Anne Carblanc[1]

Building Bridges between different approaches of privacy

1. Background

While there is a difference between those countries who see the protection of privacy as a matter of human rights and those who have approached it as a practical matter which must be addressed to ensure continued transborder data flows, all OECD Member countries share the same commitment to the protection of privacy, based on the OECD Privacy Guidelines.

Indeed in 1998, at the OECD Ministerial level Conference »A Borderless World: Realising the Potential of Global Electronic Commerce« held in Ottawa on 7-9 October 1998, Ministers reaffirmed this commitment to privacy protection in order to ensure the respect of important rights, build confidence in the online environment, and to prevent unnecessary restrictions on transborder flows of personal data. They declared they would build bridges between their traditional national approaches and take the necessary steps to ensure, by various specified measures, the effective implementation of the OECD 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[2].

The online environment

Digital computer and network technologies, and in particular the Internet, have facilitated information exchange, allowed the creation of new products and services, and increased user and consumer choice. However, as Internet users leave behind electronic »footprints« or records of where they have been, what they spent time looking at, the thoughts they aired, or the goods and services they purchased, concerns over the protection of privacy and personal data have increased deriving from the fear that all this computerprocessable personal information, whether automatically generated or not, be collected, stored, detailed, individualised, and easily linked and put to a variety of uses in places geographically dispersed all around the world, without the user knowledge or consent.

In this context, the OECD was considered the appropriate forum to foster a dialogue among governments, the private sector, the user and consumer communities, and data protection authorities in order to:

»Offer a balanced understanding of the issues linked to the protection of privacy and transborder flows of personal data in relation to global networks«

»Consider the various solutions which would facilitate the seamless implementation of privacy protection online and contribute towards building a trustworthy environment for the development of electronic commerce«.

The two traditional approaches to protection of privacy

Privacy protection has traditionally been approached as if there were primarily two approaches: government regulatory and legislative actions and market-based self-regulatory efforts. Each of these approaches has advantages and disadvantages and it cannot be assumed that one system is more effective than the other is. Government efforts offer predictable, enforceable legal protections and redress mechanisms yet they may lack the predictive skills and flexibility to adequately regulate the online environment. Self-regulatory efforts enable organisations in different sectors to tailor detailed guidelines to work within specific circumstances. However, the resulting policy patchwork and divergent implementation may not provide the necessary transparency, uniformity and legal certainty. Whatever the approach is, enforceability is crucial because compliance either with statutory or self-regulation is not automatic, and more and more, the »summa divisio« between regulation and self-regulation is seen as a false dichotomy.

The 1980 OECD Privacy Guidelines

The widely accepted and technologically neutral privacy principles found in the OECD Privacy Guidelines represent an international consensus on basic principles for protecting privacy and personal information. Irrespective of differences in national approaches to privacy, they still provide appropriate guidance for handling personal data on global networks. The eight principles are:

- Collection Limitation: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- Data Quality: Personal data should be relevant to the purpose 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: 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: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except:
  a) With the consent of the data subject; or
  b) By the authority of law.
- Security Safeguards: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
- Openness: There should be a general policy of openness about develop-

ments, practices and polices with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purpose of their use, as well as the identity and usual residence of the data controller.
- Individual Participation: An individual should have the right:
  a) To obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
  b) To have communicated to him, data relating to him
  i) Within a reasonable time;
  ii) At a charge, if any that is not excessive;
  iii) In a reasonable manner; and
  iv) In a form that is readily intelligible to him;
  c) To be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
  d) To challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.
- Accountability: A data controller should be accountable for complying with measures which give effect to the principles stated above.

The OECD ministerial mandate

Since 1998, the OECD has focused much of its work on the implementation of the elements of the six-step programme of work for online privacy protection approved by Ministers at the Ottawa Conference. These steps included:
- 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, and
- encouraging the use and development of contractual solutions for online transborder data flows.

To carry out this programme of work, the OECD has closely co-operated with business, industry, privacy experts and consumer representatives, as well as with relevant regional and international organisations. The work achieved has accelerated consensus on effective protection within the framework of either industry-led self-regulation or legal regulation.

The OECD has adopted a pragmatic approach with 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. User education and awareness about pri-

vacy has been considered in each component of the work achieved, in particular when designing the Privacy Generator and examining PETs.

2. Work achieved by the OECD Committee for Information, Computer and Consumer Policy (ICCP[3])

The exchange and analysis of information

In furtherance of the Privacy Declaration, the OECD has commenced new studies by compiling inventories and overviews, and organising broad-based workshops to better inform itself before performing analysis.

