed" data processing systems, and there are stages in the processing of data which may or may not lead to automatic treatment. These difficulties tend to be further complicated by ongoing technological developments, such as the introduction of advanced semi-automated methods based on the use of microfilm, or microcomputers which may increasingly be used for private purposes that are both harmless and impossible to control. Moreover, by concentrating exclusively on computers the Guidelines might lead to inconsistency and lacunae, and opportunities for record-keepers to circumvent rules which implement the Guidelines by using non-automatic means for purposes which may be offensive.

36. Because of the difficulties mentioned, the Guidelines do not put forward a definition of "automatic data processing" although the concept is referred to in the preamble and in paragraph 3 of the Annex. It may be assumed that guidance for the interpretation of the concept can be obtained from sources such as standard technical vocabularies.

37. Above all, the principles for the protection of privacy and individual liberties expressed in the Guidelines are valid for the processing of data in general, irrespective of the particular technology employed. The Guidelines therefore apply to personal data in general or, more precisely, to personal data which, because of the manner in which they are processed, or because of their nature or context, pose a danger to privacy and individual liberties.

38. It should be noted, however, that the Guidelines do not constitute a set of general privacy protection principles; invasions of privacy by, for instance, candid photography, physical maltreatment, or defamation are outside their scope unless such acts are in one way or another associated with the handling of personal data. Thus, the Guidelines deal with the building-up and use of aggregates of data which are organised for retrieval,

decision-making, research, surveys and similar purposes. It should be emphasized that the Guidelines are neutral with regard to the particular technology used; automatic methods are only one of the problems raised in the Guidelines although, particularly in the context of transborder data flows, this is clearly an important one.

B. Detailed comments

General

39. The comments which follow relate to the actual Guidelines set out in the Annex to the Recommendation. They seek to clarify the debate in the Expert Group.

Paragraph 1: Definitions

40. The list of definitions has been kept short. The term "data controller" is of vital importance. It attempts to define a subject who, under domestic law, should carry ultimate responsibility for activities concerned with the processing of personal data. As defined, the data controller is a party who is legally competent to decide about the contents and use of data, regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf. The data controller may be a legal or natural person, public authority, agency or any other body. The definition excludes at least four categories which may be involved in the processing of data, *viz.*:

a. Licensing authorities and similar bodies which exist in some Member countries and which authorise the processing of data but are not entitled to decide (in the proper sense of the word) what activities should be carried out and for what purposes.

b. Data processing service bureaux which carry out data processing on behalf of others.

c. Telecommunications authorities and similar bodies which act as mere conduits; and

d. "Dependent users" who may have access to data but who are not authorised to decide what data should be stored, who should be able to use them, etc. In implementing the Guidelines, countries may develop more complex schemes of levels and types of responsibilities. Paragraphs 14 and 19 of the Guidelines provide a basis for efforts in this direction.

41. The terms "personal data" and "data subject" serve to underscore that the Guidelines are concerned with physical persons. The precise dividing line between personal data in the sense of information relating to identified or identifiable individuals and anonymous data may be difficult

to draw and must be left to the regulation of each Member country. In principle, personal data convey information which by direct (*e.g.* a civil registration number) or indirect linkages (*e.g.* an address) may be connected to a particular physical person.

42. The term "transborder flows of personal data" restricts the application of certain provisions of the Guidelines to international data flows and consequently omits the data flow problems particular to federal states. The movements of data will often take place through electronic transmission but other means of data communication may also be involved. Transborder flows as understood in the Guidelines includes the transmission of data by satellite.

Paragraph 2: Area of application

43. The Section of the Memorandum dealing with the scope and purpose of the Guidelines introduces the issue of their application to the automatic as against non-automatic processing of personal data. Paragraph 2 of the Guidelines, which deals with this problem, is based on two limiting criteria. The first is associated with the concept of personal data: the Guidelines apply to data which can be related to identified or identifiable individuals. Collections of data which do not offer such possibilities (collections of statistical data in anonymous form) are not included. The second criterion is more complex and relates to a specific risk element of a factual nature, *viz.* that data pose a danger to privacy and individual liberties. Such dangers can arise because of the use of automated data processing methods (the manner in which data are processed), but a broad variety of other possible risk sources is implied. Thus, data which are in themselves simple and factual may be used in a context where they become offensive to a data subject. On the other hand, the risks as expressed in Paragraph 2 of the Guidelines are intended to exclude data collections of an obviously innocent nature (*e.g.* personal notebooks). The dangers referred to in Paragraph 2 of the Guidelines should relate to privacy and individual liberties. However, the protected interests are broad (cf. paragraph 2 above) and may be viewed differently by different Member countries and at different times. A delimitation as far as the Guidelines are concerned and a common basic approach are provided by the principles set out in Paragraphs 7 to 13.

44. As explained in Paragraph 2 of the Guidelines, they are intended to cover both the private and the public sector. These notions may be defined differently by different Member countries.

Paragraph 3: Different degrees of sensitivity

45. The Guidelines should not be applied in a mechanistic way irrespective of the kind of data and processing activities involved. The framework provided by the basic principles in Part Two of the Guidelines permits

Member countries to exercise their discretion with respect to the degree of stringency with which the Guidelines are to be implemented, and with respect to the scope of the measures to be taken. In particular, Paragraph 3 b) provides for many "trivial" cases of collection and use of personal data (cf. above) to be completely excluded from the application of the Guidelines. Obviously this does not mean that Paragraph 3 should be regarded as a vehicle for demolishing the standards set up by the Guidelines. But, generally speaking, the Guidelines do not presuppose their uniform implementation by Member countries with respect to details. For instance, different traditions and different attitudes by the general public have to be taken into account. Thus, in one country universal personal identifiers may be considered both harmless and useful whereas in another country they may be regarded as highly sensitive and their use restricted or even forbidden. In one country, protection may be afforded to data relating to groups and similar entities whereas such protection is completely non-existent in another country, and so forth. To conclude, some Member countries may find it appropriate to restrict the application of the Guidelines to the automatic processing of personal data. Paragraph 3 c) provides for such a limitation.

Paragraph 4: Exceptions to the guidelines

46. To provide formally for exceptions in Guidelines which are part of non-binding Recommendation may seem superfluous. However, the Expert Group has found it appropriate to include a provision dealing with this subject and stating that two general criteria ought to guide national policies in limiting the application of the Guidelines: exceptions should be as few as possible, and they should be made known to the public (*e.g.* through publication in an official government gazette). General knowledge of the existence of certain data or files would be sufficient to meet the second criterion, although details concerning particular data etc. may have to be kept secret. The formula provided in Paragraph 4 is intended to cover many different kinds of concerns and limiting factors, as it was obviously not possible to provide an exhaustive list of exceptions - hence the wording that they include national sovereignty, national security and public policy ("ordre public"). Another overriding national concern would be, for instance, the financial interests of the State ("crédit public"). Moreover, Paragraph 4 allows for different ways of implementing the Guidelines: it should be borne in mind that Member countries are at present at different stages of development with respect to privacy protection rules and institutions and will probably proceed at different paces, applying different strategies, *e.g.* the regulation of certain types of data or activities as compared to regulation of a general nature ("omnibus approach").

47. The Expert Group recognised that Member countries might apply the Guidelines differentially to different kinds of personal data. There may be differences in the permissible frequency of inspection, in ways of balancing

competing interests such as the confidentiality of medical records versus the individual's right to inspect data relating to him, and so forth. Some examples of areas which may be treated differently are credit reporting, criminal investigation and banking. Member countries may also choose different solutions with respect to exceptions associated with, for example, research and statistics. An exhaustive enumeration of all such situations and concerns is neither required nor possible. Some of the subsequent paragraphs of the Guidelines and the comments referring to them provide further clarification of the area of application of the Guidelines and of the closely related issues of balancing opposing interests (compare with Paragraphs 7, 8, 17 and 18 of the Guidelines). To summarise, the Expert Group has assumed that exceptions will be limited to those which are necessary in a democratic society.

Paragraph 5: Federal countries

48. In Federal countries, the application of the Guidelines is subject to various constitutional limitations. Paragraph 5, accordingly, serves to underscore that no commitments exist to apply the Guidelines beyond the limits of constitutional competence.

Paragraph 6: Minimum standards

49. First, Paragraph 6 describes the Guidelines as minimum standards for adoption in domestic legislation. Secondly, and in consequence, it has been agreed that the Guidelines are capable of being supplemented by additional measures for the protection of privacy and individual liberties at the national as well as the international level.

Paragraph 7: Collection limitation principle

50. As an introductory comment on the principles set out in Paragraphs 7 to 14 of the Guidelines it should be pointed out that these principles are interrelated and partly overlapping. Thus, the distinctions between different activities and stages involved in the processing of data which are assumed in the principles, are somewhat artificial and it is essential that the principles are treated together and studied as a whole. Paragraph 7 deals with two issues, *viz.* a) limits to the collection of data which, because of the manner in which they are to be processed, their nature, the context in which they are to be used or other circumstances, are regarded as specially sensitive; and b) requirements concerning data collection methods. Different views are frequently put forward with respect to the first issue. It could be argued that it is both possible and desirable to enumerate types or categories of data which are per se sensitive and the collection of which should be restricted or even prohibited. There are precedents in European legislation to this effect (race, religious beliefs, criminal records, for instance). On the other hand, it may be held that no

data are intrinsically "private" or "sensitive" but may become so in view of their context and use. This view is reflected, for example, in the privacy legislation of the United States.

51. The Expert Group has discussed a number of sensitivity criteria, such as the risk of discrimination, but has not found it possible to define any set of data which are universally regarded as sensitive. Consequently, Paragraph 7 merely contains a general statement that there should be limits to the collection of personal data. For one thing, this represents an affirmative recommendation to lawmakers to decide on limits which would put an end to the indiscriminate collection of personal data. The nature of the limits is not spelt out but it is understood that the limits may relate to: - data quality aspects (*i.e.* that it should be possible to derive information of sufficiently high quality from the data collected, that data should be collected in a proper information framework, etc.); - limits associated with the purpose of the processing of data (*i.e.* that only certain categories of data ought to be collected and, possibly, that data collection should be restricted to the minimum necessary to fulfil the specified purpose); - "earmarking" of specially sensitive data according to traditions and attitudes in each Member country; - limits to data collection activities of certain data controllers; - civil rights concerns.

52. The second part of Paragraph 7 (data collection methods) is directed against practices which involve, for instance, the use of hidden data registration devices such as tape recorders, or deceiving data subjects to make them supply information. The knowledge or consent of the data subject is as a rule essential, knowledge being the minimum requirement. On the other hand, consent cannot always be imposed, for practical reasons. In addition, Paragraph 7 contains a reminder ("where appropriate") that there are situations where for practical or policy reasons the data subject's knowledge or consent cannot be considered necessary. Criminal investigation activities and the routine up-dating of mailing lists may be mentioned as examples. Finally, Paragraph 7 does not exclude the possibility of a data subject being represented by another party, for instance in the case of minors, mentally disabled persons, etc.

Paragraph 8: Data quality principle

53. Requirements that data be relevant can be viewed in different ways. In fact, some members of the Expert Group hesitated as to whether such requirements actually fitted into the framework of privacy protection. The conclusion of the Group was to the effect, however, that data should be related to the purpose for which they are to be used. For instance, data concerning opinions may easily be misleading if they are used for purposes to which they bear no relation, and the same is true of evaluative data. Paragraph 8 also deals with accuracy, completeness and up-to-dateness which are all important elements of the data quality concept. The requirements in this respect are linked to the purposes of data, *i.e.* they are

not intended to be more far-reaching than is necessary for the purposes for which the data are used. Thus, historical data may often have to be collected or retained; cases in point are social research, involving so-called longitudinal studies of developments in society, historical research, and the activities of archives. The "purpose test" will often involve the problem of whether or not harm can be caused to data subjects because of lack of accuracy, completeness and up-dating.

Paragraph 9: Purpose specification principle

54. The Purpose Specification Principle is closely associated with the two surrounding principles, *i.e.* the Data Quality Principle and the Use Limitation Principle. Basically, Paragraph 9 implies that before, and in any case not later than at the time of data collection, it should be possible to identify the purposes for which these data are to be used, and that later changes of purposes should likewise be specified. Such specification of purposes can be made in a number of alternative or complementary ways, *e.g.* by public declarations, information to data subjects, legislation, administrative decrees, and licences provided by supervisory bodies. According to Paragraphs 9 and 10, new purposes should not be introduced arbitrarily; freedom to make changes should imply compatibility with the original purposes. Finally, when data no longer serve a purpose, and if it is practicable, it may be necessary to have them destroyed (erased) or given an anonymous form. The reason is that control over data may be lost when data are no longer of interest; this may lead to risks of theft, unauthorised copying or the like.

Paragraph 10: Use limitation principle

55. This paragraph deals with uses of different kinds, including disclosure, which involve deviations from specified purposes. For instance, data may be transmitted from one computer to another where they can be used for unauthorised purposes without being inspected and thus disclosed in the proper sense of the word. As a rule the initially or subsequently specified purposes should be decisive for the uses to which data can be put. Paragraph 10 foresees two general exceptions to this principle: the consent of the data subject (or his representative - see Paragraph 52 above) and the authority of law (including, for example, licences granted by supervisory bodies). For instance, it may be provided that data which have been collected for purposes of administrative decision-making may be made available for research, statistics and social planning.

Paragraph 11: Security safeguards principle

56. Security and privacy issues are not identical. However, limitations on data use and disclosure should be reinforced by security safeguards. Such safeguards include physical measures (locked doors and identification

cards, for instance), organisational measures (such as authority levels with regard to access to data) and, particularly in computer systems, informational measures (such as enciphering and threat monitoring of unusual activities and responses to them). It should be emphasized that the category of organisational measures includes obligations for data processing personnel to maintain confidentiality. Paragraph 11 has a broad coverage. The cases mentioned in the provision are to some extent overlapping (*e.g.* access/disclosure). "Loss" of data encompasses such cases as accidental erasure of data, destruction of data storage media (and thus destruction of data) and theft of data storage media. "Modified" should be construed to cover unauthorised input of data, and "use" to cover unauthorised copying.

Paragraph 12: Openness principle

57. The Openness Principle may be viewed as a prerequisite for the Individual Participation Principle (Paragraph 13); for the latter principle to be effective, it must be possible in practice to acquire information about the collection, storage or use of personal data. Regular information from data controllers on a voluntary basis, publication in official registers of descriptions of activities concerned with the processing of personal data, and registration with public bodies are some, though not all, of the ways by which this may be brought about. The reference to means which are "readily available" implies that individuals should be able to obtain information without unreasonable effort as to time, advance knowledge, travelling, and so forth, and without unreasonable cost.

Paragraph 13: Individual participation principle

58. The right of individuals to access and challenge personal data is generally regarded as perhaps the most important privacy protection safeguard. This view is shared by the Expert Group which, although aware that the right to access and challenge cannot be absolute, has chosen to express it in clear and fairly specific language. With respect to the individual sub-paragraphs, the following explanations are called for:

59. The right to access should as a rule be simple to exercise. This may mean, among other things, that it should be part of the day-to-day activities of the data controller or his representative and should not involve any legal process or similar measures. In some cases it may be appropriate to provide for intermediate access to data; for example, in the medical area a medical practitioner can serve as a go-between. In some countries supervisory organs, such as data inspection authorities, may provide similar services. The requirement that data be communicated within reasonable time may be satisfied in different ways. For instance, a data controller who provides information to data subjects at regular intervals may be exempted from obligations to respond at once to individual

requests. Normally, the time is to be counted from the receipt of a request. Its length may vary to some extent from one situation to another depending on circumstances such as the nature of the data processing activity. Communication of such data "in a reasonable manner" means, among other things, that problems of geographical distance should be given due attention. Moreover, if intervals are prescribed between the times when requests for access must be met, such intervals should be reasonable. The extent to which data subjects should be able to obtain copies of data relating to them is a matter of implementation which must be left to the decision of each Member country.

60. The right to reasons in Paragraph 13 c) is narrow in the sense that it is limited to situations where requests for information have been refused. A broadening of this right to include reasons for adverse decisions in general, based on the use of personal data, met with sympathy in the Expert Group. However, on final consideration a right of this kind was thought to be too broad for insertion in the privacy framework constituted by the Guidelines. This is not to say that a right to reasons for adverse decisions may not be appropriate, *e.g.* in order to inform and alert a subject to his rights so that he can exercise them effectively.

61. The right to challenge in 13 c) and d) is broad in scope and includes first instance challenges to data controllers as well as subsequent challenges in courts, administrative bodies, professional organs or other institutions according to domestic rules of procedure (compare with Paragraph 19 of the Guidelines). The right to challenge does not imply that the data subject can decide what remedy or relief is available (rectification, annotation that data are in dispute, etc.): such matters will be decided by domestic law and legal procedures. Generally speaking, the criteria which decide the outcome of a challenge are those which are stated elsewhere in the Guidelines.

Paragraph 14: Accountability principle

62. The data controller decides about data and data processing activities. It is for his benefit that the processing of data is carried out. Accordingly, it is essential that under domestic law accountability for complying with privacy protection rules and decisions should be placed on the data controller who should not be relieved of this obligation merely because the processing of data is carried out on his behalf by another party, such as a service bureau. On the other hand, nothing in the Guidelines prevents service bureaux personnel, "dependent users" (see Paragraph 40) and others from also being held accountable. For instance, sanctions against breaches of confidentiality obligations may be directed against all parties entrusted with the handling of personal information (cf. Paragraph 19 of the Guidelines). Accountability under Paragraph 14 refers to accountability supported by legal sanctions, as well as to accountability established by codes of conduct, for instance.

Paragraphs 15-18: Basic principles of international application

63. The principles of international application are closely interrelated. Generally speaking, Paragraph 15 concerns respect by Member countries for each other's interest in protecting personal data, and the privacy and individual liberties of their nationals and residents. Paragraph 16 deals with security issues in a broad sense and may be said to correspond, at the international level, to Paragraph 11 of the Guidelines. Paragraphs 17 and 18 deal with restrictions on free flows of personal data between Member countries; basically, as far as protection of privacy and individual liberties is concerned, such flows should be admitted as soon as requirements of the Guidelines for the protection of these interests have been substantially, *i.e.* effectively, fulfilled. The question of other possible bases of restricting transborder flows of personal data is not dealt with in the Guidelines.

64. For domestic processing Paragraph 15 has two implications. First, it is directed against liberal policies which are contrary to the spirit of the Guidelines and which facilitate attempts to circumvent or violate protective legislation of other Member countries. However, such circumvention or violation, although condemned by all Member countries, is not specifically mentioned in this Paragraph as a number of countries felt it to be unacceptable that one Member country should be required to directly or indirectly enforce, extraterritorially, the laws of other Member countries. It should be noted that the provision explicitly mentions the re-export of personal data. In this respect, Member countries should bear in mind the need to support each other's efforts to ensure that personal data are not deprived of protection as a result of their transfer to territories and facilities for the processing of data where control is slack or non-existent.

65. Secondly, Member countries are implicitly encouraged to consider the need to adapt rules and practices for the processing of data to the particular circumstances which may arise when foreign data and data on non-nationals are involved. By way of illustration, a situation may arise where data on foreign nationals are made available for purposes which serve the particular interests of their country of nationality (*e.g.* access to the addresses of nationals living abroad).

66. As far as the Guidelines are concerned, the encouragement of international flows of personal data is not an undisputed goal in itself. To the extent that such flows take place they should, however, according to Paragraph 16, be uninterrupted and secure, *i.e.* protected against unauthorised access, loss of data and similar events. Such protection should also be given to data in transit, *i.e.* data which pass through a Member country without being used or stored with a view to usage in that country. The general commitment under Paragraph 16 should, as far as computer networks are concerned, be viewed against the background of the International Telecommunications Convention of Malaga-Torremolinos (25th October, 1973). According to that Convention, the members of the International Telecommunications Union, including the

OECD Member countries, have agreed, inter alia, to ensure the establishment, under the best technical conditions, of the channels and installations necessary to carry on the rapid and uninterrupted exchange of international telecommunications. Moreover, the members of ITU have agreed to take all possible measures compatible with the telecommunications system used to ensure the secrecy of international correspondence. As regards exceptions, the right to suspend international telecommunications services has been reserved and so has the right to communicate international correspondence to the competent authorities in order to ensure the application of internal laws or the execution of international conventions to which members of the ITU are parties. These provisions apply as long as data move through telecommunications lines. In their context, the Guidelines constitute a complementary safeguard that international flows of personal data should be uninterrupted and secure.

