

**Unclassified**

**DSTI/ICCP/REG(2002)3/FINAL**



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

**21-Jan-2003**

**English - Or. English**

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

**Cancels & replaces the same document of 13 January 2003**

**Working Party on Information Security and Privacy**

**PRIVACY ONLINE: POLICY AND PRACTICAL GUIDANCE**

**DSTI/ICCP/REG(2002)3/FINAL  
Unclassified**

**English - Or. English**

**JT00137976**

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

## **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.

**Copyright OECD, 2003.**

**Applications for permission to reproduce or translate all or part of this material should be made to:**

**Head of Publications Service, OECD, 2 rue André-Pascal, 75775 Paris Cedex 16, France.**

## TABLE OF CONTENTS

MAIN POINTS.....	4
INTRODUCTION .....	5
The 1980 OECD Privacy Guidelines .....	5
Privacy protection in the global information society .....	5
Background to the Ministerial Mandate.....	6
Ministerial Declaration.....	6
OECD Action Plan.....	7
I. FULFILLING THE MINISTERIAL MANDATE: OECD WORK.....	8
1) Encouraging the adoption of privacy policies .....	8
2) Encouraging the online notification of privacy policies to users .....	9
3) Ensuring that enforcement and redress mechanisms are available to users in cases of non-compliance with privacy principles and policies.....	9
4) Promoting user education and awareness about online privacy and the means of protecting privacy.....	12
5) Encouraging the use of privacy enhancing technologies.....	12
6) Encouraging the use and development of contractual solutions for online transborder data flows.....	13
II. MOVING FORWARD: POLICY AND PRACTICAL GUIDANCE FOR IMPLEMENTING PRIVACY PROTECTION ONLINE .....	15
Blending approaches .....	15
Strengthening co-operation .....	16
PRACTICAL GUIDANCE ON POLICY FOR OECD MEMBER COUNTRIES .....	16
At the national level.....	16
At the global level .....	18
PRACTICAL GUIDANCE FOR BUSINESSES AND OTHER ORGANISATIONS .....	19
PRACTICAL GUIDANCE FOR INDIVIDUAL USERS AND CONSUMERS .....	19
III. ANNEXES.....	20

## 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.<sup>1</sup> The eight principles are:

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

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

### Privacy protection in the global information society

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

In the digital economy, individuals may leave behind electronic “footprints” or records of where they have been, what they spent time looking at, the thoughts they aired, the messages they sent, and the goods and services they purchased. The related privacy issues arise from the fact that all this computer-processable personal information, whether automatically generated or not, can potentially be collected, stored, detailed, individualised, linked and put to a variety of uses in places geographically dispersed all around the world, possibly without user knowledge or consent.

---

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.

## 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,<sup>2</sup> and launched action in this area to be pursued over the next few years.

## Ministerial Declaration

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

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

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

---

2. See Annex II.

## 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.<sup>3</sup> In this context, the Working Party on Information Security and Privacy (WPISP), under the auspices of the Committee for Information, Computer and Communications Policy (ICCP) focused much of its work on the implementation of the elements of the OECD six-step programme of work for online privacy protection:

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

All documents and other instruments (*e.g.* Internet-based tools) produced by the WPISP and declassified by the ICCP are 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.

---

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).

## 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<sup>4</sup> included horizontal or sectoral data protection laws, codes of conduct, industry standards and industry-led technological solutions, including privacy enhancing technologies (PETs), online educational tools, systems for labelling, certifying and attaching privacy seals, and dispute resolution schemes. It was noted that technological tools were increasingly used to protect privacy rights online. The fact that effective protection of privacy online required online participants to be not only “information technology literate”, but also aware of the privacy implications of their actions was emphasised.

### 1) Encouraging the adoption of privacy policies

OECD member countries developed a Privacy Policy Statement Generator<sup>5</sup> (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.

---

4. See Annex III.

5. See Annex IV for a “paper copy”. The Generator is accessible at [www.oecd.org/sti/security-privacy](http://www.oecd.org/sti/security-privacy) or <http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm>.

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.<sup>6</sup> The inclusion of links to relevant government and private sector Web sites is intended to increase business and other organisations' as well as individual user and consumer awareness of the privacy protection framework that applies to their online activities.

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

The positive perception by the public of online privacy policies is confirmed by a few public opinion polls and surveys. For example, a study conducted in 2000 showed that 75% of online users and consumers tended to trust Web sites more when privacy policy statements were posted on those merchants' sites.<sup>7</sup> Similarly, a May 2002<sup>8</sup> 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<sup>9</sup> 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.

---

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/>.

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.