Inventory of Instruments and Mechanisms Contributing to the Implementation and Enforcement of the OECD Privacy Guidelines on Global Networks (1998-1999)

With a focus on the online environment, the OECD 1999 inventory surveyed, at international, regional and national levels, the legal and self-regulatory instruments, practices, techniques and technologies, either in use or being developed, to implement and enforce privacy principles in networked environments. If the inventory recognised the wide variety of traditional instruments to implement the OECD Privacy Guidelines, it also drew attention to the emerging trend for privacy rights to be protected online through technological tools, some of which allow users to take charge of their own data protection and privacy. It emphasised that effective protection of privacy online requires an online public not only knowledgeable enough to look after themselves through use of these tools, but also aware of the privacy implications of their actions.

Report on Transborder Data Flow Contracts in the Wider Framework of Mechanisms for Privacy Protection Online (1999-2000)

The report aimed at helping develop a common understanding of the issues raised by applying contractual analysis and structures to online communications, in particular to business to consumer (or B2C) communications. Recognising the potential of contracts, and in particular B2B model contracts, to satisfy privacy protection expectations as measured against various privacy instruments, regardless of whether or not the transfer occurs in an online or offline environment, the report, however, stressed the need to address effectively the issue of the recourse of the individual under a B2B transborder data flow contract. In this respect, the support of ancillary measures, such as notice to the individuals at the point of data collection, was mentioned.

Therefore, the report recommended the monitoring of future developments in the work of other international organisations[4] having expertise and experience in the area of B to B privacy model contracts.

As concerns B2C contracts, the report demonstrated that attempts to design privacy protection measures for online B2C interactions within the constraints of a contractual framework posed many difficulties. In this respect, the difficulty of establishing a binding intention to contract, between an individual visiting a Web site and the data controller of that Web site, or the difficulties facing any individual wishing to obtain redress under a contract were mentioned. The report therefore recommended focussing less on contractual solutions, and more on exploring how to ensure redress through online alternative dispute resolution measures.

Alternative Dispute Resolution (ADR) Mechanisms for B2C Privacy and Consumer Protection Disputes (2000-2002)

Alternative Dispute Resolution (ADR) refers to mechanisms and processes intended to supplement court adjudication in assisting parties in resolving differences. The objective of the Joint OECD Conference with the Hague Conference on Private International Law and the International Chamber of Commerce (ICC), was to explore whether and how online ADR mechanisms can help resolve B 2 C disputes arising from privacy and consumer protection issues, and thus improve trust for global electronic commerce. The primary focus of the conference was on B 2 C disputes involving small values and/or low levels of harm, as well as on informal, flexible systems that allow for the necessary balancing between the type of dispute and the formality of the process for resolution (e.g. assisted negotiation and mediation). Socio-economic issues, legal issues, technological issues, educational issues, and issues related to trust seals and compliance were discussed.

The Conference's main conclusions were that:

- Complaints in relation to e-commerce are growing.
- Strong stakeholder co-operation is key.
- Settling disputes as soon as possible is most effective.
- Flexibility and variety in ADR mechanisms are valuable.
- Some common principles are already emerging, such as accessibility, low cost for consumers, transparency, speed of decision, impartiality, but there remains a debate about other important matters, such as voluntary or mandatory recourse to ADR, the binding or non-binding effect of outcomes, and their enforcement.
- Socio-economic/cultural barriers, such as language or differences in how cultures approach disputes and disagreements, must be addressed.
- Appropriate technological developments may facilitate more effective ADR mechanisms.

Following up the Conference, the OECD undertook to help provide guidance

as to how best to use ADR with regard to the OECD Privacy and Consumer Protection Guidelines by updating the list of online ADR mechanisms in co-operation with the ICC; developing an educational instrument including a series of questions for potential parties to online ADR (individual users and businesses, notably SMEs) and intended to inform and guide them; and finally, surveying potential cross-border legal challenges to resolving privacy and consumer-related disputes through online ADR. This work is close to its completion.

The exploration of technology

The OECD has also explored how the capabilities of network technologies and their interactive characteristics could provide a potential effective means of education and protection for users, by facilitating access to information and developing skills, thus improving the practical ability to protect oneself. The OECD has notably developed a privacy statement generator, and examined privacy-enhancing-technologies.

The OECD Privacy Policy Statement Generator (1999-2000)

An educational Internet technology based tool (the Privacy Generator[5]) was developed with the help of DaimlerChrysler and Microsoft to provide an information resource about privacy protection at the international, regional and national levels. The objective was to offer guidance on compliance with the OECD Privacy Guidelines and to assist organisations in developing privacy policies and statements for display on their Web sites. In particular, the Generator was designed to produce a draft statement that furnishes an indication of the extent to which the privacy practices of a Web site are consistent with the Privacy Guidelines, so as to provide organisations with an online step by step guidance tool to help them respect privacy protection in their activities at a global level.