67. Paragraph 17 reinforces Paragraph 16 as far as relationships between Member countries are concerned. It deals with interests which are opposed to free transborder flows of personal data but which may nevertheless constitute legitimate grounds for restricting such flows between Member countries. A typical example would be attempts to circumvent national legislation by processing data in a Member country which does not yet substantially observe the Guidelines. Paragraph 17 establishes a standard of equivalent protection, by which is meant protection which is substantially similar in effect to that of the exporting country, but which need not be identical in form or in all respects. As in Paragraph 15, the re-export of personal data is specifically mentioned - in this case with a view to preventing attempts to circumvent the domestic privacy legislation of Member countries. The third category of grounds for legitimate restrictions mentioned in Paragraph 17, concerning personal data of a special nature, covers situations where important interests of Member countries could be affected. Generally speaking, however, Paragraph 17 is subject to Paragraph 4 of the Guidelines which implies that restrictions on flows of personal data should be kept to a minimum.

68. Paragraph 18 attempts to ensure that privacy protection interests are balanced against interests of free transborder flows of personal data. It is directed in the first place against the creation of barriers to flows of personal data which are artificial from the point of view of protection of privacy and individual liberties and fulfil restrictive purposes of other kinds which are thus not openly announced. However, Paragraph 18 is not intended to limit the rights of Member countries to regulate transborder flows of personal data in areas relating to free trade, tariffs, employment, and related economic conditions for international data traffic. These are matters which were not addressed by the Expert Group, being outside its Mandate.

Paragraph 19: National implementation

69. The detailed implementation of Parts Two and Three of the Guidelines is left in the first place to Member countries. It is bound to vary according to different legal systems and traditions, and Paragraph 19 therefore attempts merely to establish a general framework indicating in broad terms what kind of national machinery is envisaged for putting the Guidelines into effect. The opening sentence shows the different approaches which might be taken by countries, both generally and with respect to control mechanisms (*e.g.* especially set-up supervisory bodies, existing control facilities such as courts, public authorities, etc.).

70. In Paragraph 19 a) countries are invited to adopt appropriate domestic legislation, the word "appropriate" foreshadowing the judgement by individual countries of the appropriateness or otherwise of legislative solutions. Paragraph 19 b) concerning self-regulation is addressed primarily to common law countries where non-legislative implementation of the Guidelines would complement legislative action. Paragraph 19 c) should be given a broad interpretation; it includes such means as advice from data controllers and the provision of assistance, including legal aid. Paragraph 19 d) deals with criminal, civil and administrative punishment. It permits different approaches to the issue of control mechanisms: briefly, either the setting-up of special supervisory bodies, or reliance on already existing control facilities, whether in the form of courts, existing public authorities or otherwise. Paragraph 19 e) dealing with discrimination is directed against unfair practices but leaves open the possibility of "benign discrimination" to support disadvantaged groups, for instance. The provision is directed against unfair discrimination on such bases as nationality and domicile, sex, race, creed, or trade union affiliation.

Paragraph 20: Information exchange and compatible procedures

71. Two major problems are dealt with here, *viz.* a) the need to ensure that information can be obtained about rules, regulations, decisions, etc. which implement the Guidelines, and b) the need to avoid transborder flows of personal data being hampered by an unnecessarily complex and disparate framework of procedures and compliance requirements. The first problem arises because of the complexity of privacy protection regulation and data policies in general. There are often several levels of regulation (in a broad sense) and many important rules cannot be laid down permanently in detailed statutory provisions; they have to be kept fairly open and left to the discretion of lower-level decision-making bodies.

72. The importance of the second problem is, generally speaking proportional to the number of domestic laws which affect transborder flows of personal data. Even at the present stage, there are obvious needs for co-ordinating special provisions on transborder data flows in domestic

laws, including special arrangements relating to compliance control and, where required, licences to operate data processing systems.

Paragraph 21: Machinery for co-operation

73. The provision on national procedures assumes that the Guidelines will form a basis for continued co-operation. Data protection authorities and specialised bodies dealing with policy issues in information and data communications are obvious partners in such a co-operation. In particular, the second purpose of such measures, contained in Paragraph 21 ii), *i.e.* mutual aid in procedural matters and requests for information, is future-oriented: its practical significance is likely to grow as international data networks and the complications associated with them become more numerous.

Paragraph 22: Conflicts of laws

74. The Expert Group has devoted considerable attention to issues of conflicts of laws, and in the first place to the questions as to which courts should have jurisdiction over specific issues (choice of jurisdiction) and which system of law should govern specific issues (choice of law). The discussion of different strategies and proposed principles has confirmed the view that at the present stage, with the advent of such rapid changes in technology, and given the non-binding nature of the Guidelines, no attempt should be made to put forward specific, detailed solutions. Difficulties are bound to arise with respect to both the choice of a theoretically sound regulatory model and the need for additional experience about the implications of solutions which in themselves are possible.

75. As regards the question of choice of law, one way of approaching these problems is to identify one or more connecting factors which, at best, indicate one applicable law. This is particularly difficult in the case of international computer networks where, because of dispersed location and rapid movement of data, and geographically dispersed data processing activities, several connecting factors could occur in a complex manner involving elements of legal novelty. Moreover, it is not evident what value should presently be attributed to rules which by mechanistic application establish the specific national law to be applied. For one thing, the appropriateness of such a solution seems to depend upon the existence of both similar legal concepts and rule structures, and binding commitments of nations to observe certain standards of personal data protection. In the absence of these conditions, an attempt could be made to formulate more flexible principles which involve a search for a "proper law" and are linked to the purpose of ensuring effective protection of privacy and individual liberties. Thus, in a situation where several laws may be applicable, it has been suggested that one solution could be to give preference to the domestic law offering the best protection of personal data. On the other

hand, it may be argued that solutions of this kind leave too much uncertainty, not least from the point of view of the data controllers who may wish to know, where necessary in advance, by which national systems of rules an international data processing system will be governed.

76. In view of these difficulties, and considering that problems of conflicts of laws might best be handled within the total framework of personal and non-personal data, the Expert Group has decided to content itself with a statement which merely signals the issues and recommends that Member countries should work towards their solution.

Follow-up

77. The Expert Group called attention to the terms of Recommendation 4 on the Guidelines which suggests that Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of the Guidelines.

DECLARATION ON THE PROTECTION OF PRIVACY ON GLOBAL NETWORKS (1998)

The Governments of OECD Member countries[1] at the Conference "A Borderless World: Realising the Potential of Global Electronic Commerce," Ottawa, Canada,

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

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

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

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

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

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

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

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

Considering that different effective approaches to privacy protection developed by Member countries, including the adoption and

1. Including the European Communities.

implementation of laws or industry self-regulation, can work together to achieve effective privacy protection on global networks;

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

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

REAFFIRM the objectives set forth in:

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

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

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

DECLARE that**:**

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

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

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

- Encourage the adoption of privacy policies, whether implemented by legal, self-regulatory, administrative or technological means.
- Encourage the online notification of privacy policies to users.
- Ensure that effective enforcement mechanisms are available both to address non-compliance with privacy principles and policies and to ensure access to redress.
- Promote user education and awareness about online privacy issues and the means at their disposal for protecting privacy on global networks.

- Encourage the use of privacy-enhancing technologies; and
- Encourage the use of contractual solutions and the development of model contractual solutions for online transborder data flows.

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

FURTHER DECLARE that the OECD should**:**

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

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

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

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

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

INVITE:

Non-member countries to take account of this Declaration;

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

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

PRIVACY ONLINE: POLICY AND PRACTICAL GUIDANCE (2003)

Note by the secretariat

The OECD has, over the last six years, placed high priority on work on the global information infrastructure, the global information society and electronic commerce.

Based on the work achieved by OECD member countries to fulfil the 1998 Ministerial Declaration on the Protection of Privacy on Global Networks, this report reflects the ministerial high level objective to build bridges between different national approaches in order to ensure the effective protection of privacy and personal data as well as the continued transborder flow of personal data on global networks.

The report includes policy and practical guidance for implementing privacy protection online. Addressed to OECD member countries, business and other organisations, individual users and consumers, the report is intended to reinforce the impact and visibility of the action of the OECD, and the importance of the OECD Privacy Guidelines in the development and implementation of a mix of solutions for ensuring global privacy.

Main points

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

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

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

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

Privacy protection online: introduction

The 1980 OECD privacy guidelines

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

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

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

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

Privacy protection in the global information society

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

In the digital economy, individuals may leave behind electronic "footprints" or records of where they have been, what they spent time looking at, the thoughts they aired, the messages they sent, and the goods and services they purchased. The related privacy issues arise from the fact that all this computer-processable personal information, whether

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

automatically generated or not, can potentially be collected, stored, detailed, individualised, linked and put to a variety of uses in places geographically dispersed all around the world, possibly without user knowledge or consent.

Background to the ministerial mandate

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

- Raise issues linked to the protection of privacy and transborder flows of personal data in relation to global networks; and

- Consider various solutions that could facilitate the seamless implementation of privacy protection online and contribute to building a trustworthy environment for the development of electronic commerce.

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

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

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

2. See Annex II.

Ministerial declaration

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

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

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

OECD action plan

The action items approved by ministers at the Ottawa conference were integrated in the OECD Action Plan, and assigned to the appropriate committees and working parties.[3] In this context, the Working Party on Information Security and Privacy (WPISP), under the auspices of the Committee for Information, Computer and Communications Policy (ICCP)

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

focused much of its work on the implementation of the elements of the OECD six-step programme of work for online privacy protection:

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

All documents and other instruments (*e.g.* Internet-based tools) produced by the WPISP and declassified by the ICCP are annexed to the present report (see Part III). They are presented in Part I of this report under the headings of the six-step programme of work mentioned above and form the basic output material upon which Part II on policy and practical guidance draws.

I. Fulfilling the ministerial mandate: OECD work

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

OECD member countries first undertook to survey, at international, regional and national levels, the variety of legal instruments, practices and technologies, either in use or being developed, to implement and enforce privacy principles in the online environment. The inventory[4] included horizontal or sectoral data protection laws, codes of conduct, industry standards and industry-led technological solutions, including privacy enhancing technologies (PETs), online educational tools, systems for labelling, certifying and attaching privacy seals, and dispute resolution schemes. It was noted that technological tools were increasingly used to protect privacy rights online. The fact that effective protection of privacy online required online participants to be not only "information technology literate", but also aware of the privacy implications of their actions was emphasised.

4. See Annex III.

1) Encouraging the adoption of privacy policies

OECD member countries developed a Privacy Policy Statement Generator[5] (OECD Privacy Generator) as an educational Internet technology tool which provides organisations with support and guidance in developing policies and practices consistent with the OECD Privacy Guidelines. In particular, the generator was designed to assist organisations in developing privacy policies and statements for display on their Web sites.

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

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

Member countries also considered that use of the OECD Privacy Generator should promote greater consistency in privacy protection across national borders. It can help organisations to understand the requirements of privacy protection principles at national and international levels and to build trust with other organisations and individual users online. It can also help individual users to become educated to look for privacy statements as a routine part of their online experiences.

2) Encouraging the online notification of privacy policies to users

By making the Privacy Policy Statement Generator freely available, the OECD has contributed to both organisation and individual user awareness of online privacy issues. The generator makes it easier for organisations to provide individual users with online notice of their privacy policies.[6] The

5. See Annex IV for a "paper copy". The Generator is accessible at www.oecd.org/sti/security-privacy or http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm.

6. In June 2001, Visa International obliged its online merchants to post privacy policies and encouraged the use of the OECD Generator for their creation. See http://international.visa.com/fb/merchants/news/.

inclusion of links to relevant government and private sector Web sites is intended to increase business and other organisations' as well as individual user and consumer awareness of the privacy protection framework that applies to their online activities.

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

The positive perception by the public of online privacy policies is confirmed by a few public opinion polls and surveys. For example, a study conducted in 2000 showed that 75% of online users and consumers tended to trust Web sites more when privacy policy statements were posted on those merchants' sites.[7] Similarly, a May 2002[8] study concluded that up to USD 24.5 billion in online sales were likely to be lost by 2006 because of bad privacy policies: "For a business with poor online privacy policies, offline sales will slip as consumers shift to more privacy-sensitive competitors," the report said. Since 1997 however, commercial Web sites have embraced the practice of posting privacy policies in an effort to build trust on line. In March 2002, the Progress and Freedom Foundation[9] reported that 98% of the 100 most frequently visited web sites post a privacy policy, and 88% of random sites also post privacy statements.

3) Ensuring that enforcement and redress mechanisms are available to users in cases of:

Non-compliance with privacy principles and policies

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

Alternative dispute resolution

OECD member countries undertook a series of studies on ADR, which consists of practical out-of-court methods involving a neutral third-party

7. The survey found that a combined 75% of people who have seen a privacy policy online, view notices explaining how personal information will be used, as either "absolutely essential" or "very important." (Business Week/Harris, March 2000).

8. Jupiter Research (2002), "Online Privacy: Managing Complexity to Realize Marketing Benefits," 17 May.

9. The survey "Privacy Online: A Report on the Information Practices and Policies of Commercial Websites" released in March of 2002 by the Progress and Freedom Foundation studied over 5 500 Web sites and 100 of the busiest sites.

to resolve disputes in a quick and inexpensive way. In December 2000 the OECD,[10] in conjunction with The Hague Conference on International Law and the International Chamber of Commerce, held a conference in The Hague on "Online Alternative Dispute Resolution Mechanisms for Privacy and Consumer Protection Disputes".[11] The aim of the conference was to explore if and how online ADR mechanisms can help resolve business to consumer (B2C) disputes arising from privacy and consumer protection issues and thus improve trust for global electronic commerce. The primary focus of the conference was on low levels of harm, as well as on informal, flexible systems that allow for the necessary balancing between the type of dispute and the formality of the process for resolution (*e.g.* assisted negotiation and mediation).

A consensus emerged on some principles, such as: settling disputes at an early stage is most effective; flexibility and variety in ADR mechanisms is valuable; appropriate technological developments may facilitate ADR; individual users need information about processes in order to participate effectively; procedural safeguards are important in some disputes.

The conference was followed up with a work programme focused on legal and educational aspects of ADR. The legal aspect of the programme aimed to generate an overview of national legal regimes applicable to B2C ADR in member countries, with a view to understanding if and how existing legal provisions impact recourse to ADR. A report[12] was developed on the basis of member country responses to a survey on existing laws and regulations related to ADR. The report highlighted that there is not a single set of rules governing ADR. Different rules have developed in different contexts. In a number of areas the existing legal framework provides guidance to potential parties to an ADR procedure at the national level. For example, many countries regulate the provision of arbitration services. However, there are fewer regulations that would generally govern the provision of less formal types of B2C ADR. What regulation there is typically addresses the provision of ADR through mechanisms established, funded or run by governments. As regards flexible and informal ADR mechanisms designed for the online world, no member country reported the existence of specific legal provisions although most expressed an interest in promoting fair and effective online ADR as a way to resolve small value B2C disputes, particularly cross-border disputes. Looking more specifically at the cross-border context, national differences appeared as to the validity of agreements to submit to ADR, the procedural principles for use during an ADR, confidentiality and security of proceedings, validity of settlement

10. Work conducted by the WPISP in close co-operation with the OECD Committee on Consumer Policy (CCP).

11. See Annex V.

12. See Annex VI.

agreements arising out of an ADR, and the availability of enforcement mechanisms.

The educational part of the programme aimed to inform individual users and businesses, notably small and medium-sized enterprises (SMEs) about the availability of ADR and its potential benefits. A first set of questions was produced to help individual users determine whether online ADR can help them resolve a dispute, such as what to think about before considering ADR, how to choose a particular form of ADR, where to locate ADR providers, and what to do if ADR cannot help.[13] A second set of questions aimed at guiding SMEs is under preparation.

Finally, the OECD helped to produce further information regarding the availability of ADR by assisting the ICC to produce an inventory of ADR programmes world-wide. The resulting report and inventory are available on the ICC Web site.[14]

Compliance and enforcement mechanisms

Recognising that the higher the level of compliance, the less need there is for enforcement, and that a strong level of enforcement may motivate actors to adopt a higher level of compliance, OECD member countries undertook to survey and analyse enforcement mechanisms that are available both to address non-compliance with privacy principles and policies and to ensure access to redress.[15] The objective was to gather information through a questionnaire addressed to member countries and the private sector that would: *(i)* lead to a better understanding of how privacy safeguards, enforcement mechanisms, and potential remedies can enhance privacy as set forth in the OECD Privacy Guidelines and the Ottawa Ministerial Declaration; and *(ii)* form the basis for assessing the practical application of available compliance and enforcement instruments in a networked environment and their ability to meet the objectives of the OECD Privacy Guidelines, including effectiveness and coverage across jurisdictions.

The summary and the analysis of the responses to the questionnaire[16] demonstrated that the legal landscape for privacy compliance and enforcement has changed: if government regulation remains the foundation upon which individual user trust in the area of privacy is based, regulation is increasingly combined with complementary technical,

13. See Annex VII.

14. See http://www.iccwbo.org/home/news_archives/2002/stories/adr.asp. "Alternative Dispute Resolutions Providers: A Global Inventory", July 2002.

    See http://www.iccwbo.org/home/news_archives/2002/stories/adr.asp.

15. See Annex VIII.

16. Draft prepared by a consultant to the OECD, Chris Kuner, a partner in the law firm Hunton & Williams.

organisational, and self-regulatory mechanisms in order to attain maximum effectiveness. It was noted that many such initiatives are now underway in member countries, and that there is every sign that their use will grow rapidly in the coming years. Moreover, the report stressed that efforts to ensure compliance before the fact impose less burden than having to rely on enforcement actions. It also demonstrated that it is critical that privacy protection be viewed in a global perspective, rather than in a purely national one, in order to better facilitate redress for privacy violations that cross national borders.

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

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

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

5) Encouraging the use of privacy enhancing technologies

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

to the different privacy concerns. There are continuous significant advances in the development and use of such technologies.[17]

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

The Inventory of Privacy Enhancing Technologies[18] was produced to analyse the availability and variety of PETs, consider the factors affecting their adoption, analyse the relationship between technology and privacy, and form a basis for policy makers to discuss the use and deployment of such technologies. The paper[19] discussed methods of online personal data collection, analysed different types of PETs and made recommendations to the private sector for encouraging their increased development and use. Technological tools that can assist in safeguarding online privacy, PETs were shown to present a range of characteristics. Some filter "cookies" and other tracking technologies; some allow for "anonymous" Web-browsing and e-mail; some provide protection by encrypting data; some focus on allowing privacy and security in e-commerce purchases; and some allow for the advanced, automated management of users' individual data on their behalf. In essence, PETs reinforce transparency and choice, which can lead to greater individual control of data protection. However, many technologies can be used in many different ways. Different products, technologies and various functions can serve different purposes depending on the preferences of the user and the implementation of the particular technology.

A Forum Session on Privacy Enhancing Technologies[20] was held at the OECD in October 2001 in order to facilitate discussion *(i)* on the policy implications of PETs; *(ii)* the future of such tools in the wider context of online privacy protection; and *(iii)* the challenges of, and methods for, educating business about the importance of privacy by design and the use of PETs, and for educating individuals about the benefits and limitations of PETs. The session made it clear, in particular, that technically speaking, PETs did not offer a full range of functionalities that would provide total privacy protection in line with the OECD Privacy Guidelines (*e.g.* among the PETs surveyed (see paragraph below), only one tool addressed five of the eight privacy principles and 58 applied to only one principle).