### *Alternative dispute resolution*

OECD member countries undertook a series of studies on ADR, which consists of practical out-of-court methods involving a neutral third-party to resolve disputes in a quick and inexpensive way. In December 2000 the OECD,<sup>10</sup> 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”.<sup>11</sup> 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<sup>12</sup> was developed on the basis of member country responses to a survey on existing laws and regulations related to ADR. The report highlighted that there is not a single set of rules governing ADR. Different rules have developed in different contexts. In a number of areas the existing legal framework provides guidance to potential parties to an ADR procedure at the national level. For example, many countries regulate the provision of arbitration services. However, there are fewer regulations that would generally govern the provision of less formal types of B2C ADR. What regulation there is typically addresses the provision of ADR through mechanisms established, funded or run by governments. As regards flexible and informal ADR mechanisms designed for the online world, no member country reported the existence of specific legal provisions although most expressed an interest in promoting fair and effective online ADR as a way to resolve small value B2C disputes, particularly cross-border disputes. Looking more specifically at the cross-border context, national differences appeared as to the validity of agreements to submit to ADR, the procedural principles for use during an ADR, confidentiality and security of proceedings, validity of settlement agreements arising out of an ADR, and the availability of enforcement mechanisms.

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

---

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.

13. See Annex VII.

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.<sup>14</sup>

### ***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.<sup>15</sup> 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<sup>16</sup> demonstrated that the legal landscape for privacy compliance and enforcement has changed: if government regulation remains the foundation upon which individual user trust in the area of privacy is based, regulation is increasingly combined with complementary technical, organisational, and self-regulatory mechanisms in order to attain maximum effectiveness. It was noted that many such initiatives are now underway in member countries, and that there is every sign that their use will grow rapidly in the coming years. Moreover, the report stressed that efforts to ensure compliance before the fact impose less burden than having to rely on enforcement actions. It also demonstrated that it is critical that privacy protection be viewed in a global perspective, rather than in a purely national one, in order to better facilitate redress for privacy violations that cross national borders.

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

---

14. See [http://www.iccwbo.org/home/news\\_archives/2002/stories/adr.asp](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](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.

**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.<sup>17</sup>

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

The Inventory of Privacy Enhancing Technologies<sup>18</sup> 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<sup>19</sup> 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<sup>20</sup> 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

---

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.

Privacy Guidelines (*e.g.* among the PETs surveyed (see paragraph below), only one tool addressed five of the eight privacy principles and 58 applied to only one principle).

A study and a research paper<sup>21</sup> 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.<sup>22</sup> They can empower individual users seeking to control the disclosure, use and distribution of personal information online. PETs can also aid organisations in enforcing their own privacy policies and practices, and more generally, in an era of individual user concerns about online privacy, PETs are crucial tools in managing the flow of personal information on global networks.

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

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

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

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

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

### **“Part Three – Basic Principles of International Application: Free Flow and Legitimate Restrictions**

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

---

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.

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.<sup>23</sup> The report<sup>24</sup> 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.<sup>25</sup>

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.

---

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).

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](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.

## 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,<sup>26</sup> OECD member countries agreed that each of these approaches had advantages and disadvantages. Government efforts seemed to offer predictable, enforceable legal protections and redress mechanisms, and self-regulatory efforts appeared to enable organisations in different sectors to tailor detailed guidelines to work within specific circumstances. In both approaches, difficulties in adequately addressing privacy online were foreseen, particularly with respect to cross-border issues. The debate moved then to discuss what mix of instruments and techniques would be best tailored to the protection of privacy in the global online environment.

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

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

---

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>.

## **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.<sup>27</sup>

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<sup>28</sup> 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>.

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.

---

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.

- 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<sup>29</sup> related to International Co-operation, and endeavour to establish procedures to improve bilateral and

---

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.”

multilateral mechanisms for cross-border co-operation between public enforcement agencies in the procedural and investigative matters involved or called for in the Guidelines.

- Continue to co-ordinate with the private sector and explore how recourse to public/private partnerships could help building organisations' and individual user trust online in areas where technology and regulation are closely interrelated such as online dispute resolution and privacy enhancing technologies.
- Promote co-operation with other international organisations as appropriate.
- Continue to explore ways to further online trust across all participants through appropriate outreach, education, co-operation and consultation.

## **PRACTICAL GUIDANCE FOR BUSINESSES AND OTHER ORGANISATIONS**

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

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

## **PRACTICAL GUIDANCE FOR INDIVIDUAL USERS AND CONSUMERS**

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

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

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

### 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	<a href="http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm">http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm</a>
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 publication of the same name, “Privacy Online: Policy and Practical Guidance”. The annex files are too large in memory to include in this OLIS release.