By endorsing the Privacy Generator, OECD Member countries took a key practical step towards encouraging openness and trust in electronic commerce among visitors to Web sites. By making the Generator widely available free of charge on the Web, OECD Member countries intended to increase business and individual awareness of the privacy protection framework that applies to their online activities. They emphasised that by dealing fairly and in good faith with the Generator and the substance of the statements which it produces, businesses can help ensure that their privacy policy and statement will not misrepresent their privacy practices or be inconsistent with applicable regulations. They stressed that the online notification of such privacy statements can also help individual users to make informed choices about entrusting an organisation with personal data. They recalled that, once their privacy state-

ments are publicly posted, businesses may be legally liable if they fail to abide by it or if their statement does not comply with local laws.

Privacy-Enhancing Technologies (PETs) (2001-2002)

PETs are technological tools that can assist in safeguarding the privacy of users and consumers. They are part of the wider package of privacy initiatives and can help implement privacy principles, such as those contained in the OECD Privacy Guidelines, within the framework of either industry-led self-regulation or legal regulation. 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 advances in the development and use of such technologies. Work on PETs by the OECD included an inventory of these technologies, and a special Forum session.

An inventory was produced by a consultant to the OECD[6] to analyse the availability and variety of PETs, consider the factors affecting adoption of PETs, analyse the relationship between technology and privacy, and form a basis for policy makers to discuss the use and deployment of such technologies. The paper 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, different technologies and various functions can serve different purposes depending on the preferences of the user and the implementation of the particular technology.

A special Forum Session on Privacy-Enhancing Technologies was held at the OECD on 8 October 2001 in order to facilitate discussion on: the policy implications of PETs and the future of PETs in the wider context of online privacy protection; and the challenges of, and methods for educating business about the importance of privacy by design and the use of PETs, and educating individuals about the benefits and limitations of PETs. The session made it clear, in particular, that technically speaking, none of the tools identified used a full range of functionalities that would provide total privacy protection in line with the OECD Privacy Guidelines, e.g. only one tool addressed five of the eight privacy principles and fifty eight concerned only one principle.

A study and a research paper by two consultants to the OECD[7] included a

synthesis of a survey of PETs currently 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.

The discussion highlighted that though PETs are helpful technological tools that can assist in safeguarding online privacy, they are part of a wider package of online privacy initiatives.[8] The need to encourage both individual and corporate users, as well as software developers to develop, deploy and use PETs as part of a broader online privacy protection strategy was also stressed. It was also agreed that the early stage of any technological development is its most critical, and that all stakeholders need to be actively involved in the development of technologies to help ensure that global rights and protections can be taken into account and integrated into systems from the beginning (the concept of »privacy by design«).

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

Report on Regulatory and Self-regulatory Legal and Technical Instruments and Mechanisms for Compliance with and Enforcement of Privacy Protection (2002)

This still ongoing work gathers information about existing systems for compliance, enforcement and redress for privacy protection, examining their availability and efficiency on global networks. It is expected that the information gathered will 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 Ministerial Declaration. It will assess the practical application of available compliance and enforcement instruments in a networked environment and their ability to meet the objectives of the OECD Guidelines, including effectiveness and coverage across jurisdictions. It is hoped that this exercise will help identify gaps and barriers to interoperability, and suggest solutions to facilitate seamless privacy protection.

3. Conclusion

Considering the work already achieved and what still needs to be done to help ensure effective privacy protection and build trust online, it is important that governments continue to co-operate among themselves and with the other stakeholders.

Efforts to implement privacy protection online at the global level should take account of the following:

Any approach to implementing the privacy Guidelines online must have flexibility as a key principle to allow for differences between nations and cultures and to respond to the social and psychological diversity of the various actors on global networks. A mixture of regulatory and self-regulatory approaches as well as of legal, technical and educational solutions is likely to deliver privacy most effectively.

The first step toward respect for privacy online is to provide transparency. To this end, businesses should continue to develop and publicise their privacy practices, and to offer effective and efficient user/consumer service (e.g. privacy contact person or chief privacy officer) and complaints handling systems. Development and use of other mechanisms such as trustmark programmes, privacy-enhancing-technologies are also positive, as part of the wider privacy package.

Education is essential even though it cannot be a substitute for proper regulation or practices. Practical guidance and sufficient information should be made available so that users/consumers can understand the capabilities of the technology, assert their rights, and make appropriate choices about whether or not to entrust businesses with the collection and use of their personal information.

1 This paper represents the views of the author and not necessarily those of the OECD.
2 OECD Ministerial Declaration on the Protection of Privacy on Global Networks [C(98)177].
3 The documents and other instruments (e.g. Internet-based tools) listed below have been produced by the OECD Committee for Information, Computer and Consumer Policy (ICCP), and can be found on the OECD web site www.oecd.org/sti/security-privacy.
4 Such as the ICC, the Council of Europe and the European Commission.
5 http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm
6 Lauren Hall, Executive Vice President of the Software & Information Industry Association.
7 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.
8 The wider privacy package includes notably the development and notification of privacy policies, the use of contractual solutions, and an increasing availability of online redress mechanisms – in addition to privacy-enhancing technologies.