17. See US Department of Commerce Workshop (September 2000): http://www.ntia.doc.gov/ntiahome/privacy/.

18. Draft prepared by a consultant to the OECD, Lauren Hall, Director, Technology Policy, Advanced Strategy and Policies, Microsoft Corporation, former Executive Vice President of the Software & Information Industry Association.

19. See Annex IX.

20. See Annex X.

A study and a research paper[21] included a synthesis of a survey of PETs available on the Web, and a table of the surveyed technologies, as well as a discussion of the question of when, for whom, and under what circumstances, "communication" about PETs might work, in the sense of encouraging businesses to supply such tools and individuals to use them.

PETs were considered to be helpful technological tools to assist in protecting online privacy as part of a wider package of online privacy initiatives.[22] They can empower individual users seeking to control the disclosure, use and distribution of personal information online. PETs can also aid organisations in enforcing their own privacy policies and practices, and more generally, in an era of individual user concerns about online privacy, PETs are crucial tools in managing the flow of personal information on global networks.

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

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

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

21. Drafts prepared by two consultants to the OECD: Laurent Bernat, Head Information and Strategy, Projetweb, and Perri 6, Director, The Policy Programme, Institute for Applied Health and Social Policy, King's College, London.

22. The wider privacy package includes among others, development and notification of privacy policies and an increasing availability of online redress mechanisms – in addition to privacy enhancing technologies.

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

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

> "Part Three – Basic Principles of International Application: Free Flow and Legitimate Restrictions
>
> 15. Member countries should take into consideration the implications for other member countries of domestic processing and re-export of personal data.
>
> 16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a member country, are uninterrupted and secure.
>
> 17. A member country should refrain from restricting transborder flows of personal data between itself and another member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other member country provides no equivalent protection.
>
> 18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection."

To contribute to the resolution of problems related to transborder transactions, OECD member countries prepared a report on transborder data flow contracts in the online context.[23] The report[24] which was partly directed at online business-to-business transactions should be read with later documents such as the model contracts published by the European Commission, the Council of Europe and the International Chamber of Commerce.[25]

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

24. See Annex XI.

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

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

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

II. Moving forward: policy and practical guidance for implementing privacy protection online

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

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

Blending approaches

Although many systems are hybrid approaches combining self-regulation and legislative actions, privacy protection has traditionally been approached as if there were primarily two approaches: government regulatory and legislative actions and market-based self-regulatory efforts. Early in 1998,[26] OECD member countries agreed that each of these approaches had advantages and disadvantages. Government efforts

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

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

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

seemed to offer predictable, enforceable legal protections and redress mechanisms, and self-regulatory efforts appeared to enable organisations in different sectors to tailor detailed guidelines to work within specific circumstances. In both approaches, difficulties in adequately addressing privacy online were foreseen, particularly with respect to cross-border issues. The debate moved then to discuss what mix of instruments and techniques would be best tailored to the protection of privacy in the global online environment.

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

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

Strengthening co-operation

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

Therefore, member countries, businesses and other organisations, as well as individual users and consumers are recommended to give effect to, and

disseminate the following policy and practical guidance, and non member countries are also invited to take account of it.

Practical guidance on policy for OECD member countries

At the national level

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

1) The adoption of privacy policies through:

Encouraging organisations with a presence online to:

- Systematically conduct an extensive review of their privacy practices and to develop a privacy policy that would give effect to the OECD privacy principles.
- Review laws or self-regulatory schemes which may apply to their collection and use of personal data, review their practices against such regulation, and amend them where necessary to better ensure compliance.
- Reassess on a regular basis their privacy practices and policy.
- Use the OECD Privacy Policy Statement Generator.[27]

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

- Taking initiatives to create hyperlinks from national Web sites to the OECD Web site.
- Translating the Generator into their language.
- Using the source code[28] to implement the Generator in their language and/or to enhance it by adding a section on additional national privacy requirements.

27. See Annex IV and http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm.

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

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

Encouraging organisations with a presence online to:

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

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

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

- Fostering the design and offering of flexible and informal online alternative dispute resolution mechanisms that would take into account the global nature of electronic commerce (*e.g.* functioning in multiple languages), and be able to cope with transborder disputes.
- Striving to reduce national differences in existing legal frameworks that may affect the operability of alternative dispute resolution mechanisms in the cross-border context.
- Further providing advice to individual users on how to file complaints and obtain redress for breaches of their privacy in relation to online interactions, and raising awareness of what kinds of alternative dispute resolution programmes are offered in different countries and what rules they operate under.

Actively fostering compliance with privacy principles and policies by:

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

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

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

- Strengthening enforcement against organisations misrepresenting compliance with privacy policies and other privacy promises to individual users.

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

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

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

- Actively encouraging developers of systems and software applications to incorporate privacy into the design of information technologies.
- Actively encouraging organisations to consider at an early stage the privacy implications of their technologies and services.
- Providing incentives, such as appropriate joint action with the private sector, for the further development of a sustainable market for privacy enhancing technologies designed for individual users as well as for organisations, and encouraging a wider use of such tools.
- More generally, educating and raising awareness about technical solutions and encouraging organisations to provide such user-friendly and transparent technologies to individual users – and likewise, encouraging users to utilise these technologies and to seek information and education about online privacy protection options.

At the global level

OECD member countries should reaffirm their intention to co-operate among themselves and with the other participants to implement the OECD Privacy Guidelines online in the public and private sectors. As stated by OECD Ministers in their 1998 Declaration, member countries should also

consider reassessing periodically the need for any other further action to ensure the protection of personal data at the global level.

In particular, member countries should, in the context of global electronic commerce:

- Emphasise the importance of Part Five of the 1980 Privacy Guidelines[29] related to International Co-operation, and endeavour to establish procedures to improve bilateral and multilateral mechanisms for cross-border co-operation between public enforcement agencies in the procedural and investigative matters involved or called for in the Guidelines.
- Continue to co-ordinate with the private sector and explore how recourse to public/private partnerships could help building organisations' and individual user trust online in areas where technology and regulation are closely interrelated such as online dispute resolution and privacy enhancing technologies.
- Promote co-operation with other international organisations as appropriate.
- Continue to explore ways to further online trust across all participants through appropriate outreach, education, co-operation and consultation.

Practical guidance for businesses and other organisations

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

- Develop privacy policies based on the OECD Guidelines, use the OECD Privacy Policy Statement Generator and similar mechanisms as useful tools

29. PART FIVE. INTERNATIONAL CO-OPERATION

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

21. Member countries should establish procedures to facilitate:

- information exchange related to these Guidelines, and

- mutual assistance in the procedural and investigative matters involved.

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

to assist in developing policies, and post their privacy policies on their home page.

- Evaluate whether the following self-regulatory tools are appropriate to their activities and where so, implement and adhere to them: trustmark programmes; codes of conduct; labelling systems; privacy icons or symbols; auditing whether by self-assessment or by a third-party; and effective redress mechanisms, including alternative dispute resolution.
- Work with government to develop innovative and flexible implementation models for existing or emerging regulatory and self-regulatory models to help assure that the legitimate needs for information flows are considered as well as the legitimate needs for protection of personal data.

Practical guidance for individual users and consumers

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

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

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

III. Annexes

Annex I	Guidelines on the Protection of Privacy and Transborder Flows of Personal Data	Publication, OECD, 1980. Reprinted 2002
Annex II	Ministerial Declaration on the Protection of Privacy on Global Networks	DSTI/ICCP/REG(98)10/FINAL Published with the Privacy Guidelines, 2002
Annex III	Inventory of Instruments and Mechanisms Contributing to the Implementation and Enforcement of the OECD Privacy Guidelines on Global Networks	DSTI/ICCP/REG(98)12/FINAL
Annex IV	OECD Privacy Policy Statement Generator	http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm
Annex V	Building Trust in the Online Environment: Business-to-Consumer Dispute Resolution – Report of the Conference	DSTI/ICCP/REG/CP(2001)2 Released as Unclassified
Annex VI	Legal Provisions Related to Business-to-Consumer Alternative Dispute Resolution in Relation to Privacy and Consumer Protection	DSTI/ICCP/REG/CP(2002)1/FINAL
Annex VII	Resolving E-commerce Disputes Online: Asking the Right Questions about ADR	DSTI/ICCP/REG/CP(2002)2/FINAL
Annex VIII	Report on Compliance with and Enforcement of Privacy Protection	DSTI/ICCP/REG(2002)5/FINAL
Annex IX	Inventory of Privacy Enhancing Technologies (PETs)	DSTI/ICCP/REG(2001)1/FINAL
Annex X	Report on the OECD Forum Session on Privacy Enhancing Technologies (PETs)	DSTI/ICCP/REG(2001)6/FINAL
Annex XI	Transborder Data Flow Contracts in the Wider Framework of Mechanisms for Privacy Protection on Global Networks	DSTI/ICCP/REG(99)15/FINAL

All of these annexes have been included in the OECD publication of the same name, "Privacy Online: Policy and Practical Guidance".

RECOMMENDATION OF THE COUNCIL ON CROSS-BORDER CO-OPERATION IN THE ENFORCEMENT OF LAWS PROTECTING PRIVACY (2007)

THE COUNCIL,

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

Having regard to the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [C(80)58/FINAL], which recognises that Member countries have a common interest in protecting individuals' privacy without unduly impeding transborder data flows, and states that Member countries should establish procedures to facilitate "mutual assistance in the procedural and investigative matters involved"

Having regard to the Declaration on the Protection of Privacy on Global Networks [C(98)177, Annex 1], which recognises that different effective approaches to privacy protection can work together to achieve effective privacy protection on global networks and states that Member countries will take steps to "ensure that effective enforcement mechanisms" are available both to address non-compliance with privacy principles and to ensure access to redress;

Having regard to the Recommendation of the Council concerning Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders [C(2003)116] and the Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws against Spam [C(2006)57], which set forth principles for international law enforcement co-operation in combating cross-border fraud and deception and illegal spam, respectively, and which illustrate how cross-border co operation among Member countries can be improved;

Recognising the benefits in terms of business efficiency and user convenience that the increase in transborder flows of data has brought to organisations and individuals;

Recognising that the increase in these flows, which include personal data, has also raised new challenges and concerns with respect to the protection of privacy;

Recognising that, while there are differences in their laws and enforcement mechanisms, Member countries share an interest in fostering closer international co-operation among their privacy law enforcement authorities as a means of better safeguarding personal data and minimising disruptions to transborder data flows;

Recognising that, although there are regional instruments and other arrangements under which such co-operation will continue to take place, a more global and comprehensive approach to this co-operation is desirable;

On the proposal of the Committee for Information, Computer and Communications Policy:

RECOMMENDS:

That Member countries co-operate across borders in the enforcement of laws protecting privacy, taking appropriate steps to:

- Improve their domestic frameworks for privacy law enforcement to better enable their authorities to co-operate with foreign authorities.

- Develop effective international mechanisms to facilitate cross-border privacy law enforcement co-operation.

- Provide mutual assistance to one another in the enforcement of laws protecting privacy, including through notification, complaint referral, investigative assistance and information sharing, subject to appropriate safeguards.

- Engage relevant stakeholders in discussion and activities aimed at furthering co-operation in the enforcement of laws protecting privacy.

That Member countries implement this Recommendation, as set forth in greater detail in the Annex, of which it forms an integral part.

INVITES non-Member economies to take account of the Recommendation and collaborate with Member countries in its implementation.

INSTRUCTS the Committee for Information, Computer and Communications Policy to exchange information on progress and experiences with respect to the implementation of this Recommendation, review that information, and report to the Council within three years of its adoption and thereafter as appropriate.

Annex

I. Definitions

1. For the purposes of this Recommendation:

a. "Laws Protecting Privacy" means national laws or regulations, the enforcement of which has the effect of protecting personal data consistent with the OECD Privacy Guidelines.

b. "Privacy Enforcement Authority" means any public body, as determined by each Member country, that is responsible for enforcing Laws Protecting Privacy, and that has powers to conduct investigations or pursue enforcement proceedings.

II. Objectives and scope

2. This Recommendation is intended to foster international co-operation among Privacy Enforcement Authorities to address the challenges of protecting the personal information of individuals wherever the information or individuals may be located. It reflects a commitment by Member countries to improve their enforcement systems and laws where needed to increase their effectiveness in protecting privacy.

3. The main focus of this Recommendation is the authority and enforcement activity of Privacy Enforcement Authorities. However, it is recognised that other entities, such as criminal law enforcement authorities, privacy officers in public and private organisations and private sector oversight groups, also play an important role in the effective protection of privacy across borders, and appropriate co-operation with these entities is encouraged.

4. Given that cross-border co-operation can be complex and resource-intensive, this Recommendation is focused on co-operation with respect to those violations of Laws Protecting Privacy that are most serious in nature. Important factors to consider include the nature of the violation, the magnitude of the harms or risks as well as the number of individuals affected.

5. Although this Recommendation is primarily aimed at facilitating co-operation in the enforcement of Laws Protecting Privacy governing the private sector, Member countries may also wish to co-operate on matters involving the processing of personal data in the public sector.

6. This Recommendation is not intended to interfere with governmental activities relating to national sovereignty, national security, and public policy ("ordre public").

III. Domestic measures to enable co-operation

7. In order to improve cross-border co-operation in the enforcement of Laws Protecting Privacy, Member countries should work to develop and maintain effective domestic measures that enable Privacy Enforcement Authorities to co-operate effectively both with foreign and other domestic Privacy Enforcement Authorities.

8. Member countries should review as needed, and where appropriate adjust, their domestic frameworks to ensure their effectiveness for cross-border co-operation in the enforcement of Laws Protecting Privacy.

9. Member countries should consider ways to improve remedies, including redress where appropriate, available to individuals who suffer harm from actions that violate Laws Protecting Privacy wherever they may be located.

10. Member countries should consider how, in cases of mutual concern, their own Privacy Enforcement Authorities might use evidence, judgments, and enforceable orders obtained by a Privacy Enforcement Authority in another country to improve their ability to address the same or related conduct in their own countries.

A. Providing effective powers and authority

11. Member countries should take steps to ensure that Privacy Enforcement Authorities have the necessary authority to prevent and act in a timely manner against violations of Laws Protecting Privacy that are committed from their territory or cause effects in their territory. In particular, such authority should include effective measures to:

a. Deter and sanction violations of Laws Protecting Privacy;
b. Permit effective investigations, including the ability to obtain access to relevant information, relating to possible violations of Laws Protecting Privacy;
c. Permit corrective action to be taken against data controllers engaged in violations of Laws Protecting Privacy.

B. Improving the ability to co-operate

12. Member countries should take steps to improve the ability of their Privacy Enforcement Authorities to co-operate, upon request and subject to appropriate safeguards, with foreign Privacy Enforcement Authorities, including by:

a. Providing their Privacy Enforcement Authorities with mechanisms to share relevant information with foreign authorities relating to possible violations of Laws Protecting Privacy;
b. Enabling their Privacy Enforcement Authorities to provide assistance to foreign authorities relating to possible violations of

their Laws Protecting Privacy, in particular with regard to obtaining information from persons; obtaining documents or records; or locating or identifying organisations or persons involved or things.

IV. International co-operation

13. Member countries and their Privacy Enforcement Authorities should co-operate with each other, consistent with the provisions of this Recommendation and national law, to address cross-border aspects arising out of the enforcement of Laws Protecting Privacy. Such co-operation may be facilitated by appropriate bilateral or multilateral enforcement arrangements.

A. Mutual assistance

14. Privacy Enforcement Authorities requesting assistance from Privacy Enforcement Authorities in other Member countries in procedural, investigative and other matters involved in the enforcement of Laws Protecting Privacy across borders should take the following into account:

a. Requests for assistance should include sufficient information for the requested Privacy Enforcement Authority to take action. Such information may include a description of the facts underlying the request and the type of assistance sought, as well as an indication of any special precautions that should be taken in the course of fulfilling the request.
b. Requests for assistance should specify the purpose for which the information requested will be used.
c. Prior to requesting assistance, a Privacy Enforcement Authority should perform a preliminary inquiry to ensure that the request is consistent with the scope of this Recommendation and does not impose an excessive burden on the requested Privacy Enforcement Authority.

15. The requested Privacy Enforcement Authority may exercise its discretion to decline the request for assistance, or limit or condition its co-operation, in particular where it is outside the scope of this Recommendation, or more generally where it would be inconsistent with domestic laws, or important interests or priorities. The reasons for declining or limiting assistance should be communicated to the requesting authority.

16. Privacy Enforcement Authorities requesting and receiving assistance on enforcement matters should communicate with each other about matters that may assist ongoing investigations.

17. Privacy Enforcement Authorities should, as appropriate, refer complaints or provide notice of possible violations of the Laws Protecting

Privacy of other Member countries to the relevant Privacy Enforcement Authority.

18. In providing mutual assistance, Privacy Enforcement Authorities should:

a. Refrain from using non-public information obtained from another Privacy Enforcement Authority for purposes other than those specified in the request for assistance;
b. Take appropriate steps to maintain the confidentiality of non-public information exchanged and respect any safeguards requested by the Privacy Enforcement Authority that provided the information;
c. Co-ordinate their investigations and enforcement activity with that of Privacy Enforcement Authorities in other member countries to promote more effective enforcement and avoid interference with ongoing investigations;
d. Use their best efforts to resolve any disagreements related to co-operation that may arise.

B. Engaging in collective initiatives to support mutual assistance

19. Member countries should designate a national contact point for co-operation and mutual assistance under this Recommendation and provide this information to the OECD Secretary-General. The designation of the contact point is intended to complement rather than replace other channels for co-operation. Updated information regarding Laws Protecting Privacy should also be provided to the OECD Secretary-General, who will maintain a record of information about the laws and contact points for the benefit of all Member countries.

20. Privacy Enforcement Authorities should share information on enforcement outcomes to improve their collective understanding of how privacy law enforcement is conducted.

21. Member countries should foster the establishment of an informal network of Privacy Enforcement Authorities and other appropriate stakeholders to discuss the practical aspects of privacy law enforcement co-operation, share best practices in addressing cross-border challenges, work to develop shared enforcement priorities, and support joint enforcement initiatives and awareness raising campaigns.

C. Co-operating with other authorities and stakeholders

22. Member countries should encourage Privacy Enforcement Authorities to consult with:

a. Criminal law enforcement authorities to identify how best to co-operate in relation to privacy matters of a criminal nature for the purpose of protecting privacy across borders most effectively;

b. Privacy officers in public and private organisations and private sector oversight groups on how they could help resolve privacy-related complaints at an early stage with maximum ease and effectiveness;
c. Civil society and business on their respective roles in facilitating cross-border enforcement of Laws Protecting Privacy, and in particular in helping raise awareness among individuals on how to submit complaints and obtain remedies, with special attention to the cross-border context.

INFORMATION SECURITY

RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS - TOWARDS A CULTURE OF SECURITY (2002)

THE COUNCIL,

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

Having regard to the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 [C(80)58(Final)];

Having regard to the Declaration on Transborder Data Flows adopted by the Governments of OECD Member countries on 11 April 1985 [Annex to C(85)139];

Having regard to the Recommendation of the Council concerning Guidelines for Cryptography Policy of 27 March 1997 [C(97)62/FINAL];

Having regard to the Ministerial Declaration on the Protection of Privacy on Global Networks of 7-9 December 1998 [Annex to C(98)177/FINAL];

Having regard to the Ministerial Declaration on Authentication for Electronic Commerce of 7-9 December 1998 [Annex to C(98)177/FINAL];

Recognising that information systems and networks are of increasing use and value to governments, businesses, other organisations and individual users;

Recognising that the increasingly significant role of information systems and networks, and the growing dependence on them for stable and efficient national economies and international trade and in social, cultural and political life call for special efforts to protect and foster confidence in them;

Recognising that information systems and networks and their worldwide proliferation have been accompanied by new and increasing risks;

Recognising that data and information stored on and transmitted over information systems and networks are subject to threats from various means of unauthorised access, use, misappropriation, alteration, malicious code transmissions, denial of service or destruction and require appropriate safeguards;

Recognising that there is a need to raise awareness of risks to information systems and networks and of the policies, practices, measures and procedures available to respond to those risks, and to encourage appropriate behaviour as a crucial step towards the development of a culture of security;

Recognising that there is a need to review current policies, practices, measures, and procedures to help assure that they meet the evolving challenges posed by threats to information systems and networks;

Recognising that there is a common interest in promoting the security of information systems and networks by means of a culture of security that fosters international co-ordination and co-operation to meet the challenges posed by the potential harm from security failures to national economies, international trade and participation in social, cultural and political life;

And further recognising that the Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security set out in the Annex to this Recommendation are voluntary and do not affect the sovereign rights of nations;

And recognising that these Guidelines are not meant to suggest that any one solution exists for security or what policies, practices, measures and procedures are appropriate to any particular situation, but rather to provide a framework of principles to promote better understanding of how participants may both benefit from, and contribute to, the development of a culture of security;

COMMENDS these Guidelines for the Security of the Information Systems and Networks: Towards a Culture of Security to governments, businesses, other organisations and individual users who develop, own, provide, manage, service, and use information systems and networks;

RECOMMENDS that Member countries:

Establish new, or amend existing, policies, practices, measures and procedures to reflect and take into account the Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security by adopting and promoting a culture of security as set out in the Guidelines;

Consult, co-ordinate and co-operate at national and international levels to implement the Guidelines;

Disseminate the Guidelines throughout the public and private sectors, including to governments, business, other organisations, and individual users to promote a culture of security, and to encourage all concerned parties to be responsible and to take necessary steps to implement the Guidelines in a manner appropriate to their individual roles;

Make the Guidelines available to non-member countries in a timely and appropriate manner;

Review the Guidelines every five years so as to foster international co-operation on issues relating to the security of information systems and networks;

INSTRUCTS the OECD Committee for Information, Computer and Communication Policy to promote the implementation of the Guidelines.

This Recommendation replaces the Recommendation of the Council concerning Guidelines for the Security of Information Systems of 26 November 1992 [C(92)188/FINAL].

Annex
Guidelines for the Security of Information Systems and Networks towards a Culture of Security

Preface

1. The use of information systems and networks and the entire information technology environment have changed dramatically since 1992 when the OECD first put forward the Guidelines for the Security of Information Systems. These continuing changes offer significant advantages but also require a much greater emphasis on security by governments, businesses, other organisations and individual users who develop, own, provide, manage, service, and use information systems and networks ("participants").

2. Ever more powerful personal computers, converging technologies and the widespread use of the Internet have replaced what were modest, stand-alone systems in predominantly closed networks. Today, participants are increasingly interconnected and the connections cross national borders. In addition, the Internet supports critical infrastructures such as energy, transportation and finance and plays a major part in how companies do business, how governments provide services to citizens and enterprises and how individual citizens communicate and exchange information. The nature and type of technologies that constitute the communications and information infrastructure also have changed significantly. The number and nature of infrastructure access devices have multiplied to include fixed, wireless and mobile devices and a growing percentage of access is through "always on" connections. Consequently, the nature, volume and sensitivity of information that is exchanged has expanded substantially.

3. As a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities. This raises new issues for security. For these reasons, these Guidelines apply to all participants in the new information society and suggest the need for a greater awareness and understanding of security issues and the need to develop a "culture of security".

4. These Guidelines respond to an ever changing security environment by promoting the development of a culture of security that is, a focus on security in the development of information systems and networks and the adoption of new ways of thinking and behaving when using and interacting within information systems and networks. The Guidelines signal a clear

break with a time when secure design and use of networks and systems were too often afterthoughts. Participants are becoming more dependent on information systems, networks and related services, all of which need to be reliable and secure. Only an approach that takes due account of the interests of all participants, and the nature of the systems, networks and related services, can provide effective security.

5. Each participant is an important actor for ensuring security. Participants, as appropriate to their roles, should be aware of the relevant security risks and preventive measures, assume responsibility and take steps to enhance the security of information systems and networks.

6. Promotion of a culture of security will require both leadership and extensive participation and should result in a heightened priority for security planning and management, as well as an understanding of the need for security among all participants. Security issues should be topics of concern and responsibility at all levels of government and business and for all participants. These Guidelines constitute a foundation for work towards a culture of security throughout society. This will enable participants to factor security into the design and use of all information systems and networks. They propose that all participants adopt and promote a culture of security as a way of thinking about, assessing, and acting on, the operations of information systems and networks.

I. Aims

7. These Guidelines aim to:

- Promote a culture of security among all participants as a means of protecting information systems and networks.

- Raise awareness about the risk to information systems and networks; the policies, practices, measures and procedures available to address those risks; and the need for their adoption and implementation.

- Foster greater confidence among all participants in information systems and networks and the way in which they are provided and used.

- Create a general frame of reference that will help participants understand security issues and respect ethical values in the development and implementation of coherent policies, practices, measures and procedures for the security of information systems and networks.

- Promote co-operation and information sharing, as appropriate, among all participants in the development and implementation of security policies, practices, measures and procedures.

- Promote the consideration of security as an important objective among all participants involved in the development or implementation of standards.

II. Principles

8. The following nine principles are complementary and should be read as a whole. They concern participants at all levels, including policy and operational levels. Under these Guidelines, the responsibilities of participants vary according to their roles. All participants will be aided by awareness, education, information sharing and training that can lead to adoption of better security understanding and practices. Efforts to enhance the security of information systems and networks should be consistent with the values of a democratic society, particularly the need for an open and free flow of information and basic concerns for personal privacy1.

1) Awareness

Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

Awareness of the risks and available safeguards is the first line of defence for the security of information systems and networks. Information systems and networks can be affected by both internal and external risks. Participants should understand that security failures may significantly harm systems and networks under their control. They should also be aware of the potential harm to others arising from interconnectivity and interdependency. Participants should be aware of the configuration of, and available updates for, their system, its place within networks, good practices that they can implement to enhance security, and the needs of other participants.

2) Responsibility

All participants are responsible for the security of information systems and networks.

Participants depend upon interconnected local and global information systems and networks and should understand their responsibility for the security of those information systems and networks. They should be

1. In addition to these Security Guidelines, the OECD has developed complementary recommendations concerning guidelines on other issues important to the world's information society. They relate to privacy (the 1980 OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data) and cryptography (the 1997 OECD Guidelines for Cryptography Policy). These Security Guidelines should be read in conjunction with them.

accountable in a manner appropriate to their individual roles. Participants should review their own policies, practices, measures, and procedures regularly and assess whether these are appropriate to their environment. Those who develop, design and supply products and services should address system and network security and distribute appropriate information including updates in a timely manner so that users are better able to understand the security functionality of products and services and their responsibilities related to security.

3) Response

Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.

Recognising the interconnectivity of information systems and networks and the potential for rapid and widespread damage, participants should act in a timely and co-operative manner to address security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective co-operation to prevent, detect and respond to security incidents. Where permissible, this may involve cross-border information sharing and co-operation.

4) Ethics

Participants should respect the legitimate interests of others.

Given the pervasiveness of information systems and networks in our societies, participants need to recognise that their action or inaction may harm others. Ethical conduct is therefore crucial and participants should strive to develop and adopt best practices and to promote conduct that recognises security needs and respects the legitimate interests of others.

5) Democracy

The security of information systems and networks should be compatible with essential values of a democratic society.

Security should be implemented in a manner consistent with the values recognised by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency.

6) Risk assessment

Participants should conduct risk assessments.

Risk assessment identifies threats and vulnerabilities and should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications. Risk assessment will allow determination of the acceptable level of risk and assist the selection of appropriate controls to manage the risk of potential harm to information systems and networks in light of the nature and importance of the information to be protected. Because of the growing interconnectivity of information systems, risk assessment should include consideration of the potential harm that may originate from others or be caused to others.

7) Security design and implementation

Participants should incorporate security as an essential element of information systems and networks.

Systems, networks and policies need to be properly designed, implemented and co-ordinated to optimise security. A major, but not exclusive, focus of this effort is the design and adoption of appropriate safeguards and solutions to avoid or limit potential harm from identified threats and vulnerabilities. Both technical and non-technical safeguards and solutions are required and should be proportionate to the value of the information on the organisation's systems and networks. Security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. For end users, security design and implementation consists largely of selecting and configuring products and services for their system.

8) Security management

Participants should adopt a comprehensive approach to security management.

Security management should be based on risk assessment and should be dynamic, encompassing all levels of participants¡¦ activities and all aspects of their operations. It should include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit. Information system and network security policies, practices, measures and procedures should be co-ordinated and integrated to create a coherent system of security. The requirements of security management depend upon the level of involvement, the role of the participant, the risk involved and system requirements.

9) Reassessment

Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

New and changing threats and vulnerabilities are continuously discovered. Participants should continually review, reassess and modify all aspects of security to deal with these evolving risks.

RECOMMENDATION OF THE COUNCIL ON PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURES (2008)

THE COUNCIL

Having regard to Article 5 b) of the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960;

Having regard to the Recommendation of the Council concerning Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security [C(2002)131], hereinafter the "Security Guidelines"

Having regard to the Resolution 58/199 adopted by the General Assembly of the United Nations on the creation of a global culture of cybersecurity and the protection of critical information infrastructures;

Recognising that the functioning of our economies and societies increasingly relies on information systems and networks that are interconnected and interdependent, domestically and across borders; that a number of those systems and networks are of national critical importance; and that their protection is a priority area for national policy and international cooperation;

Recognising that in order to improve the protection of domestic and cross-border critical information infrastructures, Member countries need to share their knowledge and experience in developing policies and practices and cooperate more closely between themselves as well as with non Member economies;

Recognising that the protection of critical information infrastructures requires coordination domestically and across borders with the private sector owners and operators of such infrastructures, hereinafter the "private sector"

On the proposal of the Committee for Information, Computer and Communication Policy:

AGREES that:

For the purposes of this Recommendation, critical information infrastructures, hereinafter "CII", should be understood as referring to those interconnected information systems and networks, the disruption or

destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy;

National CII are identified through a risk assessment process and typically include one or more of the following:

- Information components supporting critical infrastructures, and/or.
- Information infrastructures supporting essential components of government business; and/or
- Information infrastructures essential to the national economy.

RECOMMENDS that:

Member countries introduce and maintain an effective framework to implement the OECD Security Guidelines in relation to the protection of CII, taking into account the specific policy and operational guidance set out herein;

PART I. Protection of critical information infrastructures at the domestic level

Member countries should:

Demonstrate government leadership and commitment to protect CII by:

- Adopting clear policy objectives at the highest level of government.
- Identifying government agencies and organisations with responsibility and authority to implement these policy objectives.
- Consulting with private sector owners and operators of CII to establish mutual cooperation for the implementation of these objectives.
- Ensuring transparency on the delegations of responsibility to government authorities and agencies to facilitate closer co-operation within the government and with the private sector.
- Systematically reviewing policy and legal frameworks and self-regulatory schemes which may apply to CII, including those addressing cross-border threats, to assess the need to enhance their implementation, to amend them or to develop new instruments.
- Taking steps, where appropriate, to enhance the security level of components of information system and networks that constitute CII.

Manage risks to CII by:

- Developing a national strategy that gains commitment from all those concerned, including the highest levels of government and the private sector.
- Taking into consideration interdependencies.
- Conducting a risk assessment based on the analysis of vulnerabilities and the threats to the CII, in order to protect economies and societies against the impacts of highest national concern.
- Developing, on the basis of the assessment, and periodically reviewing a national risk management process that sets out the detailed organisation, tools and monitoring mechanisms required to implement the risk management strategy at every level, including:
    1. The appropriate organisational structure to provide guidelines and promote good security practices at the national level and to manage and monitor progress, as well as a complete set of processes to ensure preparedness, including prevention, protection, response and recovery from natural and malicious threats.
    2. A system of measurement to evaluate and appraise measures in place (including exercises and tests as appropriate) and allow for feedback and continuous update.
- Developing an incident response capability, such as a computer security incident response team (CERT/CSIRTs), in charge of monitoring, warning, alerting and carrying out recovery measures for CII; and mechanisms to foster closer cooperation and communications among those involved in incident response.

Work in partnership with the private sector by:

- Establishing trusted public-private partnerships with a focus on risk management, incident response and recovery.
- Enabling mutual and regular exchange of information by establishing information sharing arrangements that acknowledge the sensitivity of certain information.
- Fostering innovation through public-private research and development projects focused on the improvement of the security of CII and as appropriate, sharing these innovations across borders.

PART II. Protecting critical information infrastructures across borders

Member countries should cooperate among themselves and with the private sector at the strategy, policy and operational levels to ensure the

protection of CII against events and circumstances beyond the capacity of individual countries to address alone.

They should in particular proactively engage in bilateral and multilateral cooperation at regional and global levels with a view to:

- Share knowledge and experience with respect to the development of domestic policies and practices and to models for coordinating with private sector owners and operators of critical information infrastructures.
- Develop a common understanding of:
    1. Risk management applicable to cross-border dependencies and interdependencies.
    2. Generic vulnerabilities, threats and impacts on the CII, to facilitate collective action to address those that are widespread, such as security flaws and malicious software, as well as to improve risk management strategies and policies.
- Make available information regarding the national agencies involved in the protection of CII, their roles and responsibilities, to facilitate identification of counterparts and improve the timeliness of cross border action.
- Acknowledge the value of participation in international or regional networks for watch, warning and incident response, to enable robust information sharing and coordination at the operational level, as well as to better manage crisis in case of an incident developing across borders.
- Support cross-border collaboration for, and information sharing on, public-private research and development for the protection of CII.

INVITES:

Member countries to disseminate this Recommendation throughout the public and private sectors, including governments, businesses and other international organisations to encourage all relevant participants to take the necessary steps for the protection of CII;

Non-Member economies to take account of this Recommendation and collaborate with Member countries in its implementation;

INSTRUCTS the OECD Committee for Information, Computer and Communication Policy to:

Promote the implementation of this Recommendation and review it every five years to foster international co-operation on issues relating to the protection of CII.

ELECTRONIC AUTHENTICATION

DECLARATION ON AUTHENTICATION FOR ELECTRONIC COMMERCE (1998)

The Governments of OECD Member countries[1]:

Considering:

The significant social and economic benefits offered by information and communication technologies and electronic commerce;

The leading role of industry in developing information and communication technologies and electronic commerce;

The need for government and industry to foster user confidence to facilitate the growth of global electronic commerce;

The rapid development of authentication technologies and mechanisms, and their importance in the context of global information and communication technologies and electronic commerce; and

The potential impact that diverse national solutions for electronic authentication could have on the development of global electronic commerce.

Recognising:

That work is underway at the international level to facilitate transborder electronic transactions and the use of authentication technologies and mechanisms to foster the growth of global electronic commerce;

That transacting parties may select appropriate mechanisms which meet their needs for authentication in conducting electronic commerce, including particular authentication technologies, contractual arrangements and other means of validating electronic transactions, and that they can use judicial and other means of dispute resolution to prove the validity of those transactions;

That governments can play a role in promoting electronic commerce as a user of information and communication technologies, products and services, including electronic authentication mechanisms;

1. including the European Communities.

That technology or media specific rules for recording, storing or transmitting information (for example, certain paper-based requirements) could impede the development of electronic commerce and the use of electronic authentication mechanisms;

That, where appropriate, market-driven, rather than government imposed, standards and codes of practice can provide a useful tool for developing user confidence in global electronic commerce; and

The continuing dialogue within the OECD -- involving governments, business and industry, and user representatives -- to discuss the technologies and diverse models for authentication to facilitate global electronic commerce which are currently in use or emerging in Member countries, and in particular the ongoing work of the Organisation through its Information, Computers and Communications Policy (ICCP) Committee, to facilitate information exchange by compiling an inventory of approaches to authentication and certification and convening joint OECD-private sector workshops in the year ahead.

Declare their determination to:

Take a non-discriminatory approach to electronic authentication from other countries;

Encourage efforts to develop authentication technologies and mechanisms, and facilitate the use of those technologies and mechanisms for electronic commerce;

Amend, where appropriate, technology or media specific requirements in current laws or policies that may impede the use of information and communication technologies and electronic authentication mechanisms, giving favourable consideration to the relevant provisions of the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) in 1996;

Proceed with the application of electronic authentication technologies to enhance the delivery of government services and programmes to the public; and

Continue work at the international level, together with business, industry and user representatives, concerning authentication technologies and mechanisms to facilitate global electronic commerce.

RECOMMENDATION OF THE COUNCIL ON ELECTRONIC AUTHENTICATION (2007)

Foreword

The Recommendation on Electronic Authentication and the Guidance for Electronic Authentication have been developed by the OECD Committee for Information, Computer and Communications Policy (ICCP), through its Working Party on Information Security and Privacy (WPISP). The work has been led by Jane Hamilton from Industry Canada with the support of delegates from Australia, France, Hungary, Korea, Norway, the United States, the OECD Secretariat and the Business and Industry Advisory Committee (BIAC) to the OECD. The draft Recommendation was adopted as a Recommendation of the OECD Council on 12 June 2007. The Guidance for Electronic Authentication, was adopted by the ICCP Committee in April and declassified on 12 June 2007 by the OECD Council.

Preface

Electronic authentication provides a level of assurance as to whether someone or something is who or what it claims to be in a digital environment. Thus, electronic authentication plays a key role in the establishment of trust relationships for electronic commerce, electronic government and many other social interactions. It is also an essential component of any strategy to protect information systems and networks, financial data, personal information and other assets from unauthorised access or identity theft. Electronic authentication is therefore essential for establishing accountability online.

The importance of authentication for electronic government and global electronic commerce was recognised back in 1998 by OECD Ministers at the Ministerial Conference "A Borderless World: Realising the Potential of Global Electronic Commerce" held in Ottawa, Canada.[1] In their "Declaration on Authentication for Electronic Commerce," Ministers outlined a number of actions to promote the development and use of electronic authentication technologies and mechanisms. One important aspect included the need to develop consistent approaches to electronic authentication to facilitate cross-border electronic commerce.

The OECD has carried out several initiatives to support Member countries' efforts to implement the Ministerial Declaration. It has worked in particular to address two important challenges: increasing confidence in authentication processes and operators, and breaking down barriers to the use of authentication across borders. In 1999, a Joint OECD-Private Sector Workshop was organised to foster dialogue among all stakeholders,[2] followed in 2000 by the development of an "Inventory of Approaches to E-Authentication and Certification in a Global Networked Society"[3] and a report on "Progress Achieved in Furtherance of the Ministerial Declaration."[4] More recent work included a 2003 "Survey of Legal and

1. SG/EC(98)14/FINAL
www.olis.oecd.org/olis/1998doc.nsf/linkto/sg-ec(98)14-final

2. DSTI/ICCP/REG(99)14/FINAL
www.olis.oecd.org/olis/1999doc.nsf/linkto/dsti-iccp-reg(99)14-final

3. DSTI/ICCP/REG(99)13/FINAL
www.olis.oecd.org/olis/1999doc.nsf/linkto/dsti-iccp-reg(99)13-final

4. DSTI/ICCP/REG(2001)10/FINAL
www.olis.oecd.org/olis/2001doc.nsf/linkto/dsti-iccp-reg(2001)10-final

Policy Frameworks for E-Authentication and E-Signatures"[5] and a report on the "Use of Authentication across Borders"[6] completed in 2005.

In 2006, building on this work, the ICCP Working Party on Information Security and Privacy (WPISP) prepared a document providing policy and practical guidance for the development, implementation and use of electronic authentication products and services as they relate to the authentication of persons and entities.

The Guidance sets out the context and importance of electronic authentication for electronic commerce and electronic government and provides a number of foundation and operational principles that constitute a common denominator for cross-jurisdictional interoperability. It aims to help Member countries and non-Member economies establish or, as appropriate, amend their approaches to electronic authentication with a view to facilitate cross-border co-operation. The Guidance takes account of work undertaken in other fora, particularly the Asia-Pacific Economic Co-operation's (APEC) work on requirements for cross-jurisdictional authentication services. Selected national approaches to authentication have also been used as an additional input.

The Guidance document served as the basis for the OECD Council Recommendation on electronic authentication which reaffirms the important role of electronic authentication in fostering trust online and the continued development of the digital economy. The Recommendation encourages efforts by Member countries to establish compatible, technology-neutral approaches for effective domestic and cross-border electronic authentication of persons and entities.

Both the Recommendation and the Guidance conclude a work stream initiated in response to the "Declaration on Authentication for Electronic Commerce" adopted by Ministers at the Ottawa Ministerial Conference held on 7-9 October 1998 and serve as a bridge to future OECD work on identity management.

It is anticipated that they will also inform ongoing and future discussions in other international forums such as the Asia Pacific Economic Cooperation (APEC), the United Nations Commission on International Trade Law (UNCITRAL) and national and regional standards organisations.

5. DSTI/ICCP/REG(2003)9/FINAL
www.olis.oecd.org/olis/2003doc.nsf/LinkTo/dsti-iccp-reg(2003)9-final

6. DSTI/ICCP/REG(2005)4/FINAL
www.olis.oecd.org/olis/2005doc.nsf/LinkTo/dsti-iccp-reg(2005)4-final

Recommendation of the Council on Electronic Authentication

THE COUNCIL,

Having regard to Article 5 b) of the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960;

Having regard to Rule 18 b) of the Rules of Procedure;

Having regard to the Declaration on Authentication for Electronic Commerce [C(98)177];

Having regard to the Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security [C(2002)131/FINAL] hereinafter the "Guidelines for the Security of Information Systems and Networks";

Having regard to the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [C(80)58/FINAL];

Recognising that trust is a key condition for many online transactions to take place, and that, within a broader system of measures and strategies, electronic authentication of persons and entities plays an important role in this respect;

Recognising that electronic authentication, which is an essential component of the verification and management of identities online, provides a level of assurance as to whether the other party is who or what it claims to be; and thereby reduces the uncertainty inherent in domestic and cross-border electronic interactions and transactions;

Recognising that effective electronic authentication helps to strengthen systems and network security, as well as privacy by reducing risks such as unauthorised access to personal data, identity theft and data breaches, and by providing additional means of accountability;

Recognising that electronic authentication is an important element in the continued development of governmental and other social and individual activities online, enables the creation of new business opportunities, contributes to the development of electronic commerce, and is a key component of a viable and sustainable Internet;

Recognising finally, that this Recommendation addresses electronic authentication of persons and entities, but does not address other aspects of electronic authentication, such as legal assurance of validity of documents or electronic signatures;

On the proposal of the Committee for Information, Computer and Communications Policy:

RECOMMENDS that Member countries:

- Work towards establishing technology-neutral approaches for effective domestic and cross-border electronic authentication of persons and entities, consistent with the OECD Guidelines for the Security of Information Systems and Networks and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

- Foster the development, provision and use of electronic authentication products and services that embody sound business practices, including technical and non technical safeguards to meet the participants' needs, in particular with respect to security and privacy of their information and identity.

- In both the private and public sectors, encourage business and legal compatibility and technical interoperability of authentication schemas, to facilitate cross-sectoral and cross-jurisdictional online interactions and transactions and to ensure that authentication products and services can be deployed at both national and international levels.

- Take steps to raise the awareness of all participants, including those in non-Member economies, on the benefits of the use of electronic authentication at national and international levels

RECALLS the Guidance on Electronic Authentication which may assist Member countries in developing effective and compatible approaches to electronic authentication, both at the national and international levels.

INVITES non-Member economies to take account of this Recommendation.

INSTRUCTS the Committee for Information, Computer and Communications Policy to monitor developments connected with electronic authentication in OECD Member countries and other international forums, and review this Recommendation within three years of its adoption and thereafter as appropriate.

OECD GUIDANCE FOR ELECTRONIC AUTHENTICATION (2007)

Introduction

Authentication encompasses a very broad range of things. The work of the OECD however, has focussed on the authentication of persons (natural and legal). OECD began its work on authentication as part of its leading work on electronic commerce. Early on, the OECD recognised that electronic commerce transcends time and geography/location, and sometimes lacked human engagement. As such, the need to properly identify parties to a transaction was seen as essential to building trust in electronic commerce. Today, these issues can be viewed as part of the broader topic of identity management that becomes an essential element of functioning in a digital economy and information society.

Purpose of this guidance

This guidance document:

- Sets out the context and importance of authentication.
- Defines a set of Principles that provide a framework for the development, implementation and use of authentication products and services as they relate to the authentication of persons and entities. The principles also address cross-border authentication challenges.
- Identifies continuing issues associated with the use of authentication.

The guidance will be useful to OECD Member and non-Member countries in establishing their approaches to authentication and assist those with existing policies to identify and address potential amendments to their approach. While it is understood that Member countries need to comply with the legal provisions in their jurisdiction, the guidance offers a common denominator that opens possibilities for cross-jurisdictional inter-operability.

In addition to offering guidance on electronic authentication that can be referenced by OECD Member countries and non-Member economies, the document also functions as an inventory of instruments and mechanisms that contributed to the work and findings of the WPISP in this area. On this basis, in addition to being a useful tool for individual jurisdictions, it

also has utility for ongoing and future discussions in international fora such as APEC's Telecommunications and Information Working Group and Electronic Commerce Steering Group, UNCITRAL and national, regional and international standards organisations among others.

Finally, and while the main purpose of the document is to provide policy and practical guidance for authentication based on OECD work that has been completed to date, it identifies those outstanding issues that the OECD considers should still be addressed, by Member countries and other international fora.

On this basis, this document:

- Ties together some of the results of OECD work to date on authentication.
- Provides a general set of guidance on some of the more complex issues associated with authentication.
- Highlights where further work may be appropriate by OECD or other bodies.

Authentication in context

Authentication can mean a variety of things depending on the context in which the term is used. An Internet search on the term "authentication" yields a very broad range of definitions, some addressing authentication of persons or other entities, others addressing things, documents and systems. Across these definitions, authentication is accomplished through processes that have various degrees of detail and technical specificity. These processes are aimed at determining whether someone or something is, in fact, who or what it claims to be. As such, effective authentication is a key contributor to the establishment of a trust relationship in a digital environment. For the purposes of this guidance, authentication is defined as:

A function for establishing the validity and assurance of a claimed identity of a user, device or another entity in an information or communications system.

This definition implies two processes and one result:

- A claim related to a person, other entity or thing is presented (claiming process).
- That claim is substantiated (substantiation process).
- As a result, a degree of confidence, or lack thereof, in the claim is generated.

Authentication is not an end, but rather a sub-process in a security system that must work in conjunction with authorisations, rights management, access control and audit processes. Authentication is dependent on substantiating one or more of the following factors: something the claimant knows (*e.g.* a shared secret such as a password), something the claimant has (*e.g.* a token) and something the claimant is (*e.g.* a biometric or set of attributes like height, age and weight). Once a person, other entity or thing has been authenticated (*e.g.* the claim is valid as stated), a variety of things can be enabled. For example, in the case of authenticating an individual, certain rights may be provided to that authenticated individual (authorisation process), along with the responsibilities that may be associated with exercising those rights. Authentication may be bi-directional and offer assurances[1] for both parties to a transaction.

Most often, in the case of authenticating a person, the interest lies in authenticating the person's identity. However, there are circumstances where the interest rests in authenticating an attribute related to a person rather than their identity. For example, in certain online transactions, authentication is employed to ensure that Web site visitors are above a certain age prescribed by law. In such cases, the attribute – age (something the customer is), is the main point of the authentication. It is therefore possible to use electronic authentication technologies to authenticate attributes without providing information on identity.

Providing a degree of anonymity can also play an important role to help build trust in online systems. Authentication technologies that do not collect personal information can ensure that information that is not necessary for the transaction in the first place is not collected or used for another purpose in the future. Simply not using authentication at all when it is not needed is another way of contributing to user trust.

While document authentication has long existed through notarisation and its antecedents, new forms of electronic document authentication are also being developed. In the physical world, this may require the presence of the person and the presentation of a credential with both a signature and a photograph. In the online environment, there are a variety of new means of creating digital credentials. Such credentials may be used to authenticate persons (or entities) and they may enable electronic "signing" of documents. The use of electronic signatures for producing legal effect equivalent to handwritten signatures raises several issues which are addressed by the UNCITRAL 2001 Model Law on Electronic Signatures. OECD Member countries support the use of electronic signatures as equivalent to handwritten signatures and advocate technology neutrality in their use.

Even more complexity exists where an automated set of software agents and authentication of systems or machines is introduced. Many legal

1. See Appendix B Authentication Assurance Levels.

concepts are predicated on intent between human actors. This then begs the question of how to convey intent and apportion obligation upon transactions that are not human mediated.

In digital environments, authentication raises other complex issues and a range of challenges. Some of the issues relate to how identity is defined and captured in a way that promotes trust in a virtual environment where every aspect needs to be formalised in order to allow for automated processing. While in many respects these issues are the same as in the physical world, the increased level of ambiguity, coupled with serious security threats in the online environment introduces new complexities that must be addressed. The challenges can be considered technological (*e.g.* interoperability, security), legal (*e.g.* legal recognition, liability, privacy) and economic (*e.g.* cost of deployment and of use). There may be significant variance across sectoral implementations which also serve to increase complexity. These challenges are made more difficult by the scale and speed of technological innovations.

A further challenge is the fact that approaches to authentication have emerged on a sectoral or an application-by-application (or service) and proprietary basis. In order to capture some of the economies of scale which may be essential to the economic viability of authentication service providers, commonality among applications needs to be identified. These challenges illustrate the need to adopt a more comprehensive and holistic approach to trust and confidence concerns and to explore secure, privacy enhancing, efficient and convenient approaches to managing identities online in order to realise the full benefits of the online environment. It is hoped that future OECD work on identity management will facilitate the resolution of some of the issues which have been mentioned above, such as this sectoral, or "silo", approach to authentication.

Authentication mechanisms need to be continually upgraded to keep ahead of new forms of fraud (*e.g.* attackers steal credentials and use them to perpetrate fraud or other crimes). It is therefore desirable for authentication methods to be implemented with the ability to leverage more robust authentication technologies in the future. The growing use of multi-factor authentication, as well as the use of biometrics (*e.g.* iris scanning or finger printing), is an example of this trend.

Viable business models for authentication services are a prerequisite for sustainable development and use of new authentication methods. Such models need to take into account the specific characteristics of the

authentication marketplace, where network effects[2] and two-sided market effects[3] are paramount.

It is important to understand the broad complexity of the issues surrounding authentication; both in terms of interrelation with other systems and procedures as well as the variety of uses that may be possible. This broad set of topics has been introduced with the intention of providing some context to this guidance. However, the scope of the principles offered is limited to aspects that flow from OECD work to date on authentication which addressed two of the major challenges of authentication: the confidence in authentication processes and operators, and the challenges relying parties can encounter across borders. To the extent that authentication is a basic component of any identity management process or system, the principles below establish a "bridge" between the OECD authentication work that has now reached a certain degree of maturity and the nascent work on the more general topic of identity management. The history of this work since the "Declaration on Authentication for Electronic Commerce", and a summary of the surveys, reports and workshops that have been carried out by the OECD have been summarised in Appendix A. The list of OECD documents related to authentication since 1998 can be found in the References section at the end of this document.

Importance of authentication

Businesses, governments and individuals all have sensitive data and assets to protect. Assurance is needed in particular in case of monetary transfers, when legally binding declarations are made or when transactions result in disclosure of personal information. By providing a level of assurance regarding the identity claimed by parties engaged in an online relationship, authentication reduces uncertainty inherent in transactions at a distance, thus fostering trust in electronic interactions, and participates to the broader fight against online threats and criminal activities.

Authentication is an element of a wider system of practices, procedures and technical implementations, that work together to secure information systems, networks and the electronic communications they support. The *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*[4] recognise the inter-related, inter-

2. Meaning that the usefulness of a given product increases with the number of participants using the product (e.g. the fax machine).

3. Meaning that the authentication market consists of at least two types of products/services that are complementary (i.e. authentication credentials/services and the applications using them). Both are needed for the market to function.

4. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html.

dependent nature of these systems and emphasise the need to take a comprehensive and coherent approach to system security if organisational security goals are to be met, policies implemented and a culture of security achieved. Given that authentication forms the basis for most types of access control and for establishing accountability online, it should be viewed as critical building block of information security. In addition, effective authentication contributes to the protection of privacy by contributing to the reduction of risks such as unauthorised access to personal information and identity theft.

More broadly, authentication is a critical tool in achieving trust and online identity protection, which are essential to foster e-commerce and e-government.

Principles for electronic authentication

The Principles contained in this document are intended to ensure that authentication products and services embody sound business and market practices, meet the needs of users, aim to achieve interoperability to the extent possible, and are accepted internationally. They function as benchmarks for the development, provision and use of authentication services operating at both the national and international levels. On this basis, the Principles aim to facilitate cross-border electronic communications.

These Principles have been developed with a view towards establishing a consistent approach to evaluating risks inherent in e-transactions and a basis for comparison of mechanisms based on widely different technologies. On this basis, the Principles are intended to promote the compatibility of different authentication schemas. OECD Member countries are encouraged to take the Principles into consideration in their national approaches to electronic authentication. The Principles can also form the basis for voluntary initiatives that are tailored to the requirements of specific industries.

Important points about the principles

These Principles identify the functions and responsibilities of participants in authentication systems and provide a framework within which to assess and manage the risks that accompany these responsibilities. The Principles also identify security, privacy, disclosure and complaint-handling matters that need to be taken into account in each stage of the design, development, implementation and assessment of an authentication process.

The Principles are intended to apply to authentication processes used in connection with electronic communications that take place between businesses or governments and other organisations (B2B, B2G and G2G),

between organisations and individuals (consumers or citizens – B2C, G2C) and between individuals (C2C).

A range of technical, legal, contractual and commercial relationships can exist between providers of authentication services and users of those services. Many of these relationships are governed by agreements. The Principles contained in this document are intended to guide the development of these agreements and to apply to the full range of relationships.

The provisions in the various Principles are inter-related and inter-dependent. On this basis, it would be difficult for them to achieve their purpose if they are implemented selectively. Those applying the Principles to define or implement authentication processes are encouraged to exceed the benchmarks that the Principles establish and to expand upon them to address the requirements of their particular security environment or application.

The Principles are expressed at a high level of generality and technological neutrality. A wide variety of authentication technologies and techniques is available and choices should be governed by the nature of the particular communication and the requirements of the participants. The implementation of authentication processes also differs, depending on the business or legal objectives to be met, as well as the characteristics of the environment in which electronic communication takes place, such as security and privacy needs and other legislative or regulatory obligations. These factors define the functionality required of an authentication process and, in some cases, even the type of authentication to be used. Choices will also depend on the degree of deployment of various types of authentication solutions *(i.e.* what solutions or credentials are already present).

The Principles contemplate authentication in its broadest sense but:

- Do not contemplate the authentication of documents.

- Do not include device or domain-level authentication but do have linkages to elements of the Anti-Spam Toolkit developed by the OECD Spam Task Force[5] (*e.g.* authentication applications aimed at reducing spam and harmful e-mail).

- Do not include "authorisation" (which is a separate but related process that refers to verifying the person's or organisation's authority to conduct specified transactions). Typically, decisions concerning authorisation are the purview of the relying party (*i.e.* the entity or person that is relying on the identity assertion to make the authorisation decision).

5. Cf. "OECD anti-spam Toolkit", www.oecd-antispam.org.

- Do not address electronic signatures per se (or digital signatures where the authentication is tightly bound to the signed object).

On this basis, it is possible that aspects of authentication, or subjects beyond the scope of these Principles may need to be explored and complementary policy tools developed (by the OECD and other fora) to ensure that the needs of specific users and applications are adequately addressed.

The authentication environment is dynamic and the technologies used will continue to evolve. Although every effort has been made to define Principles that can encompass foreseeable developments, they are open to revision as needed to take into account significant technological advances, changes in market characteristics, and international developments.

Concepts and terminology

These Principles relate to the authentication of electronic communication in its broadest sense. Therefore, the concepts and terms used relate to all participants, actions and techniques comprising all aspects of authentication, whether considered from the technical, legal or business perspective. Each concept or term relates to the others; none should be considered in isolation.

In developing the following, existing definitions were considered, particularly those created by international standards groups such as the International Organization for Standardization (ISO). However, the broad scope of this guidance and its policy orientation resulted in definitions that may not correspond to similar terms used elsewhere in specific contexts or at a technical level.

- **Authentication:** A function for establishing the validity and assurance of a claimed identity of a user, device or another entity in an information or communications system.
- **Assurance:** A process to confirm one of several security goals to protect information and information systems, including authentication, integrity, availability, confidentiality, and accountability. Assurance is not absolute: it is a defined level of confidence. Assurance levels relating to authentication may be approached from various points of view – one of them being risk management practices and the other suitable technological solutions.
- **Attributes:** Information concerning specific types of characteristics of a given identity.
- **Authorisation:** The actions an authenticated person or entity is permitted as a result of authentication. Authorisation may depend on selected attributes of an identity. Decisions concerning authorisation are the purview of relying parties.

- **Credential:** Data that is used to establish the claimed attributes or identity of a person or an entity.
- **Electronic Communication:** An electronic transmission, message or transaction.
- **Electronic Signature:** Data in electronic form in, affixed to, or logically associated with, a data message and used by, or on behalf of a person with the intent to identify that person.
- **Encryption:** The conversion of data (plaintext) into a form called a ciphertext that cannot be easily understood by unauthorised recipients. Decryption is the process of converting encrypted data back into its original form, so it can be understood. Common encryption types include symmetric and asymmetric (public-key) encryption.[6]
- **Identity:** At the operational level, a dynamic set of attributes defining a unique reference to a person or an entity, including where attributes are provided in electronic form, using some sort of credential. The attributes may be context-specific based on the nature of the interaction.
- **Participants:** Individuals or organisations participating in authentication processes. Includes individuals or organisations asserting identity, relying parties, third party authorities providing identity credentials, trust service providers and system certifiers, such as auditors, accreditation bodies, federation governance bodies, government supervisory bodies. Participants may have multiple roles.
- **Relying party:** The entity or person that is relying on an identity credential or assertion of identity to make a decision as to what action to take in a given application context.

In an effort to address the benefits of national and cross-jurisdictional authentication methods, the following foundation and operational principles are offered. The foundation principles constitute guiding principles for the use and implementation of authentication methods, and are inter-related to one another and the operational principles. The operational principles serve as guidance to all users, and in particular to those involved in the design, development and deployment of authentication services and products.

6. The OECD Guidelines for Cryptography Policy are an important reference. The Guidelines recognize the important role encryption plays in helping to ensure the security of data and the protection of privacy in national and global information and communication infrastructures, networks and systems. www.oecd.org/document/11/0,2340,en_2649_201185_1814731_1_1_1_1,00.html.

Part A – Foundation principles

1. Systems approach

The design, development and implementation of authentication solutions should be seen as a coherent system development process involving all relevant participants at appropriate stages. Particular attention should be paid to the involvement of end users of authentication at the system design stage. Interoperability of authentication solutions should be addressed at this stage as well. Technical and non-technical safeguards should be considered as complementary parts of system design of authentication solutions.

When designing and implementing authentication solutions, overall system security should be a key driver. Threats and challenges introduced by all relevant participants in the data transmission and storage process should be addressed at all stages of system design and development of authentication solutions.

The selection of assurance levels and mechanisms for authentication should be based on a risk assessment of the various system components and of the participant behaviour(s). User friendliness and ease of use should be a leading principle for selecting authentication mechanisms as well as it contributes to fostering trust in online transactions. Security features and ease of use need to be balanced in such a way so as to ensure that overall system security is in place.

2. Proportionality

The degree of responsibility and risk that each participant in the authentication process assumes should be in proportion to the degree of knowledge and control that the participant can reasonably be expected to have and to exercise, as well as to the nature and value of the transaction or communication itself. Since participants can perform multiple functions in varying combinations, the degree of responsibility and risk assumed by any one participant may vary, depending on these functions.

3. Roles and responsibilities

Participants in authentication processes should be aware of their roles, the functions they are performing and of the responsibilities associated with those functions. Functions and responsibilities should be clearly formulated and disclosed. All participants should act prudently and take reasonable steps to inform themselves of the nature of the authentication process, including its requirements and limitations, to protect information associated with the process, and to manage the risks to which they are exposed.

4. Security and trust

All participants in authentication processes have the responsibility to contribute to the security and mitigation of risk through sound security practices, as laid out in the OECD Security Guidelines' eighth principle on security management.[7]

All participants in an authentication process should be responsible and accountable for security, in proportion to their roles in that process. Those designing and implementing security and trust services, should bear more responsibility than others for mitigating risk. This includes fostering a global culture of security by building security and trust (*e.g.* privacy protection) features into information systems and technologies. By practicing sound security principles, organisations will contribute towards building trust in the use of technologies that facilitate online transactions. Authentication plays a key role in securing trust in online transactions and e-commerce by establishing reliable access controls and accountability.

5. Privacy

Organisations engaged in the design or operation of authentication processes should comply with the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* and with relevant codes of practice, in addition to applicable legislation. This principle is particularly important in the context of cross-border authentication, where privacy laws and regulations may vary.

Those designing and implementing authentication processes should consider how systems can appropriately respect privacy and data protection at every stage of the process. This would involve limiting the collection, use, storage, transfer and disclosure of personal information to the purposes deemed necessary for accomplishing authentication. Where notice is provided to individuals, notice should be accurate, clear, conspicuous and unambiguous. Individual control over personal data by the authentication subject is encouraged even if stewardship of that data is by a public authority or other third party.

The level of authentication (and, by definition the amount of personal information collected for that authentication process) should be in proportion to the nature of the transaction or communication and take into account the degree of importance and sensitivity required. This principle is particularly important in the context of cross-border authentication where privacy laws and regulations can vary.

Authentication offers ways to protect privacy but only if it is used in a manner that is fit for purpose and takes into account the interests of users. There may be a tendency to require the strongest level of authentication

7. This Principle adopts the OECD Guidelines for the Security of Information Systems and Networks. The complete text of the Guidelines is available at www.oecd.org/dataoecd/16/22/15582260.pdf

for all transactions with a view to protecting systems and their users. However, while a greater amount of personal information may be required to attain the more reliable credential (identity proofing), systems can, and should be designed so as to not expose this information during routine parts of the authentication transaction or the electronic communication.

6. Risk management

The risks associated with authentication processes for electronic communications should be identified, assessed and managed in a reasonable, fair and efficient manner. The responsibilities of participants concerning risk management should be in proportion to the degree of knowledge, control and power to act that each participant can reasonably be expected to have and to exercise. The ability of participants to identify, assess and manage risks will vary substantially and some types of participants *(e.g.* consumers and small enterprises) may not reasonably be expected to do this to the same extent as other participants. (See Principle 2 – Proportionality)

This principle should also be applied when considering the selection of appropriate assurance levels for various types of applications. The selection of assurance level of authentication should be guided by the likelihood and consequences of identified risks and impacts (*e.g.* misappropriation of identity for all participants).

The selection of assurance levels based on risk analysis should be closely associated with selection of appropriate authentication mechanisms that match the identified risks and impacts with appropriate security features in a cost-effective and efficient manner.

Part B – Operational principles

1. ***Usability:*** Authentication processes should be effective, efficient, reliable and easy to use and should take into account the interests and requirements of individuals and organisations. Usability should be guided by minimising the risks associated with use.

2. ***Fit for purpose****:* Authentication, like many security related practices and technologies, exists along a continuum of risk. This means that authentication technologies and processes must be considered in the context of an application and be appropriate and proportional to its function and desired use. There should be enough security to address risk in an acceptable fashion, but not be unreasonably burdensome to accomplish the electronic communication. The business requirements for trust are reflected in the assurance level provided and are related to the type of credential used. *(See Appendix B for more information and examples of assurance levels.)* Market-based decisions should be key drivers in determining which authentication technologies should be used**.**

Service providers should consider the level of risk to the system as a whole, the cost of implementation, practicality, overall business benefit and applicable legal requirements.

3. Business continuity: Establishment of business continuity and incident recovery planning provisions will develop user ***confidence*** and facilitate cross-jurisdictional acceptance of reliable authentication activities or tools**.**

4. ***Education and awareness:*** Effective authentication processes can be an effective deterrent to the theft of online assets and information. Education and awareness of the benefits and proper uses of authentication are prerequisites for wide penetration of electronic authentication, and critical for continued user trust in networks and information systems. Education campaigns should stress the importance of tools that are user-friendly and yet achieve an appropriate degree of security. Special attention should be paid to consumer and small enterprises education focussing not only on the benefits of authentication, but also the responsibilities and risks associated with its use.

5. ***Disclosure:*** Participants that offer authentication services should disclose information to the other participants to ensure that all participants are aware of the risks and the responsibilities associated with the use of authentication. Appropriate disclosure requires the information to be provided in sufficient detail for the purpose, be in plain language and be conspicuous. All three factors will have a bearing on the knowledge other participants can reasonably be expected to have of the disclosed information.

6. ***Complaints Handling:*** Organisations that utilize authentication processes should make available a complaints-handling process that enables participants to resolve complaints efficiently and effectively and to respond appropriately to non-compliance issues. Complaints handling processes should be visible, accessible, responsive, and objective.

7. ***Independent audit and assessments:*** The use of compliance audits and assessments by independent parties, preferably according to internationally recognised standards, will develop user confidence and facilitate cross-jurisdictional acceptance of services. Each step of the authentication process, from identity proofing to technical or administrative management of the service, influences whether the process is trustworthy and in compliance. Ideally each step in the process should be consistent in its strength and robustness. Accreditation bodies that oversee the requirements for certification and accredit the auditors doing the certification also have an important role to play. Their adherence to generally recognised procedures can also facilitate cross-jurisdictional acceptance of services.

8. ***Cross-jurisdictional approaches:*** National approaches to authentication should ideally allow for foreign-based authentication services to be accepted as long as local requirements, or their equivalent, are met. Such local requirements should not be created or implemented in a discriminatory manner. Consistency in applying standards and general agreement on how to define levels of assurance can facilitate cross-jurisdictional (and cross-sectoral) interoperability. Business, technical and legal inter-operability are necessary for cross-sectoral and cross-jurisdictional transactions. Interoperability needs to be considered at the design stage wherever possible.

9. ***Standards:*** Wide deployment of authentication technologies that may be used in a global context is heavily dependent on standards, both *de facto* and *de jure*. Standards aim at consolidating requirements of suppliers, users, relying parties and government legislative bodies into frameworks that may be used for co-ordinated implementation of authentication schemes. Relevant standards bodies that issue standards important for global interoperability of authentication schemes include: ISO, ITU, ETSI, CEN, ANSI, NIST, OASIS – Liberty Alliance, W3C, IETF and CC (Common Criteria) Multilateral Arrangement.

In order to achieve some degree of interoperability of various authentication schemes, standards should be applied when developing and implementing authentication solutions, in particular considering enrolment procedures, credential deployment, technical capabilities and security of credentials, management of credentials, technical interfaces between authentication solutions and applications, as well as any government supervising procedures for authentication suppliers.

Continuing issues

The above principles provide a framework to help foster common approaches to authentication in order to foster the use of authentication at national and cross-border levels. However, several issues identified in previous OECD work and in discussions between Member countries, business and the civil society which took place in the OECD Working Party on Information Security and Privacy (WPISP) and Committee for Information, Computer and Communications Policy (ICCP) remain unaddressed. These continuing issues are offered as considerations for the appropriate OECD committee(s) and other international fora, industry and civil society to consider in discussions pertaining to the digital economy and future challenges with identity management.

- The wide variety of existing authentication methods in use could be a source of confusion for users and providers in determining which method best suits their needs. This variety may become a barrier to inter-organisational or cross-border services. International standards

could possibly remove some of the complexity currently existing in the authentication marketplace, but wider agreements on assurance levels and authentication methods that may be associated with these are needed in order to establish sustainable solutions, both nationally and at the cross-border level.

- In a globalised marketplace, efforts towards harmonisation of standards are essential to maximise their efficiency. Some efforts in that direction have already achieved results, *e.g.* US-Canadian Government cooperation on "bridge solutions" and the U.S.-EU/ETSI recognition of schemas for defining requirements for certification authorities (PKI services suppliers). Such efforts could be encouraged further and standards-mapping exercises could to be carried out under the auspices of relevant international bodies.

- Differences in the legal treatment and recognition of electronic documents and signatures are still an obstacle to the cross-border use of authentication. While work within international organisations such as UNCITRAL establishes common approaches, additional multilateral work at the practical level is still necessary.

- Mechanisms for recognising foreign authentication services have been developed but there is limited experience in cross-jurisdictional applications. Jurisdictions need some means of assessing the trust framework of their partners. This guidance document and the framework it offers may assist in this regard but more comprehensive work on the issue needs to be carried out.

- Previous OECD work identified the lack of business cases for authentication as an impediment to its wider use. Successes in the marketplace (*e.g.* home banking) could provide elements for such business cases and be leveraged to stimulate the wider adoption of authentication.

- Biometrics and Radiofrequency identification (RFID) are related to authentication as they encompass technology that can further enhance verification methods. It may be valuable to examine the impact of these emerging technologies on the business of authenticating and providing improved online security and identity management.

REFERENCES

OECD documents

The Use of Authentication Across Borders in OECD Countries (Summary of responses, 2005). DSTI/ICCP/REG(2005)4/FINAL www.olis.oecd.org/olis/2005doc.nsf/LinkTo/dsti-iccp-reg(2005)4-final

Draft OECD Questionnaire for Preparing a Fact-Finding Report to Take Stock of the Current Usage of Authentication Across Borders (2004). DSTI/ICCP/REG(2004)5/FINAL

Summary of Responses to the Survey of Legal and Policy Frameworks for Electronic Authentication Services and E-Signatures in OECD Member Countries (2004). DSTI/ICCP/REG(2003)9/FINAL www.olis.oecd.org/olis/2003doc.nsf/LinkTo/dsti-iccp-reg(2003)9-final

Survey of Legal and Policy Frameworks for Electronic Authentication Services and E-Signatures in OECD Member Countries (Questionnaire, 2003) DSTI/ICCP/REG(2003)4/REV1

Electronic Authentication: Analysis and Mapping of Key Elements for Establishing Confidence in Certification Services (2002). DSTI/ICCP/REG(2002)4

Electronic Authentication: Framework for Analysis of Key Elements for Establishing Trust in Certification Processes (RD submitted by Canada, 2002) DSTI/ICCP/REG/RD(2002)3

Electronic Authentication: Information Paper on the Work of the APEC eSecurity Task Group - Draft for Discussion Purposes Only (RD submitted by Australia, 2002). DSTI/ICCP/REG/RD(2002)1

Progress Achieved by OECD Member Countries in Furtherance of the Ottawa Declaration on Authentication for Electronic Commerce (2002). DSTI/ICCP/REG(2001)10/FINAL www.olis.oecd.org/olis/2001doc.nsf/linkto/dsti-iccp-reg(2001)10-final

Revised Inventory of Approaches to Authentication and Certifications in a Global Networked Society (2000). DSTI/ICCP/REG(2000)1/REV1

Questionnaire for the Survey on Form Requirements (2000) DSTI/ICCP/REG(2000)2

Inventory of Approaches to Authentication and Certifications in a Global Networked Society (1999). DSTI/ICCP/REG(99)13/FINAL www.olis.oecd.org/olis/1999doc.nsf/linkto/dsti-iccp-reg(99)13-final

Joint OECD-Private Sector Workshop on Electronic Authentication. Menlo-Park, California, USA. 2-4 June 1999. In co-operation with private sector representatives and with The Stanford Program in Law, Science & Technology, Stanford Law School (1999).

DSTI/ICCP/REG(99)14/FINAL including the "Background Paper on Electronic Authentication Technologies and Issues" [DSTI/ICCP/REG(99)6/REV1] www.olis.oecd.org/olis/1999doc.nsf/linkto/dsti-iccp-reg(99)14-final

Proposal by the Delegation of the United Kingdom for Guidelines on Policy for Authentication and Electronic Signatures (1999). DSTI/ICCP/REG/AH(99)1

Discussion Paper on Authentication and Certification (1998). DSTI/ICCP/REG(98)1

OECD Ministerial Declaration on Authentication for Electronic Commerce (1998). DSTI/ICCP/REG(98)9/FINAL www.olis.oecd.org/olis/1998doc.nsf/linkto/dsti-iccp-reg(98)9-final

Inventory of Approaches to Authentication and Certification in a Global Networked Society (1998). DSTI/ICCP/REG(98)3/REV1

See also:

- Anti-Spam Toolkit: Technical Measures to Combat Spam www.olis.oecd.org/olis/2005doc.nsf/linkto/dsti-cp-iccp-spam(2005)3-final

Other resources

International

- UNCITRAL Model Law on Electronic Commerce with Guide to Enactment (1996) www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html

- UNCITRAL Model Law on Electronic Signatures with Guide to Enactment (2001) www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html

Regional

- EU "Signposts Towards e-Government 2010" http://europa.eu.int/information_society/activities/egovernment_research/doc/minconf2005/signposts2005.pdf

- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures, Official Journal L 013 , 19 January 2000, p. 0012 – 0020 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML

National

- Australian government authentication framework:
  www.agimo.gov.au/infrastructure/authentication/agaf/impguidegovt
  www.agimo.gov.au/infrastructure/authentication/agaf/overview

- Canadian Authentication Principles
  http://strategis.ic.gc.ca/authen

- New Zealand government authentication framework:
  www.e.govt.nz/resources/news/2002/apr-2002/2002042801.html

- United Kingdom: "Registration and Authentication - e-Government Strategy Framework Policy and Guidelines" www.govtalk.gov.uk/policydocs/policydocs_document.asp?docnum=654&topic=56&topictitle=Security+Framework&subjecttitle=.

- United States:

  - NIST Special Publication 800 – 63 Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology (NIST), USA
    http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf

  - OMB's E-Authentication Guidance for U.S. Federal Agencies (M-04-04)
    www.whitehouse.gov/OMB/memoranda/fy04/m04-04.pdf

Non-Governmental

- Center for Democracy and Technology "Authentication Privacy Principles Working Group. Interim Report". 13 May 2003. www.cdt.org/privacy/authentication/030513interim.shtml

- International Chamber of Commerce (ICC): General Usage for International Digitally Ensured Commerce (version II) - GUIDEC II
  www.iccwbo.org/home/guidec/guidec_two/foreword.asp

Appendix A
Overview of OECD work on authentication (1998 – 2005)

The Ottawa Ministerial Declaration

On 7-9 October 1998, OECD Ministers adopted the "Declaration on Authentication for Electronic Commerce" at the Ministerial Conference "A Borderless World: Realising the Potential of Global Electronic Commerce" held in Ottawa, Canada.[8] The Declaration recognised the importance of authentication for electronic commerce and outlined a number of actions to promote the development and use of electronic authentication technologies and mechanisms. In particular, Ministers declared their determination to:

- Take a non-discriminatory approach to electronic authentication from other countries.
- Encourage efforts to develop authentication technologies and mechanisms, and facilitate the use of those technologies and mechanisms for electronic commerce.
- Amend, where appropriate, technology or media specific requirements in current laws or policies that may impede the use of information and communication technologies and electronic authentication mechanisms, giving favourable consideration to the relevant provisions of the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) in 1996.
- Proceed with the application of electronic authentication technologies to enhance the delivery of government services and programmes to the public.
- Continue work at the international level, together with business, industry and user representatives, concerning authentication technologies and mechanisms to facilitate global electronic commerce.

8. www.olis.oecd.org/olis/1998doc.nsf/linkto/sg-ec(98)14-final

Inventory of Approaches to E-Authentication and Joint OECD-Private Sector Workshop

As a preparatory step, the OECD ICCP Committee's Working Party on Information Security and Privacy (WPISP) surveyed Member country approaches to authentication and certification on global networks, including laws, policies and initiatives, in both the public and private sectors and at the national, regional and international levels. The resulting 1999 "Inventory of Approaches to Authentication and Certification in a Global Networked Society"[9] provided a useful resource on national approaches in particular on private contractual agreements, technology requirements, standards, and certification authorities.

In addition, the WPISP organised a joint OECD-Private Sector Workshop on Electronic Authentication[10] at Stanford, California, on 2-4 June 1999 to foster the dialogue among all stakeholders and further gather information on approaches to e-authentication. 200 representatives from OECD governments, Asia-Pacific Economic Co-operation (APEC) Telecommunications Working Group, private sector, international organisations, consumer advocacy and user organisations discussed business and government models, approaches of different industry sectors, and issues for implementing electronic authentication including requirements for the international operation of global authentication systems.

Report on Progress Achieved in Furtherance of the Ministerial Declaration

Following the workshop, a Steering Group was established by the WPISP to monitor the implementation of national policies and laws with regards to the objectives of the Ministerial declaration. The group updated in 2000 the "Inventory of Approaches to Authentication and Certifications in a Global Networked Society"[11] to take account of progress made at national level.

This work, along with information from APEC Member economies were integrated in a report on "Progress Achieved by OECD Member Countries in Furtherance of the Ottawa Declaration on Authentication for Electronic Commerce"[12].

The report concluded that progress had been made on issues such as the legal recognition of electronic signatures and the application of

9. DSTI/ICCP/REG(99)13/FINAL

10. Proceedings and background documents can be found in DSTI/ICCP/REG(99)14/FINAL

11. DSTI/ICCP/REG(2000)1/REV1

12. DSTI/ICCP/REG(2001)10/FINAL

authentication technologies to the delivery of government services. The need for compatible approaches and policies among OECD Member governments and business initiatives to establish real international marketplace interoperability of electronic authentication systems was highlighted. The report suggested that additional work could help further identify and address impediments to the global, seamless use of authentication methods.

Survey of Legal and Policy Frameworks for E-Authentication and E-Signatures

In order to help determine how varying legislative, legal and policy frameworks could be bridged to provide for cross-jurisdictional acceptance of authentication services and for legal effect of electronic signatures, the WPISP conducted in 2002-2003 a "Survey of Legal and Policy Frameworks for Electronic Authentication Services and E-Signatures in OECD Member Countries". [13] The questionnaire was designed to be coherent with the survey undertaken in APEC Member economies by the APEC e-Security Task Group.

The information provided by Member countries allowed for the identification of areas where a high degree of consistency existed among Member countries, of areas where only some degree of consistency could be found and of areas showing inconsistencies (cf. Table 1). It also identified the risk that Member countries develop divergent approaches to the recognition of foreign-based authentication services which could stifle cross-border transactions.

13. DSTI/ICCP/REG(2003)9/FINAL

Findings of the Survey of Legal and Policy Frameworks for Electronic Authentication Services and E-Signatures in OECD Member Countries

High degree of consistency	Some consistency	Inconsistencies
• Legislative/regulatory framework • for e-signatures • Licensing/accreditation/approval requirements for authentication services • Technology neutrality • Secure e-government • Approach to "foreign"-based signatures and services • Credential requirements	• Registration processes • Evaluation of services	• Nature of audit requirements • Recognition of foreign authentication services • Technical standards, even if some degree of consistency exists • (*e.g.* for PKI)

Report on the Use of Authentication across Borders

On the basis of these findings, the WPISP agreed in October 2003 that a better understanding of the existing cross-border authentication marketplace was necessary to further help bridge national approaches and foster cross-border use of authentication. A survey of current authentication implementations and examples of use of authentication across borders as well as barriers to the use of digital signatures across borders from the supplier/user perspective was conducted in 2004-2005. The survey on "The Use of Authentication across Borders in OECD Countries" [14] also collected information on factors identified as fostering or impeding the national use of authentication technologies and digital signatures.

The exercise led to identify a number of common themes in Member countries responses (cf. Table 2) but the main finding revealed the need to increase usage rates of effective authentication across borders.

14. DSTI/ICCP/REG(2005)4/FINAL

Common themes identified in the report on "The Use of Authentication across Borders in OECD Countries"

Common positive themes	Common negative themes
• Maturity and robustness of public sector implementations • Maturity of financial sector implementations • Alignment of regulatory frameworks • Non-discriminatory approach to "foreign" signatures and services • Technology neutrality • PKI is alive and well • All categories of users are engaged • All applications described provide evidence of identity but with various methods of authentication	• Challenges and limitation to interoperability • Mechanisms for recognition of foreign authentication services not well developed • Acceptance of credentials as a barrier to interoperability • A range of authentication methods in use leading users to confusion • Lack of information regarding privacy enhancing features • Lack of business cases for authentication • Absence of quantitative data on usage

Appendix B
Authentication assurance levels

Assurance levels relating to authentication may be approached from various points of view – one of them being risk management practices and another being suitable technological solutions. Both approaches had been used by Member countries' governments in the policy documents published in recent years.[15]

The risk management approach considers the possible consequences or degree of harm of a security breach following inadequate/failed authentication process. Degrees of harm may be expressed in qualitative (*e.g.* privacy harm) and/or quantitative terms (*e.g.* loss of revenue). Some risks that could be considered include: financial, health, safety and criminal activity. Risks to both the individual and the organisation should be considered.

One could envisage three basic levels of assurance, defined along these lines:

- Low: security breach (*i.e.* misappropriation of e-identity) may lead to moderate losses of an economic or other nature (*e.g.* loss of non-confidential data); a repudiation of transaction based on this type of identification may lead to a moderate pecuniary loss.

- Medium: security breach (*i.e.* misappropriation of e-identity) may lead some losses, but not of a very serious nature; it may cause loss of confidential data; a repudiation of a transaction based on this type of identification may lead to a significant pecuniary loss.

- High: security breach (*i.e.* misappropriation of e-identity) may lead to significant losses; it may cause loss of highly confidential data; a repudiation of a transaction based on this type of identification may lead to a very significant pecuniary loss.

The above scheme provides just one example of many possible assurance level definitions.

The technology approach (suitable authentication mechanisms) considers generic requirements for authentication mechanisms, including

15. Cf. e.g. UK "Registration and Authentication" published in 2002 or the Australian Government e-Authentication Framework (see list of references).

associated security procedures. Examples of such requirements may be authentication enrolment procedures (registration procedures), capabilities and security of credentials, deployment procedures for credentials, management of identities associated with credentials, necessary accreditations with certification schemes, etc.

One can envisage assurance levels, defined in agreement with such generic requirements, as follows:

- Basic: single-factor authentication: *e.g.* user name and password issued as a result of a two-channels procedure (*i.e.* both online and by mail).

- Medium: two-factor authentication: *e.g.* SMS to mobile phone, token devices with challenge-response protocols, software-based PKI certificates, all issued by a two-channel registration and deployment procedure.

- High: two-factor authentication with very secure registration procedure (such as physical appearance, requirement of legally valid identity credential) and deployment by a two-channel procedure, *e.g.* PKI-certificates on a smart card or secure USB-token, or in a HSM (Hardware Security Module).

Again, the above definitions are offered as just one example of many possible assurance level schemes. Less granulated or more granulated approaches, *i.e.* fewer or several more levels, may be employed. The authentication mechanisms mentioned are provided for illustrative purposes only and should not be interpreted as an exhaustive or exclusive list.

It could be recommended to merge these two approaches into a single, unified approach, where assurance levels defined on the basis of risks posed by a security breach are associated with adequate levels of security in authentication mechanisms.

Any defined authentication level scheme needs to be closely associated with the actual application area (or several areas) it is to be used within. Application areas will constitute the necessary context for precise definitions of losses or consequences and specific selections of appropriate mechanisms for authentication.

Introduction of the concept of federation of identities[16] creates an additional challenge for definitions of assurance levels. Identity federation is a mechanism commonly used to facilitate a single-sign-on feature for users of associated information systems. Single-sign-on may also be facilitated by other mechanisms (*e.g.* common security portals). Defining

16. Cf. Liberty Alliance Project Whitepaper: Personal Identity, March 23, 2006. www.projectliberty.org/about/whitepapers/Personal_Identity.pdf.

an assurance level for an authentication mechanism that may be used in a federated environment and/or for single-sign-on purposes requires additional security considerations and a specific risk analysis. Such analysis needs to be targeted at security risks posed by multiple use of one credential against many systems and/or reuse of identity validation information provided by the first system a credential had been used against in other systems. Federated systems introduce a greater level of technical complexity and thus introduce new vulnerabilities in an authentication procedure, as compared to direct authentication against one system. This should also be taken into account in the risk analysis preceding the definition of a unified assurance level scheme.

CRYPTOGRAPHY POLICY

RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES FOR CRYPTOGRAPHY POLICY (1997)

The council,

Having regard to:

The Convention on the Organisation for Economic Co-operation and Development of 14 December 1960, in particular, articles 1 b), 1 c), 3 a) and 5 b) thereof;

The Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 [C(80)58(Final)];

The Declaration on Transborder Data Flows adopted by the Governments of OECD Member countries on 11 April 1985 [Annex to C(85)139];

The Recommendation of the Council concerning Guidelines for the Security of Information Systems of 26-27 November 1992 [C(92)188/FINAL];

The Directive [95/46/EC] of the European Parliament and of the Council of the European Union of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies agreed on 13 July 1996;

The Regulation [(EC) 3381/94] and the Decision [94/942/PESC] of the Council of the European Union of 19 December 1994 concerning the control of the export of dual-use goods;

And the Recommendation [R(95)13] of the Council of Europe of 11 September 1995 concerning problems of criminal procedural law connected with information technology;

Considering:

That national and global information infrastructures are developing rapidly to provide a seamless network for world-wide communications and access to data;

That this emerging information and communications network is likely to have an important impact on economic development and world trade;

That the users of information technology must have trust in the security of information and communications infrastructures, networks and systems; in the confidentiality, integrity, and availability of data on them; and in the ability to prove the origin and receipt of data;

That data is increasingly vulnerable to sophisticated threats to its security, and ensuring the security of data through legal, procedural and technical means is fundamentally important in order for national and international information infrastructures to reach their full potential;

Recognising:

That, as cryptography can be an effective tool for the secure use of information technology by ensuring confidentiality, integrity and availability of data and by providing authentication and non-repudiation mechanisms for that data, it is an important component of secure information and communications networks and systems;

That cryptography has a variety of applications related to the protection of privacy, intellectual property, business and financial information, public safety and national security, and the operation of electronic commerce, including secure anonymous payments and transactions;

That the failure to utilise cryptographic methods can adversely affect the protection of privacy, intellectual property, business and financial information, public safety and national security and the operation of electronic commerce because data and communications may be inadequately protected from unauthorised access, alteration, and improper use, and, therefore, users may not trust information and communications systems, networks and infrastructures;

That the use of cryptography to ensure integrity of data, including authentication and non-repudiation mechanisms, is distinct from its use to ensure confidentiality of data, and that each of these uses presents different issues;

That the quality of information protection afforded by cryptography depends not only on the selected technical means, but also on good managerial, organisational and operational procedures;

And further recognising:

That governments have wide-ranging responsibilities, several of which are specifically implicated in the use of cryptography, including protection of privacy and facilitating information and communications systems security; encouraging economic well-being by, in part, promoting commerce;

maintaining public safety; and enabling the enforcement of laws and the protection of national security;

That although there are legitimate governmental, commercial and individual needs and uses for cryptography, it may also be used by individuals or entities for illegal activities, which can affect public safety, national security, the enforcement of laws, business interests, consumer interests or privacy; therefore governments, together with industry and the general public, are challenged to develop balanced policies;

That due to the inherently global nature of information and communications networks, implementation of incompatible national policies will not meet the needs of individuals, business and governments and may create obstacles to economic co-operation and development; and, therefore, national policies may require international co-ordination;

That this Recommendation of the Council does not affect the sovereign rights of national governments and that the Guidelines contained in the Annex to this Recommendation are always subject to the requirements of national law;

On the proposal of the Committee for Information, Computer and Communications Policy;

Recommends that member countries:

1. Establish new, or amend existing, policies, methods, measures, practices and procedures to reflect and take into account the Principles concerning cryptography policy set forth in the Guidelines contained in the Annex to this Recommendation (hereinafter ?the Guidelines?), which is an integral part hereof; in so doing, also take into account the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 [C(80)58(Final)] and the Recommendation of the Council concerning Guidelines for the Security of Information Systems of 26-27 November 1992 [C(92)188/FINAL];

2. Consult, co-ordinate and co-operate at the national and international level in the implementation of the Guidelines;

3. Act on the need for practical and operational solutions in the area of international cryptography policy by using the Guidelines as a basis for agreements on specific issues related to international cryptography policy;

4. Disseminate the Guidelines throughout the public and private sectors to promote awareness of the issues and policies related to cryptography;

5. Remove, or avoid creating in the name of cryptography policy, unjustified obstacles to international trade and the development of information and communications networks;

6. State clearly and make publicly available, any national controls imposed by governments relating to the use of cryptography;

7. Review the Guidelines at least every five years, with a view to improving international co-operation on issues relating to cryptography policy.

Annex
Guidelines for cryptography policy

I. Aims

The Guidelines are intended:

- To promote the use of cryptography:
    - To foster confidence in information and communications infrastructures, networks and systems and the manner in which they are used.
    - To help ensure the security of data, and to protect privacy, in national and global information and communications infrastructures, networks and systems.
- To promote this use of cryptography without unduly jeopardising public safety, law enforcement, and national security.
- To raise awareness of the need for compatible cryptography policies and laws, as well as the need for interoperable, portable and mobile cryptographic methods in national and global information and communications networks.
- To assist decision-makers in the public and private sectors in developing and implementing coherent national and international policies, methods, measures, practices and procedures for the effective use of cryptography.
- To promote co-operation between the public and private sectors in the development and implementation of national and international cryptography policies, methods, measures, practices and procedures.
- To facilitate international trade by promoting cost-effective, interoperable, portable and mobile cryptographic systems.
- To promote international co-operation among governments, business and research communities, and standards-making bodies in achieving co-ordinated use of cryptographic methods.

II. Scope

The Guidelines are primarily aimed at governments, in terms of the policy recommendations herein, but with anticipation that they will be widely read and followed by both the private and public sectors.

It is recognised that governments have separable and distinct responsibilities for the protection of information which requires security in the national interest; the Guidelines are not intended for application in these matters.

III. Definitions

For the purposes of the Guidelines:

"Authentication" means a function for establishing the validity of a claimed identity of a user, device or another entity in an information or communications system.

"Availability" of data, information, and information and communications systems means that they are accessible and usable on a timely basis in the required manner.

"Confidentiality" of data or information means that it is not made available or disclosed to unauthorised individuals, entities, or processes.

"Cryptography" means the discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorised use.

"Cryptographic key" means a parameter used with a cryptographic algorithm to transform, validate, authenticate, encrypt or decrypt data.

"Cryptographic methods" means cryptographic techniques, services, systems, products and key management systems.

"Data" means the representation of information in a manner suitable for communication, interpretation, storage, or processing.

"Decryption" means the inverse function of encryption.

"Encryption" means the transformation of data by the use of cryptography to produce unintelligible data (encrypted data) to ensure its confidentiality.

"Integrity" of data or information means that it has not been modified or altered in an unauthorised manner.

"Interoperability" of cryptographic methods means the technical ability of multiple cryptographic methods to function together.

"Key management system" means a system for generation, storage, distribution, revocation, deletion, archiving, certification or application of cryptographic keys.

"Keyholder" means an individual or entity in possession or control of cryptographic keys. A keyholder is not necessarily a user of the key.

"Law enforcement" or "enforcement of laws" refers to the enforcement of all laws, without regard to subject matter.

"Lawful access" means access by third party individuals or entities, including governments, to plaintext, or cryptographic keys, of encrypted data, in accordance with law.

"Mobility" of cryptographic methods only means the technical ability to function in multiple countries or information and communications infrastructures.

"Non-repudiation" means a property achieved through cryptographic methods, which prevents an individual or entity from denying having performed a particular action related to data (such as mechanisms for non-rejection of authority (origin); for proof of obligation, intent, or commitment; or for proof of ownership).

"Personal data" means any information relating to an identified or identifiable individual.

"Plaintext" means intelligible data.

"Portability" of cryptographic methods means the technical ability to be adapted and function in multiple systems.

IV. Integration

The principles in Section V of this Annex, each of which addresses an important policy concern, are interdependent and should be implemented as a whole so as to balance the various interests at stake. No principle should be implemented in isolation from the rest.

V. Principles

1. Trust in cryptographic methods

Cryptographic methods should be trustworthy in order to generate confidence in the use of information and communications systems.

Market forces should serve to build trust in reliable systems, and government regulation, licensing, and use of cryptographic methods may

also encourage user trust. Evaluation of cryptographic methods, especially against market-accepted criteria, could also generate user trust.

In the interests of user trust, a contract dealing with the use of a key management system should indicate the jurisdiction whose laws apply to that system.

2. Choice of cryptographic methods

Users should have a right to choose any cryptographic method, subject to applicable law.

Users should have access to cryptography that meets their needs, so that they can trust in the security of information and communications systems, and the confidentiality and integrity of data on those systems. Individuals or entities who own, control, access, use or store data may have a responsibility to protect the confidentiality and integrity of such data, and may therefore be responsible for using appropriate cryptographic methods. It is expected that a variety of cryptographic methods may be needed to fulfil different data security requirements. Users of cryptography should be free, subject to applicable law, to determine the type and level of data security needed, and to select and implement appropriate cryptographic methods, including a key management system that suits their needs.

In order to protect an identified public interest, such as the protection of personal data or electronic commerce, governments may implement policies requiring cryptographic methods to achieve a sufficient level of protection.

Government controls on cryptographic methods should be no more than are essential to the discharge of government responsibilities and should respect user choice to the greatest extent possible. This principle should not be interpreted as implying that governments should initiate legislation which limits user choice.

3. Market driven development of cryptographic methods

Cryptographic methods should be developed in response to the needs, demands and responsibilities of individuals, businesses and governments.

The development and provision of cryptographic methods should be determined by the market in an open and competitive environment. Such an approach would best ensure that solutions keep pace with changing technology, the demands of users and evolving threats to information and communications systems security. The development of international technical standards, criteria and protocols related to cryptographic methods should also be market driven. Governments should encourage and co-operate with business and the research community in the development of cryptographic methods.

4. Standards for cryptographic methods

Technical standards, criteria and protocols for cryptographic methods should be developed and promulgated at the national and international level.

In response to the needs of the market, internationally-recognised standards-making bodies, governments, business and other relevant experts should share information and collaborate to develop and promulgate interoperable technical standards, criteria and protocols for cryptographic methods. National standards for cryptographic methods, if any, should be consistent with international standards to facilitate global interoperability, portability and mobility. Mechanisms to evaluate conformity to such technical standards, criteria and protocols for interoperability, portability and mobility of cryptographic methods should be developed. To the extent that testing of conformity to, or evaluation of, standards may occur, the broad acceptance of such results should be encouraged.

5. Protection of privacy and personal data

The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods.

Cryptographic methods can be a valuable tool for the protection of privacy, including both the confidentiality of data and communications and the protection of the identity of individuals. Cryptographic methods also offer new opportunities to minimise the collection of personal data, by enabling secure but anonymous payments, transactions and interactions. At the same time, cryptographic methods to ensure the integrity of data in electronic transactions raise privacy implications. These implications, which include the collection of personal data and the creation of systems for personal identification, should be considered and explained, and, where appropriate, privacy safeguards should be established.

The OECD Guidelines for the Protection of Privacy and Transborder Flows of Personal Data provide general guidance concerning the collection and management of personal information, and should be applied in concert with relevant national law when implementing cryptographic methods.

6. Lawful access

National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. these policies must respect the other principles contained in the guidelines to the greatest extent possible.

If considering policies on cryptographic methods that provide for lawful access, governments should carefully weigh the benefits, including the

benefits for public safety, law enforcement and national security, as well as the risks of misuse, the additional expense of any supporting infrastructure, the prospects of technical failure, and other costs. This principle should not be interpreted as implying that governments should, or should not, initiate legislation that would allow lawful access.

Where access to the plaintext, or cryptographic keys, of encrypted data is requested under lawful process, the individual or entity requesting access must have a legal right to possession of the plaintext, and once obtained the data must only be used for lawful purposes. The process through which lawful access is obtained should be recorded, so that the disclosure of the cryptographic keys or the data can be audited or reviewed in accordance with national law. Where lawful access is requested and obtained, such access should be granted within designated time limits appropriate to the circumstances. The conditions of lawful access should be stated clearly and published in a way that they are easily available to users, keyholders and providers of cryptographic methods.

Key management systems could provide a basis for a possible solution which could balance the interest of users and law enforcement authorities; these techniques could also be used to recover data, when keys are lost. Processes for lawful access to cryptographic keys must recognise the distinction between keys which are used to protect confidentiality and keys which are used for other purposes only. A cryptographic key that provides for identity or integrity only (as distinct from a cryptographic key that verifies identity or integrity only) should not be made available without the consent of the individual or entity in lawful possession of that key.

7. Liability

Whether established by contract or legislation, the liability of individuals and entities that offer cryptographic services or hold or access cryptographic keys should be clearly stated.

The liability of any individual or entity, including a government entity, that offers cryptographic services or holds or has access to cryptographic keys, should be made clear by contract or where appropriate by national legislation or international agreement. The liability of users for misuse of their own keys should also be made clear. A keyholder should not be held liable for providing cryptographic keys or plaintext of encrypted data in accordance with lawful access. The party that obtains lawful access should be liable for misuse of cryptographic keys or plaintext that it has obtained.

8. International co-operation

Governments should co-operate to co-ordinate cryptography policies. As part of this effort, governments should remove, or avoid creating in the name of cryptography policy, unjustified obstacles to trade.

In order to promote the broad international acceptance of cryptography and enable the full potential of the national and global information and communications networks, cryptography policies adopted by a country should be co-ordinated as much as possible with similar policies of other countries. To that end, the Guidelines should be used for national policy formulation.

If developed, national key management systems must, where appropriate, allow for international use of cryptography.

Lawful access across national borders may be achieved through bilateral and multilateral co-operation and agreement.

No government should impede the free flow of encrypted data passing through its jurisdiction merely on the basis of cryptography policy.

In order to promote international trade, governments should avoid developing cryptography policies and practices which create unjustified obstacles to global electronic commerce. Governments should avoid creating unjustified obstacles to international availability of cryptographic methods.

RADIO FREQUENCY IDENTIFICATION (RFID)

OECD POLICY GUIDANCE ON RADIO FREQUENCY IDENTIFICATION (2008)

Preface

The use of Radio Frequency IDentification (RFID) technologies[1] is growing. Many different RFID applications are implemented in various sectors, and used for very different purposes. RFID is now at a stage where there are potentially large benefits from wider application but barriers remain, warranting a policy framework to enhance business and consumer benefits while effectively addressing security and privacy issues. From a public policy perspective, such a framework should be supportive, technology neutral encompassing all RFID technologies and provide the basis to protect citizens from current and future negative impacts of the technologies. These policy principles address barriers to wider application of RFID. They draw on policy discussions and analytical studies on RFID carried out by the OECD from 2005 to 2007.[2]

RFID enables wireless data collection by readers from electronic tags attached to or embedded in objects, for identification and other purposes. RFID systems involve software, network and database components that enable information to flow from tags to the organisation's information infrastructure where it is processed and stored. Systems are application-specific. Some use passive, low cost tags with short read ranges, most data on the network, and only small amounts of information on tags. Others use sophisticated, high performance tags with high data capacity or read ranges that can have considerable data on tags without network connection. At present, the higher capacity tags remain less commercially viable but their cost is decreasing and they are becoming part of wider, often sensor-based, systems.

1. RFID may be considered as one of a group of automatic identification and data capturing technologies which also includes bar codes, biometrics, magnetic stripes, optical character recognition, smart cards, voice recognition and similar technologies.

2. See "Radio-Frequency Identification: a Focus on Security and Privacy" (2008) [DSTI/ICCP/REG(2007)9/FINAL], "Radio Frequency Identification Implementation in Germany: Challenges and Benefits" (2007) [DSTI/ICCP/IE(2007)6/FINAL], "Radio-Frequency Identification: Drivers, Challenges and Public Policy Considerations" (2006) [DSTI/ICCP(2005)19/FINAL], "Proceedings of the OECD Foresight Forum on Radio Frequency Identification Applications and Public Policy Considerations" (2005) [DSTI/ICCP(2006)7].

RFID applications have been in use for many years in transport (public transport entry), access control cards (building and highway entry), event ticketing and management, and, more recently, in government identity cards and passports, and extensively in manufacturing supply chains and in logistics for goods distribution. Industry sectors differ widely in RFID deployment, with many automotive companies and hospitals relying on RFID systems. Wholesale and retail businesses are rapidly adopting such systems, with a shift towards more comprehensive application strategies along sector value chains. Most tagging still occurs at the pallet and packing carton level, but there is a trend toward item-level tagging, beginning with high-value goods or components, as tag prices decline.

Business benefits are sector-specific and commonly include process optimisation, more efficient supply chain inventory management, and increased process quality and security including recycling and anti-counterfeiting applications. Most implementation projects are in their early stages and many businesses need to change the processes or their work organisation to better capture benefits. Broad societal benefits are expected from RFID in various areas ranging from food safety, product recall, drug identification, public health and medical applications, better warranty management, better, more detailed product information and improved stocking.

Technological developments are focusing on increasing real-time information of business processes, improved business performance and improved security and privacy. Combination with other technologies is important in the longer-term, and communications and sensor technologies will enable distance monitoring of ambient conditions (*e.g.* temperature, pressure) in applications such as healthcare and environment. Many of the technical challenges are imposed by the laws of physics, such as interference, power management, reflection, and signal attenuation.

Many of the potential societal challenges raised by RFID relate to its core characteristic: invisible electromagnetic communications that make the collection of information by RFID devices not obvious to the person carrying the tagged product or object. Tags' data depends on their use contexts. For example, in a supply chain/retail context, tags attached to products usually contain product-identifying information and privacy concerns arise after the point of sale; in credentials, tags sometimes contain personal information. The extent to which tags are traceable is determined by the read range of the combined tag and reader. Specific concerns include the controls of the tag reading, the protection of personal data, the ability to join trace information with other information to profile individuals and the use to which the information may be put. Longer-term concerns are related to the potential pervasiveness of tags and readers.

Like any other information technology, RFID systems are subject to security risks[3] affecting their integrity, availability and confidentiality such as denial of service, jamming, cloning, interception/eavesdropping, and unauthorised access to data ("skimming"). While not all uses of RFID implicate privacy concerns, RFID systems which collect or process information relating to identified or identifiable individuals are subject to privacy risks (*e.g.* unauthorised access to information stored in tags). The use of RFID in identity credentials, for example, poses heightened privacy concerns, and it is necessary to ensure privacy is appropriately protected. These risks, if not taken into account at an early stage, are likely to increase the costs of RFID applications and, more generally, impede the adoption of the technology and delay potential benefits.

The OECD *Security Guidelines*[4] and *Privacy Guidelines*[5] provide a comprehensive framework for the security of information systems and network and the protection of privacy and personal data. This framework applies to RFID.

The policy principles that follow provide policy and practical guidance to enhance business and consumer benefits from the use of RFID while proactively taking into account security and privacy concerns. Principles 1 to 6 cover government and business policies and practices to increase the use of, and economic benefits from, wider applications of RFID and emerging related sensor applications. Government policy roles are directed at: incentives for R&D and generic technologies and applications; developing public sector applications and being model users; information, awareness and education activities, including in privacy and security areas and for small businesses; harmonisation of standards; and spectrum allocation issues. Principles 7 to 12 provide all stakeholders with guidance to support the implementation of the *Security and Privacy Guidelines* when they deploy RFID systems. Specific issues are addressed in relation to RFID systems or RFID components in broader systems, including the need for: a comprehensive approach to security and privacy management; security risk and privacy impact assessments; technical measures to protect security and privacy; individuals' information; and a general policy of transparency. Principle 13 calls for a continued dialogue among all stakeholders. Finally, the need for monitoring developments related to RFID is highlighted in Principle 14.

3. E.g. cloning of speed-pass payment RFID cards and automobile ignition keys.

4. OECD Guidelines for the Security of Information Systems and Networks : Towards a Culture of Security (2002).

5. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980).

Principles

1. Support for R&D and new applications

Government support and incentives should focus on R&D for generic RFID-related technologies and applications.

Many of the technological areas underlying RFID are still being developed and there are wide economic benefits to be gained from continued research in areas critical to RFID development, including new materials, and new reading technologies that can be used at greater distances and that can overcome interference and operate in hostile environments. There are social benefits from continued research on issues related to RFID use in the healthcare or environmental areas *e.g.* interference with other medical devices, impact of electromagnetic fields on individuals, or the effect tags will have on recycling practices. Further efforts to research and develop cost-effective technical measures embedding security and privacy protections in RFID systems should also be encouraged (see Principle 9).

2. Technological neutrality

Government policies to encourage the use and expand the benefits of RFID should be technology-neutral.

RFID technologies and applications are highly diverse and evolving rapidly. RFID technologies vary in terms of capabilities (*e.g.* frequency range, battery and memory capacity, size). Individual RFID applications involve a wide range of different operations and industry sectors. Attempts to focus support efforts on particular technologies or applications may diminish resources for other promising avenues and distort markets for components and equipments. Government policies to foster the use and expand the benefits of RFID should not favour one technology or application over another.

3. Governments as model users

As developers and users of RFID for public purposes, governments should share their experience and good practices as widely as possible.

Governments are developing innovative RFID applications in areas ranging from tracking art works and library and museum stocks to improved airport management and defence applications. Their experience and good practices in developing such applications can benefit other actors and should be shared as widely as possible to maximise the benefits from government investments and help diffusion of the technology.

4. Awareness and information

Governments should encourage initiatives to help raise awareness of the benefits and challenges of RFID and encourage sharing of information on large-scale pilots and demonstration projects.

Governments, in conjunction with business associations, the technical community and increasingly with consumer and other citizen groups, have experience in raising awareness of the benefits and challenges of emerging technology applications and their economic and social impacts. Clear and neutral information on RFID technologies, their characteristics and related security and privacy aspects can help small business and the general public appreciate the benefits and risks of these technologies and make informed choices in relation to their use. Governments should promote provision of such information at the earliest possible stage, particularly where applications have cross-sector implications and broad social impacts.

5. Standards

The development of consensus-based global standards for RFID should be encouraged. Issues such as standards convergence should be addressed through market mechanisms to the extent possible.

The development and use of RFID technical and management standards, within and across sectors, enables interoperability, encourages new market entry and allows for economies of scale in applications particularly at the international level. The development of open global RFID standards and standards harmonisation within and across sectors should involve all stakeholders. Standards can play an equally important role in facilitating security and privacy by design and good practices for RFID systems.

6. Spectrum

Governments should encourage and facilitate RFID applications when considering spectrum licensing and allocation.

Governments, manufacturers, standardisation bodies and other stakeholders should co-operate at international level to ensure interoperability, to consider harmonisation of frequency bands as appropriate, to limit harmful interference with other radio devices and users, and to ensure that devices operating within the specified frequency bands comply with the electrical power, radio standards and policy set for those systems, and encourage the development of internationally compatible applications. The exemption of licenses for frequency usage in RFID applications is a recognised licensing option, and is known to be a driver for RFID technology adoption.

7. Security and privacy management

Participants should adopt a comprehensive approach to developing a security and, where appropriate, a privacy management strategy which should be tailored to each RFID system and take into account the interests of all parties involved, including individuals.

All RFID systems require the development of a security management strategy which considers each stage of the system's life (planning, deployment, operation, data processing and end of life) and each component of the system (tags and readers, middleware, databases, network and back-end components).

Not all RFID systems require a privacy management strategy. Such strategy is required when an RFID system collects or processes information relating to an identified or identifiable individual. An organisation which implements an RFID system should conduct a careful analysis of whether the RFID information is personal data (*e.g.* name or personal identifier), or if the RFID information, while not personal data (*e.g.* object identifier), can be linked to an identified or identifiable individual (*e.g.* at the point of sale). In both cases, the RFID system requires a privacy management strategy which considers each step of the RFID data lifecycle, each stage of the system's life, and each component of the system.

8. Security risk and privacy impact assessments

Participants should conduct and periodically review a security risk assessment and, where appropriate, a privacy impact assessment.

Security risk assessment and, where applicable, privacy impact assessment are essential tools for managing security and privacy in relation to RFID systems. Such assessments are necessary to determine the appropriate preventative and mitigation measures to manage the risk of potential harm to RFID systems, to the organisation, and to individuals in light of the nature and sensitivity of the information to be protected. Security risk assessments and privacy impact assessments should take into consideration the technology, the application and operational scenarios, and consider the entire life cycle of the actual RFID tags including those that remain functional even when no longer under the control of the organisation.

The privacy impact assessment of an RFID system should consider whether it is necessary to collect and process information relating to an identified or identifiable individual. It should also take into account the possibility of linking data collected or transmitted using RFID with other data and the potential impact those linkages could have on individuals. This becomes even more important in the case of sensitive personal data

(*e.g.* biometric, health, or identity credential data), as does the issue of protecting the data. Finally, organisations could consider making their privacy impact assessments public, as appropriate.

9. Technical measures to protect security and privacy

Participants who develop or operate RFID technologies and systems should adopt technical security and privacy protection measures in the design and operation of their systems.

A combination of technical and non-technical safeguards is required to ensure security and protect privacy in relation to RFID technologies and systems. Cost-effective technical measures embedding security and privacy protections can play a significant role in reducing risks related to, and fostering trust in, RFID technologies and systems. A number of measures are either available or under development (*e.g.* deactivation, authentication mechanisms, cryptography, data minimisation and anonymisation). Further efforts towards their adoption should be encouraged.

10. Knowledge and consent

Participants who collect or process information relating to identified or identifiable individuals using RFID should do so with the knowledge and, where appropriate, the consent of the individuals concerned.

Individuals should be informed about, or, where appropriate, have the possibility to consent to, the collection, processing, storage and dissemination of RFID data relating to them. Their knowledge or consent should be based on an understanding of the entire RFID data life cycle not just the initial transmission. Governments should encourage all participants to work towards a consensus on the circumstances under which consent should or should not be required.

11. Privacy notices

Participants who collect or process information relating to identified or identifiable individuals using RFID could include more information in RFID privacy notices than in usual privacy notices, given the invisibility of the data collection.

In addition to information about the data collected, the purpose of the collection and the right of access, privacy notices could include all or part of the following: *i)* the existence of tags, *ii)* their content, use and control, *iii)* the presence of active readers, *iv)* the ability to disable tags and *v)* where to obtain assistance. Such explanatory information would also help

educate the public about the new technology. Research towards innovative notification practices, standardised notices and technical means to improve user notification should be encouraged.

12. Transparency

Participants who provide functional tags to individuals — whether or not they collect personal data — should inform individuals about the existence of the tags, any associated privacy risks, and any measures to mitigate these risks.

Participants who provide individuals with RFID tags that remain functional and could be read at a later stage, including by third parties, should have a general policy of transparency about the existence of such tags, their content, any potential privacy risks in presence of active readers, any measures to prevent or mitigate risks such as information on how to deactivate the tags, information on where to obtain assistance, and any further relevant information. Furthermore, there should be a possibility for individuals to disable RFID tags transparently, easily and without extra cost. It is however recognised that there may be specific circumstances in which it would be impossible or involve disproportionate efforts to provide such information, or in which it would not be in the individuals' best interest to disable the RFID devices.

13. Continued dialogue

Governments should encourage all participants to continue to work towards better policies to enhance the economic and social benefits from wider applications of RFID and effectively address outstanding security and privacy issues.

A continued dialogue between all participants will enhance the economic and social benefits from wider applications of RFID, and foster increased security and privacy in RFID systems. The usefulness of such dialogue has already been mentioned in areas such as awareness and information, standards, spectrum, individuals' knowledge and consent, and transparency. Extending the dialogue to the development, publication and adoption of good practices more widely, including security and privacy practices, would facilitate wider diffusion of RFID technologies and help address concerns raised by their potential widespread adoption.

14. Looking forward: monitoring evolution

Governments should encourage research and analysis on the economic and social impacts of the use of RFID in conjunction with other technologies and systems.

Because of continuous technical innovation and its impact on the economy and society, monitoring developments and detecting trends early is essential to identify new opportunities to be seized, new challenges to be addressed, and to adjust policies. Potential developments of RFID to be monitored include their combination with sensor-based systems, their cross-border use, the convergence of these technologies on the Internet, and their potential pervasiveness.

SPAM

RECOMMENDATION OF THE COUNCIL ON CROSS-BORDER CO-OPERATION IN THE ENFORCEMENT OF LAWS AGAINST SPAM (2006)

The council,

Having regard to the Convention on the Organisation for Economic Co-operation and Development of 14th December 1960, in particular Article 5 (b) thereof;

Recognising that spam undermines consumer confidence, which is a prerequisite for the information society and for the success of e-commerce;

Recognising that spam can facilitate the spread of viruses, serve as the vehicle for traditional fraud and deception as well as for other Internet-related threats such as phishing, and that its effects can negatively impact the growth of the digital economy, thus resulting in important economic and social costs for Member countries and non-member economies;

Recognising that spam poses unique challenges for law enforcement in that senders can easily hide their identity, forge the electronic path of their email messages, and send their messages from anywhere in the world to anyone in the world, thus making spam a uniquely international problem that can only be efficiently addressed through international co-operation;

Recognising the need for global co-operation to overcome a number of challenges to information gathering and sharing, for identifying enforcement priorities and for developing effective international enforcement frameworks;

Recognising that current measures, such as numerous bi- and multilateral criminal law enforcement co-operation instruments, provide a framework for enforcement co-operation on criminal conduct associated with spam, such as malware and phishing;

Having regard to the Recommendation of the Council concerning Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders (hereinafter Cross-border Fraud Guidelines), which sets forth principles for international co-operation among consumer protection enforcement agencies in combating cross-border fraud and deception [C(2003)116];

Having regard to the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of

Personal Data [C(80)58] (hereinafter Privacy Guidelines), and the Ministerial Declaration on the Protection of Privacy on Global Networks [C(98)177];

Recognising that, in some instances, the Cross-border Fraud Guidelines and the Privacy Guidelines may apply directly to cross-border spam enforcement co-operation and that even where this is not the case, many of the principles expressed in these Guidelines can be usefully tailored to develop appropriate national frameworks and facilitate international co-operation to enforce laws against spam;

Recalling that, while cross-border enforcement co-operation is an important element in tackling the global problem of spam, it is necessary in this respect to adopt a comprehensive national approach which also addresses regulatory and policy issues, facilitates the development of appropriate technical solutions, improves education and awareness among all players and encourages industry-driven initiatives;

On the joint proposal of the Committee for Information, Computer and Communications Policy and the Committee on Consumer Policy:

Agrees that:

For the purposes of this Recommendation, and without prejudice to other existing co-operation instruments Spam Enforcement Authorities means any national public body, as determined by each Member country, that is responsible for enforcing Laws Connected with Spam and has powers to (a) co-ordinate or conduct investigations or (b) pursue enforcement proceedings, or (c) both.

For the purposes of this Recommendation, Laws Connected with Spam means (a) laws specifically targeting electronic communications; or (b) general laws, such as privacy laws, consumer protection laws or telecommunication laws that may apply to electronic communications.

This Recommendation is primarily aimed at national public bodies, with enforcement authority for Laws Connected with Spam. It is recognised that some Member countries have many competent bodies, some of which are regional or local, that can take or initiate action against spam. It is also recognised that, in some Member countries, private enforcement bodies may play a very important role in ensuring enforcement of Laws Connected with Spam, including in cross-border situations.

This Recommendation covers cross-border spam enforcement co-operation only in areas where the conduct prohibited by the Laws Connected with Spam of the Member country receiving a request for assistance is substantially similar to conduct prohibited by the Laws Connected with Spam of the Member country requesting assistance. Co-operation under this Recommendation does not affect the freedom of expression as protected in laws of Member countries.

Co-operation under this Recommendation focuses on those violations of Laws Connected with Spam that are most serious in nature, such as those that (a) cause or may cause injury (financial or otherwise) to a significant number of recipients, (b) affect particularly large numbers of recipients (c) cause substantial harm to recipients.

In all instances, the decision on whether to provide assistance under this Recommendation rests with the Spam Enforcement Authority receiving the request for assistance.

This Recommendation encourages Member countries to cooperate in this area under any other instruments, agreements, or arrangements.

Recommends that:

Member countries work to develop frameworks for closer, faster, and more efficient co-operation among their Spam Enforcement Authorities that includes, where appropriate:

a) Establishing a domestic framework.

Member countries should in this respect:

(i) Introduce and maintain an effective framework of laws, Spam Enforcement Authorities, and practices for the enforcement of Laws Connected with Spam.

(ii) Take steps to ensure that Spam Enforcement Authorities have the necessary authority to obtain evidence sufficient to investigate and take action in a timely manner against violations of Laws Connected with Spam that are committed from their territory or cause effects in their territory. Such authority should include the ability to obtain necessary information and relevant documents.

(iii) Improve the ability of Spam Enforcement Authorities to take appropriate action against (a) senders of electronic communications that violate Laws Connected with Spam and (b) individuals or companies that profit from the sending of such communications.

(iv) Review periodically their own domestic frameworks and take steps to ensure their effectiveness for cross-border co-operation in the enforcement of Laws Connected with Spam.

(v) Consider ways to improve redress for financial injury caused by spam.

b) Improving the ability to cooperate.

Member countries should improve the ability of their Spam Enforcement Authorities to cooperate with foreign Spam Enforcement Authorities.

Member countries should in this respect:

i) Provide their Spam Enforcement Authorities with mechanisms to share relevant information with foreign authorities relating to violations of their Laws Connected with Spam upon request, in appropriate cases and subject to appropriate safeguards.

ii) Enable their Spam Enforcement Authorities to provide investigative assistance to foreign authorities relating to violations of their Laws Connected with Spam upon request, in appropriate cases and subject to appropriate safeguards, in particular with regard to obtaining information from persons; obtaining documents or records; or locating or identifying persons or things.

iii) Designate a contact point for co-operation under this Recommendation and provide the OECD Secretariat with updated information regarding their Laws Connected with Spam and the Spam Enforcement Authority designated as the contact point. The OECD Secretariat will keep record of this information and make it available to interested parties.

c) Improving procedures for co-operation.

Before making requests for assistance as foreseen in the previous paragraphs, Spam Enforcement Authorities should:

i) Proceed to some preliminary investigative work to determine whether a request for assistance is warranted, and is consistent with the scope and priorities set forth by this Recommendation.

ii) Attempt to prioritise requests for assistance and, to the extent possible, make use of common resources such as the OECD Website on spam, informal channels, existing international networks and existing law enforcement co-operation instruments to implement this Recommendation.

d) Cooperating with relevant private sector entities.

Spam Enforcement Authorities, businesses, industry groups, and consumer groups should cooperate in pursuing violations of Laws Connected with Spam. In particular, Spam Enforcement Authorities should cooperate with these groups on user education, promote their referral of relevant complaint data, and encourage them to

share with Spam Enforcement Authorities investigation tools and techniques, analysis, data and trend information.

Member countries should encourage co-operation between Spam Enforcement Authorities and the private sector to facilitate the location and identification of spammers.

Member countries should also encourage participation by private sector and non-member economies in international enforcement co-operation efforts; efforts to reduce the incidence of inaccurate information about holders of domain names; and efforts to make the Internet more secure.

Where appropriate, Spam Enforcement Authorities and the private sector should continue to explore new ways to reduce spam.

Invites non-member economies to take due account of this Recommendation and collaborate with Member countries in its implementation.

Instructs the Committee for Information, Computer and Communications Policy and the Committee on Consumer Policy to monitor the progress in cross-border enforcement co-operation in the context of this Recommendation within three years of its adoption and thereafter as appropriate.